

kaspersky

Kaspersky Security Center (для Windows)

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 15.1.0.20748

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью АО Kaspersky Lab (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, "Лаборатория Касперского" ответственности не несет.

В этом документе используются зарегистрированные товарные знаки и знаки обслуживания, которые являются собственностью соответствующих правообладателей.

Дата редакции документа: 03.10.2024

© 2024 АО Kaspersky Lab

<https://www.kaspersky.ru>
<https://help.kaspersky.com/ru>
<https://support.kaspersky.ru>

О "Лаборатории Касперского" <https://www.kaspersky.ru/about/company>

Содержание

Об этом документе	14
Требования.....	15
Указания по эксплуатации и требования к среде	15
Аппаратные и программные требования.....	16
Требования к Серверу администрирования	16
Требования к Web Console	17
Требования к серверам мобильных устройств	18
Требования к Консоли администрирования	19
Требования к Агенту администрирования.....	19
Совместимые приложения и решения "Лаборатории Касперского"	25
Kaspersky Security Center	27
О Kaspersky Security Center	28
Лицензии и возможности Kaspersky Security Center.....	29
О совместимости компонентов Kaspersky Security Center.....	33
Сравнение версий Kaspersky Security Center: на базе Windows и на базе Linux	35
Основные понятия	39
Сервер администрирования	39
Удаление иерархии Серверов администрирования.....	41
Виртуальный Сервер администрирования	41
Сервер мобильных устройств	42
Веб-сервер	43
Агент администрирования	43
Группы администрирования	44
Управляемое устройство	45
Нераспределенное устройство	45
Рабочее место администратора	45
Плагин управления	46
Веб-плагин управления.....	46
Политики.....	47
Профили политик.....	48
Задачи.....	48
Область действия задачи	50
Взаимосвязь политики и локальных параметров приложения.....	51
Точка распространения.....	51
Шлюз соединения	54
Архитектура приложения	56
Основной сценарий установки	56
Порты, используемые Kaspersky Security Center.....	63
Сертификаты для работы с Kaspersky Security Center	71

О сертификатах Kaspersky Security Center	72
О сертификате Сервера администрирования	75
Требования к пользовательским сертификатам, используемым в Kaspersky Security Center	76
Сценарий: задание пользовательского сертификата Сервера администрирования.....	78
Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert	81
Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmove	83
Перевыпуск сертификата Веб-сервера	84
Схемы трафика данных и использования портов.....	87
Сервер администрирования и управляемые устройства в локальной сети (LAN).....	88
Главный Сервер администрирования в локальной сети (LAN) и два подчиненных Сервера администрирования.....	90
Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование обратного прокси-сервера	93
Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения.....	96
Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете	101
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Лучшие практики развертывания	116
Руководство по усилению защиты	117
Подготовка к развертыванию	133
Развертывание Агента администрирования и приложения безопасности	163
Установка Kaspersky Security Center	206
Подготовка к установке	206
Учетные записи для работы с СУБД.....	207
Сценарий: аутентификация Microsoft SQL Server.....	224
Рекомендации по установке Сервера администрирования	226
Стандартная установка	229
Выборочная установка	234
Развертывание отказоустойчивого кластера Kaspersky Security Center	244
Установка Сервера администрирования на отказоустойчивом кластере Windows Server	254
Установка Сервера администрирования в тихом режиме	264
Установка Консоли администрирования на рабочее место администратора	270
Изменения в системе после установки Kaspersky Security Center.....	271
Удаление приложения.....	275
Об обновлении предыдущей версии Kaspersky Security Center	275
Обновление предыдущей версии Kaspersky Security Center	276
Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center	277
Обновление Kaspersky Security Center на узлах отказоустойчивого кластера Microsoft	278
Первоначальная настройка Kaspersky Security Center	280

Руководство по усилению защиты	280
Мастер первоначальной настройки Сервера администрирования	281
Настройка подключения Консоли администрирования к Серверу администрирования	296
Подключение автономных устройств	297
Шифрование подключения TLS	317
Настройка интерфейса	320
Обнаружение устройств в сети.....	322
Сценарий: обнаружение сетевых устройств	322
Нераспределенные устройства.....	323
Инвентаризация оборудования.....	338
Лицензирование.....	340
События превышения лицензионного ограничения.....	341
О лицензировании	341
О предоставлении данных.....	347
Варианты лицензирования Kaspersky Security Center	354
Особенности лицензирования Kaspersky Security Center и управляемых приложений	355
Приложения "Лаборатории Касперского". Централизованное развертывание	357
Замещение приложений безопасности сторонних производителей	358
Установка приложений с помощью задачи удаленной установки	359
Установка приложений с помощью мастера удаленной установки	363
Работа с плагинами управления	368
Просмотр отчета о развертывании защиты	369
Удаленная деинсталляция приложений.....	370
Работа с инсталляционными пакетами	371
Получение актуальных версий приложений	381
Подготовка устройства под управлением Windows к удаленной установке	383
Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux	384
Подготовка устройства с операционной системой macOS к удаленной установке Агента администрирования.....	387
Приложения "Лаборатории Касперского": лицензирование и активация	388
Лицензирование управляемых приложений	389
Просмотр информации об используемых лицензионных ключах.....	391
Добавление лицензионного ключа в хранилище Сервера администрирования.....	392
Удаление лицензионного ключа Сервера администрирования.....	393
Распространение лицензионного ключа на клиентские устройства.....	394
Автоматическое распространение лицензионного ключа.....	398
Создание и просмотр отчета об использовании лицензионных ключей	399
Просмотр информации о лицензионных ключах приложения	400
Экспорт файла ключа.....	400
Процедура приемки	401

Безопасное состояние.....	401
Проверка работоспособности Kaspersky Security Center.....	401
Настройка защиты сети.....	403
Сценарий: настройка защиты сети	403
Настройка и распространение политик: подход, ориентированный на устройства	405
Подходы к управлению безопасностью, ориентированные на устройства и на пользователей	407
Ручная настройка политики Kaspersky Endpoint Security	408
Ручная настройка групповой задачи обновления Kaspersky Endpoint Security	412
Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security	412
Настройка расписания задачи Поиск уязвимостей и требуемых обновлений.	412
Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей	413
Настройка количества событий в хранилище событий.....	413
Установка максимального срока хранения информации о закрытых уязвимостях.....	414
Управление задачами	414
Создание иерархии групп администрирования, подчиненных виртуальному Серверу администрирования.....	429
Политики и профили политик	431
Правила перемещения устройств.....	451
Копирование правил перемещения устройств	452
Категоризация программного обеспечения	452
Необходимые условия для установки приложений на устройства организации-клиента	453
Просмотр и изменение локальных параметров приложения	454
Обновление Kaspersky Security Center и управляемых приложений.....	455
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....	455
Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского".....	460
Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского".....	467
Включение функции загрузки файлов различий.....	468
Создание задачи для загрузки обновлений в хранилище Сервера администрирования	469
Создание задачи загрузки обновлений в хранилища точек распространения	474
Настройка параметров задачи загрузки обновлений в хранилище Сервера администрирования	479
Проверка полученных обновлений	479
Настройка проверочных политик и вспомогательных задач	481
Просмотр полученных обновлений.....	482
Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства	482
Офлайн-модель получения обновлений	484
Включение и выключение офлайн-модели получения обновлений	485
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center	487
Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center	487
Автоматическое распространение обновлений.....	488

Удаление обновлений программного обеспечения из хранилища	497
Установка патча для приложения "Лаборатории Касперского" в кластерной модели	497
Управление приложениями сторонних производителей на клиентских устройствах	498
Установка обновлений приложений сторонних производителей	498
Уязвимости в приложениях	528
Группы приложений	571
Мониторинг и отчеты	592
Сценарий: мониторинг и отчеты	593
Мониторинг цветковых индикаторов и зарегистрированных событий в Консоли администрирования	595
Работа с отчетами, статистикой и уведомлениями	601
Мониторинг установки и удаления приложений	636
События компонентов Kaspersky Security Center	636
Блокировка частых событий	678
Контроль изменения состояния виртуальных машин	681
Отслеживание состояния антивирусной защиты с помощью информации в системном реестре ..	682
Просмотр и настройка действий, когда устройство неактивно	683
Выключение объявлений "Лаборатории Касперского"	685
Настройка точек распространения и шлюзов соединений	685
Типовая конфигурация точек распространения: один офис	686
Типовая конфигурация точек распространения: множество небольших удаленных офисов	687
Назначение управляемого устройства точкой распространения	688
Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне ..	691
Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения	692
Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения ..	693
Автоматическое назначение точек распространения	694
О локальной установке Агента администрирования на устройство, выбранное точкой распространения	694
Об использовании точки распространения в качестве шлюза соединений	695
Добавление IP-диапазонов в список диапазонов, опрашиваемых точкой распространения	696
Использование точки распространения в качестве извещающего сервера	697
Другие повседневные задачи	699
Управление Серверами администрирования	699
Управление группами администрирования	742
Управление клиентскими устройствами	747
Управление учетными записями пользователей	803
Удаленная установка операционных систем и приложений	843
Работа с ревизиями объектов	852
Удаление объектов	858
Хранилища данных	861

Kaspersky Security Network и Kaspersky Private Security Network	873
Переключение между онлайн-справкой и офлайн-справкой	878
Экспорт событий в SIEM-системы.....	879
Сценарий: настройка экспорта событий в SIEM-системы	879
Предварительные условия	881
О событиях в Kaspersky Security Center	881
Об экспорте событий.....	883
О настройке экспорта событий в SIEM-системе	884
Выбор событий для экспорта в SIEM-системы в формате Syslog	886
Об экспорте событий в формате Syslog	891
Об экспорте событий в форматах CEF и LEEF	891
Настройка Kaspersky Security Center для экспорта событий в SIEM-систему	892
Экспорт событий напрямую из базы данных	894
Просмотр результатов экспорта	899
Использование SNMP для отправки статистики приложениям сторонних производителей.....	900
Настройка SNMP-службы для использования с Kaspersky Security Center	900
SNMP-агент и идентификаторы объектов.....	901
Получение имени счетчика строк из идентификатора объекта	901
Значения идентификаторов объектов для SNMP	902
Устранение неисправностей.....	911
Приложения.....	913
Дополнительные возможности	913
Особенности работы с интерфейсом управления	921
Справочная информация.....	927
Поиск и экспорт данных	937
Параметры задач.....	951
Глобальный список подсетей	966
Использование Агента администрирования для Windows, macOS и Linux: сравнение	967
Kaspersky Security Center Web Console.	974
О Kaspersky Security Center Web Console	975
Аппаратные и программные требования Kaspersky Security Center Web Console	976
Схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console	979
Порты, используемые приложением Kaspersky Security Center Web Console	980
Интерфейс Kaspersky Security Center Web Console	982
Закрепление и отмена закрепления разделов главного меню.....	983
Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985
Установка.....	987
Установка Kaspersky Security Center (Стандартная установка)	987
Установка Kaspersky Security Center Web Console	988

Установка Kaspersky Security Center Web Console, подключенной к Серверу администрирования, установленного на узлах отказоустойчивого кластера "Лаборатории Касперского"	991
Обновление Kaspersky Security Center Web Console	992
Сертификаты для работы с Kaspersky Security Center Web Console.....	993
Перенос данных из Kaspersky Security Center Windows.....	999
О переносе данных в Kaspersky Security Center Cloud Console	999
О переносе данных в приложение Kaspersky Security Center Linux	1000
Экспорт групповых объектов из Kaspersky Security Center Windows	1002
Импорт экспортного файла в Kaspersky Security Center Linux	1004
Переключение управляемых устройств под управление Kaspersky Security Center Linux	1005
Вход в приложение Kaspersky Security Center Web Console и выход из него	1006
Identity and Access Manager в Kaspersky Security Center Web Console.....	1008
О компоненте Identity and Access Manager	1008
Включение Identity and Access Manager: сценарий	1009
Настройка Identity and Access Manager в Kaspersky Security Center Web Console	1011
Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console	1011
Время жизни токенов и время ожидания авторизации для Identity and Access Manager	1013
Загрузка и распространение IAM-сертификатов	1014
Отключение Identity and Access Manager	1015
Настройка доменной аутентификации с использованием протоколов NTLM и Kerberos	1015
Настройка Сервера администрирования	1016
Настройка параметров подключения Kaspersky Security Center Web Console к Серверу администрирования.....	1017
Настройка журнала событий подключения к Серверу администрирования	1018
Настройка количества событий в хранилище событий.....	1018
Параметры подключения устройств с защитой на уровне UEFI	1019
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования.....	1020
Просмотр списка подчиненных Серверов администрирования.....	1022
Удаление иерархии Серверов администрирования.....	1023
Обслуживание Сервера администрирования	1023
Настройка интерфейса	1024
Управление виртуальными Серверами администрирования.....	1025
Включение защиты учетной записи от несанкционированного изменения	1031
Двухэтапная проверка.....	1031
Резервное копирование и восстановление данных Сервера администрирования	1042
Создание задачи резервного копирования данных.....	1043
Перенос Сервера администрирования на другое устройство	1044
Первоначальная настройка Kaspersky Security Center Web Console.....	1047
Мастер первоначальной настройки (Kaspersky Security Center Web Console)	1047

Подключение автономных устройств	1064
Мастер развертывания защиты.....	1076
Запуск мастера развертывания защиты.....	1077
Шаг 1. Выбор инсталляционного пакета.....	1077
Шаг 2. Выбор способа распространения файла ключа или кода активации	1078
Шаг 3. Выбор версии Агента администрирования.....	1078
Шаг 4. Выбор устройств	1078
Шаг 5. Задание параметров задачи удаленной установки	1079
Шаг 6. Управление перезагрузкой.....	1080
Шаг 7. Удаление несовместимых приложений перед установкой	1081
Шаг 8. Перемещение устройств в папку Управляемые устройства.....	1082
Шаг 9. Выбор учетных записей для доступа к устройствам	1082
Шаг 10. Запуск установки	1083
Развертывание приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console.....	1084
Сценарий: развертывание приложений "Лаборатории Касперского"	1084
Загрузка плагинов для приложений "Лаборатории Касперского"	1086
Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"	1087
Изменение ограничения на размер пользовательского инсталляционного пакета	1088
Загрузка дистрибутивов для приложений "Лаборатории Касперского"	1089
Проверка успешности развертывания Kaspersky Endpoint Security	1090
Создание автономного инсталляционного пакета	1090
Просмотр списка автономных инсталляционных пакетов	1092
Создание пользовательского инсталляционного пакета	1093
Распространение инсталляционных пакетов на подчиненные Серверы администрирования.....	1097
Установка приложений с помощью задачи удаленной установки	1098
Указание параметров удаленной установки на устройствах под управлением Unix.....	1106
Управление мобильными устройствами.	1107
Замещение приложений безопасности сторонних производителей	1108
Обнаружение устройств в сети.....	1109
Сценарий: обнаружение сетевых устройств	1109
Обнаружение устройств.....	1110
Приложения "Лаборатории Касперского": лицензирование и активация	1123
Лицензирование управляемых приложений	1124
Добавление лицензионного ключа в хранилище Сервера администрирования.	1126
Распространение лицензионного ключа на клиентские устройства	1127
Автоматическое распространение лицензионного ключа.	1129
Просмотр информации об используемых лицензионных ключах.....	1131
Удаление лицензионного ключа из хранилища	1132
Отзыв согласия с Лицензионным соглашением	1133
Продление срока действия лицензии приложений "Лаборатории Касперского"	1135

Использование Kaspersky Marketplace для выбора бизнес-решений	1136
Настройка защиты сети	1137
Сценарий: настройка защиты сети	1138
Подходы к управлению безопасностью, ориентированные на устройства и на пользователей ...	1139
Настройка и распространение политик: подход, ориентированный на устройства	1141
Настройка и распространение политик: подход, ориентированный на пользователя	1143
Параметры политики Агента администрирования	1145
Включение и выключение режима низкого потребления ресурсов для Агента администрирования	1160
Ручная настройка политики Kaspersky Endpoint Security	1161
Ручная настройка групповой задачи обновления Kaspersky Endpoint Security	1167
Предоставление автономного доступа к внешнему устройству, заблокированному компонентом Контроль устройств	1167
Удаленная деинсталляция приложений или обновлений программного обеспечения	1169
Задачи	1172
Управление клиентскими устройствами	1192
Политики и профили политик	1241
Шифрование и защита данных	1268
Пользователи и роли пользователей	1273
Работа с ревизиями объектов	1323
Удаление объектов	1325
Kaspersky Security Network и Kaspersky Private Security Network	1327
Сценарий: обновление Kaspersky Security Center и управляемых приложений безопасности	1333
Обновление баз и приложений "Лаборатории Касперского"	1335
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	1335
Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"	1340
Создание задачи Загрузка обновлений в хранилище Сервера администрирования	1347
Проверка полученных обновлений	1353
Создание задачи загрузки обновлений в хранилища точек распространения	1355
Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center	1360
Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows	1361
Одобрение и отклонение обновлений программного обеспечения	1363
Обновление Сервера администрирования	1364
Включение и выключение офлайн-модели получения обновлений	1364
Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах	1365
Резервное копирование и восстановление веб-плагинов	1366
Настройка точек распространения и шлюзов соединений	1367
Управление приложениями сторонних производителей на клиентских устройствах	1379
О приложениях сторонних производителей	1379
Установка обновлений приложений сторонних производителей	1383

Заккрытие уязвимостей в приложениях сторонних производителей	1416
Управление запуском приложений на клиентских устройствах	1441
Создание инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"	1459
Просмотр и изменение параметров инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"	1460
Параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"	1461
Теги приложений.....	1463
Мониторинг и отчеты	1466
Сценарий: мониторинг и отчеты.....	1466
О типах мониторинга и отчетах.....	1468
Панель мониторинга и веб-виджеты.....	1469
Отчеты	1474
События и выборки событий	1484
Уведомления и статусы устройств.....	1539
Объявления "Лаборатории Касперского"	1555
Просмотр информации об обнаруженных угрозах	1558
Cloud Discovery	1559
Журнал активности Kaspersky Security Center Web Console	1563
Интеграция Kaspersky Security Center с другими решениями	1564
Установка фонового соединения	1564
Экспорт событий в SIEM-системы.....	1565
Удаленная диагностика клиентских устройств	1580
Открытие окна удаленной диагностики	1581
Включение и выключение трассировки для приложений	1582
Загрузка файла трассировки приложения.....	1584
Удаление файлов трассировки	1585
Загрузка параметров приложений	1586
Загрузка журналов событий.....	1586
Запуск, остановка и перезапуск приложения	1586
Запуск удаленной диагностики Агента администрирования Kaspersky Security Center и скачивание результатов.....	1587
Запуск приложения на клиентском устройстве	1587
Создание файла дампа для приложения	1588
Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux	1589
Загрузка и удаление файлов из Карантина и Резервного хранилища	1590
Изменение языка интерфейса Kaspersky Security Center Web Console	1590

Приложение. Сертифицированное состояние приложения: параметры и их значения	1592
Проверка целостности модулей с помощью утилит klscmodchk и integrity_checker	1597
Настройка эталонных значений параметров приложения Kaspersky Security Center Web Console	1599
Справочное руководство API	1610
Руководство по масштабированию	1616
Обращение в Службу технической поддержки	1616
Способы получения технической поддержки	1616
Техническая поддержка через Kaspersky CompanyAccount	1617
Получение файлов дампа Сервера администрирования	1617
Источники информации о приложении	1618
Глоссарий	1619
Информация о стороннем коде	1632
Уведомления о товарных знаках	1633
Список ограничений	1635
Соответствие терминов	1637

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Security Center" (для Windows) (далее также "Kaspersky Security Center", "приложение").

Подготовительные процедуры изложены в разделах "Подготовка к установке", "Установка приложения", "Подготовка приложения к работе" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки приложения, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки приложения.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование приложения, а также инструкции и указания по безопасному использованию приложения.

В документе также содержатся разделы с дополнительной информацией о приложении.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Security Center, а также поддержка организаций, использующих Kaspersky Security Center.

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы приложения, а также указания по эксплуатации и требования к среде.

В этом разделе

Указания по эксплуатации и требования к среде	15
Аппаратные и программные требования.....	16

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление приложением должны осуществляться в соответствии с эксплуатационной документацией.
2. Приложение должно эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации приложения необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ приложения ко всем объектам информационной системы, которые необходимы приложению для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость приложения с контролируруемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы приложения со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлено приложение.
8. Должна быть обеспечена синхронизация по времени между компонентами приложения, а также между приложением и средой его функционирования.
9. Персонал, ответственный за функционирование приложения, должен обеспечивать надлежащее функционирование приложения, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между приложением и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование приложения должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности приложения.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности приложения.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным приложения, должно предоставляться только уполномоченным ролям (администраторам приложения и информационной системы).

15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

Аппаратные и программные требования

Требования к Серверу администрирования

Сервер администрирования

Минимальные аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 4 ГБ.
- Объем свободного места на диске: 10 ГБ. При использовании функциональности Системное администрирование объем свободного места на диске должен быть не менее 100 ГБ.

Для развертывания в облачных окружениях требования к Серверу администрирования и серверу базы данных такие же, как и к физическому Серверу администрирования (в зависимости от того, каким количеством устройств вы хотите управлять).

Программные требования:

- Microsoft Data Access Components (MDAC) 2.8.
- Microsoft Windows DAC 6.0.
- Microsoft Windows Installer 4.5.

Операционная система:

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSC) 64-разрядная.
- Windows Server 2019 Standard/Datacenter/Core 64-разрядная.
- Windows Server 2022 Standard/Datacenter/Core 64-разрядная.
- Windows Storage Server 2019 64-разрядная.

Сервер баз данных (может быть установлен на другой машине):

- Microsoft SQL Server 2016 (все редакции) 64-разрядная.
- Microsoft SQL Server 2017 (все редакции) для Windows/Linux 64-разрядная.
- Microsoft SQL Server 2019 (все редакции) для Windows/Linux 64-разрядная (требуется дополнительные действия).

- Microsoft SQL Server 2022 (все редакции) для Windows/Linux 64-разрядная.
- MySQL 5.7 Community 32-разрядная/64-разрядная.
- MySQL 8.0 Community 32-разрядная/64-разрядная.
- MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- PostgreSQL 13.x 64-разрядная.
- PostgreSQL 14.x 64-разрядная.
- PostgreSQL 15.x 64-разрядная.
- Postgres Pro 13.x Windows/Linux 64-разрядная.
- Postgres Pro 14.x Windows/Linux 64-разрядная.

Поддерживаются следующие платформы виртуализации:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- Parallels Desktop 18.
- Oracle VM VirtualBox 7.x.

Поддерживаются следующие SIEM-системы:

- HP (Micro Focus) ArcSight ESM 7.0.
- IBM QRadar 7.3.
- Splunk 7.1.

Требования к Web Console

Сервер Kaspersky Security Center Web Console

Минимальные аппаратные требования:

- Процессор: 4 ядра, частота от 2500 МГц.
- Оперативная память: 8 ГБ.
- Объем свободного места на диске: 40 ГБ.

Программные требования:

- Окружение Node.js 14.16.0.

Одна из следующих операционных систем:

- Microsoft Windows (только 64-разрядные версии):
 - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core.
 - Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSC).

- Windows Server 2019 Standard/Datacenter/Core.
- Windows Server 2022 Standard/Datacenter/Core.
- Windows Storage Server 2019.
- Платформы виртуализации:
 - VMware vSphere 6.7.
 - VMware vSphere 7.0.
 - Citrix XenServer 7.1 LTSR.
 - Citrix XenServer 8.x.
 - Parallels Desktop 18.
 - Oracle VM VirtualBox 7.x.

Клиентские устройства

Клиентскому устройству для работы с Kaspersky Security Center Web Console требуется только браузер.

Минимальное разрешение экрана составляет 1366x768 пикселей.

Требования к аппаратному и программному обеспечению устройства соответствуют требованиям браузера, который используется для работы с Kaspersky Security Center Web Console.

Браузер:

- Google Chrome 128.0.6613.120 и выше.
- Microsoft Edge 128.0.2739.67 и выше.
- Safari 17.6 для macOS.
- Яндекс Браузер 24.7.3.1081 и выше.
- Mozilla Firefox Extended Support Release 115.14.0 и выше.

Требования к серверам мобильных устройств

Сервер мобильных устройств iOS Mobile Device Management (iOS MDM)

Аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 2 ГБ.
- Объем свободного места на диске: 2 ГБ.

Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования).

Требования к Консоли администрирования

Аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Программные требования:

- Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования):
 - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64-разрядная.
 - Windows Server 2016 Standard/Datacenter/Essentials (LTSC) 64-разрядная.
 - Windows Server 2019 Standard/Datacenter 64-разрядная.
 - Windows Server 2022 Standard/Datacenter 64-разрядная.
 - Windows Storage Server 2019 64-разрядная.
- Microsoft Management Console 2.0.
- Microsoft Windows Installer 4.5.
- Microsoft Internet Explorer 11.0 работает на:
 - Microsoft Windows Server 2012 R2.
 - Microsoft Windows Server 2016.
 - Microsoft Windows Server 2019.
 - Microsoft Windows Storage Server 2019.
- Microsoft Edge, запущенный на Microsoft Windows Server 2022 Standard.

Требования к Агенту администрирования

Минимальные аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Требования к программному обеспечению для устройств с операционной системой Linux: должен быть установлен интерпретатор языка Perl версии 5.10 или выше.

Операционные
системы.
Microsoft
Windows

Windows Embedded POSReady 2009 с последним Service Pack 32-разрядная.
Windows Embedded 7 Standard Service Pack 1 32-разрядная/64-разрядная.
Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная.
Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная.
Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная.
Windows 10 IoT Enterprise 2015 LTSB 32-разрядная/64-разрядная.
Windows 10 IoT Enterprise 2016 LTSB 32-разрядная/64-разрядная.
Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная.
Windows 10 IoT Enterprise версия 1703 32-разрядная/64-разрядная.
Windows 10 IoT Enterprise версия 1709 32-разрядная/64-разрядная.
Windows 10 IoT Enterprise версия 1803 32-разрядная/64-разрядная.
Windows 10 IoT Enterprise версия 1809 32-разрядная/64-разрядная.
Windows 10 20H2 IoT Enterprise 32-разрядная/64-разрядная.
Windows 10 21H2 IoT Enterprise 32-разрядная/64-разрядная.
Windows 10 IoT Enterprise 32-разрядная/64-разрядная.
Windows 10 IoT Enterprise версия 1909 32-разрядная/64-разрядная.
Windows 10 IoT Enterprise LTSC 2021 32-разрядная/64-разрядная.
Windows 10 IoT Enterprise версия 1607 32-разрядная/64-разрядная.
Windows 10 TH1 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 TH2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 RS1 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 RS3 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 RS5 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 19H1 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 20H1 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 21H1 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.
Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.

Windows 10 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная.

Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная.

Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная.

Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная.

Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная.

Windows 8 Pro/Enterprise 32-разрядная/64-разрядная.

Windows 8.1 Pro/Enterprise 32-разрядная/64-разрядная.

Windows 7 Home/Pro/Enterprise/Ultimate Service Pack 1 32-разрядная/64-разрядная.

Windows XP Professional Service Pack 3 и выше 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20023).

Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20023).

Windows MultiPoint Server 2011 Standard/Premium 64-разрядная.

Windows Server 2008 Standard/Enterprise/Datacenter/Foundation Service Pack 2 32-разрядная/64-разрядная.

Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation/ Service Pack 1 и выше 64-разрядная.

Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.

Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.

Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSC) 64-разрядная.

Windows Server 2019 Standard/Datacenter/Core 64-разрядная.

Windows Server 2019 RS5 Standard/Essentials 64-разрядная.

Windows Server 2022 Standard/Datacenter/Core 64-разрядная.

Windows Server 2022 21H2 Standard/Datacenter 64-разрядная.

Windows Storage Server 2019 64-разрядная.

Операционные системы. Linux

Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная.
 Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная.
 Debian GNU/Linux 12 (Bookworm) 32-разрядная/64-разрядная.
 Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная.
 Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная.
 Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
 Ubuntu Server 22.04 LTS ARM 64-разрядная.
 Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная.
 CentOS 6.7 and later 32-разрядная.
 CentOS 6.x (до 6.6) 32-разрядная/64-разрядная.
 CentOS 7.x 64-разрядная.
 CentOS Stream 8 64-разрядная.
 CentOS Stream 9 64-разрядная.
 CentOS Stream 9 ARM 64-разрядная.
 Red Hat Enterprise Linux Server 6.x 32-разрядная/64-разрядная.
 Red Hat Enterprise Linux Server 7.x 64-разрядная.
 Red Hat Enterprise Linux Server 8.x 64-разрядная.
 Red Hat Enterprise Linux Server 9.x 64-разрядная.
 SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная.
 SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
 SUSE Linux Enterprise Server 15 (все пакеты обновлений) ARM 64-разрядная.
 openSUSE 15 64-разрядная.
 EulerOS 2.0 SP10 64-разрядная.
 EulerOS 2.0 SP10 ARM 64-разрядная.
 Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5) 64-разрядная.
 Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
 Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная.
 Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная.
 Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7) ARM 64-разрядная.
 Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
 Альт Рабочая станция 10.1 64-разрядная.
 Альт Сервер 10.1 64-разрядная.
 ALT Education 10.1 64-разрядная.
 Альт СП Сервер 10 32-разрядная/64-разрядная.
 Альт СП Сервер 10 ARM 64-разрядная.
 Альт СП Рабочая станция 10 32-разрядная/64-разрядная.
 Альт СП Рабочая станция 10 ARM 64-разрядная.
 Альт Сервер 10 64-разрядная.
 Альт Сервер 10 ARM 64-разрядная.
 Альт Рабочая станция 10 32-разрядная/64-разрядная.
 Альт 8 СП Рабочая станция (8.4) ARM 64-разрядная.
 Альт 8 СП Сервер (8.4) ARM 64-разрядная.

Альт 8 СП Сервер (ЛКНВ.11100-01) 32-разрядная/64-разрядная.
 Альт 8 СП Рабочая станция (ЛКНВ.11100-01) 32-разрядная/64-разрядная.
 Mageia 4 32-разрядная.
 Oracle Linux 7 64-разрядная.
 Oracle Linux 8 64-разрядная.
 Oracle Linux 9 64-разрядная.
 Linux Mint 20.x 64-разрядная.
 Linux Mint 21.1 и выше 64-разрядная.
 AlterOS 7.5 или выше 64-разрядная.
 ГосЛинукс IC6/7.17 64-разрядная.
 ГосЛинукс IC6/7.2 64-разрядная.
 SberOS 3.2.0 64-разрядная.
 Platform V SberLinux OS Server (SLO) 8.8 64-разрядная.
 Platform V SberLinux OS Server (SLO) 8.9.2 64-разрядная.
 РЕД ОС 7.3 ARM 64-разрядная.
 РЕД ОС 7.3 Сервер 64-разрядная.
 РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
 РЕД ОС 8 Сертифицированная редакция 64-разрядная.
 ROSA Enterprise Linux Server 7.9 64-разрядная.
 ROSA Enterprise Linux Desktop 7.9 64-разрядная.
 РОСА "КОБАЛЬТ" 7.9 64-разрядная.
 РОСА "ХРОМ" 12 64-разрядная.
 AlmaLinux 8 и выше 64-разрядная.
 AlmaLinux 9 и выше 64-разрядная.
 Rocky Linux 8 и выше 64-разрядная.
 Rocky Linux 9 и выше 64-разрядная.
 Атлант, сборка Alcyone, версия 2022.02 64-разрядная.
 МСВСфера 9.2 Сервер 64-разрядная.
 МСВСфера 9.2 АРМ 64-разрядная.
 СинтезМ Сервер 8.6 64-разрядная.
 СинтезМ Клиент 8.6 64-разрядная.
 ОСнова 2.10 64-разрядная.
 Kylin 10 64-разрядная.
 EMIAS 1.0 64-разрядная.
 Amazon Linux 2 64-разрядная.
 МосОС 15.4 Arbat 64-разрядная.
 М ОС (Moscow Electronic School) 64-разрядная.
 macOS Monterey (12.x).
 macOS Ventura 13.x.
 macOS Sonoma (14.x).

Операционные
системы. macOS

Для Агента администрирования поддерживается архитектура Apple Silicon (M1), также, как и Intel.
Поддерживаются следующие платформы виртуализации:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- Parallels Desktop 18.
- Oracle VM VirtualBox 7.x.
- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- Kernel-based Virtual Machine (все операционные системы Linux, поддерживаемые Агентом администрирования).

На устройствах под управлением Windows 10 версии RS4 или RS5 Kaspersky Security Center может не обнаруживать некоторые уязвимости в папках, в которых включен учет регистра.

Перед установкой Агента администрирования на устройства под управлением Windows 7, Windows Server 2008 или Windows Server 2008 R2 убедитесь, что вы установили обновление безопасности KB3063858 для ОС Windows (Обновление безопасности для Windows 7 (KB3063858) <https://www.microsoft.com/en-us/download/details.aspx?id=47409>, Обновление безопасности для Windows 7 для систем на базе x64 (KB3063858) (<https://www.microsoft.com/en-us/download/details.aspx?id=47442>), Обновление безопасности для Windows Server 2008 (KB3063858) <https://www.microsoft.com/en-us/download/details.aspx?id=47411>, Обновление безопасности для Windows Server 2008 x64 Edition (KB3063858) <https://www.microsoft.com/en-us/download/details.aspx?id=47414>, Обновление безопасности для Windows Server 2008 R2 x64 Edition (KB3063858) <https://www.microsoft.com/en-us/download/details.aspx?id=47479>).

В Microsoft Windows XP Агент администрирования может не выполнять некоторые операции правильно (см. раздел "Развертывание Агента администрирования и приложения безопасности" на стр. 163). Вы можете установить или обновить Агент администрирования для Windows XP только в Microsoft Windows XP. Поддерживаемые редакции Microsoft Windows XP и соответствующие им версии Агента администрирования указаны в списке поддерживаемых операционных систем. Вы можете скачать необходимую версию Агента администрирования для Microsoft Windows XP с этой страницы <https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint>. Рекомендуется устанавливать ту же версию Агента администрирования, что и Kaspersky Security Center. Kaspersky Security Center полностью поддерживает Агент администрирования той же или выше. Агент администрирования для macOS поставляется вместе с приложением безопасности "Лаборатории Касперского" для этой операционной системы.

Совместимые приложения и решения "Лаборатории Касперского"

Kaspersky Security Center поддерживает централизованное развертывание и управление всеми поддерживаемыми на данный момент приложениями и решениями "Лаборатории Касперского". В таблице ниже показано, какие приложения и решения "Лаборатории Касперского" поддерживаются Консолью администрирования на основе MMC и Kaspersky Security Center Web Console. Подробнее о версиях программ и решений см. на странице "Жизненный цикл программ"

<https://support.kaspersky.com/corporate/lifecycle>.

Таблица 1. Список приложений "Лаборатории Касперского" и решений поддерживаемых приложением Kaspersky Security Center

Название приложения "Лаборатории Касперского" или решения	Поддерживается Консоль администрирования на основе MMC	Поддерживается Kaspersky Security Center Web Console
Для рабочих станций		
Kaspersky Endpoint Security для Windows	✓	✓
Kaspersky Endpoint Security для Linux	✓	✓
Kaspersky Endpoint Security для Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security для Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security для Windows	✓	✓
Kaspersky Embedded Systems Security для Linux	—	✓
Для промышленных решений		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (централизованное развертывание не поддерживается)	✓	✓

Название приложения "Лаборатории Касперского" или решения	Поддерживается Консоль администрирования на основе MMC	Поддерживается Kaspersky Security Center Web Console
Для мобильных устройств		
Kaspersky Endpoint Security для Android	✓	✓
Kaspersky Security для iOS	—	✓
Для файловых серверов:		
Kaspersky Security для Windows Server	✓	✓
Kaspersky Endpoint Security для Windows	✓	✓
Kaspersky Endpoint Security для Linux	✓	✓
Для виртуальных сред		
Kaspersky Security для виртуальных сред Легкий агент	✓	✓
Kaspersky Security для виртуальных сред Защита без агента	✓	—
Для почтовых систем серверов совместной работы		
Kaspersky Security для Microsoft Exchange Servers	✓	—
Для обнаружения целевых атак		
Kaspersky Sandbox Server	—	✓
Kaspersky Endpoint Detection and Response Optimum	—	✓
Kaspersky Managed Detection and Response	—	✓
Для устройств с операционной системой KasperskyOS		
Kaspersky IoT Secure Gateway	—	✓
KasperskyOS for Thin Client	—	✓
Репутационные базы данных		
Kaspersky Private Security Network	—	✓

См. также:

Основной сценарий установки 56

Kaspersky Security Center

В этом руководстве представлена информация о Kaspersky Security Center.

Информация в справке может отличаться от информации в документах, входящих в состав комплекта документов к приложению. В этом случае актуальной считается информация в справке. Перейти в справку можно по ссылкам, встроенным в интерфейс приложения, или по ссылке из документации. Справка может обновляться без уведомления. При необходимости вы можете переключаться между онлайн-справкой и офлайн-справкой (см. раздел "Переключение между онлайн-справкой и офлайн-справкой" на стр. [878](#)).

В этом разделе

О Kaspersky Security Center	28
Основные понятия	39
Архитектура приложения	56
Основной сценарий установки	56
Порты, используемые Kaspersky Security Center	63
Сертификаты для работы с Kaspersky Security Center	71
Схемы трафика данных и использования портов	87
Лучшие практики развертывания	116
Установка Kaspersky Security Center	206
Об обновлении предыдущей версии Kaspersky Security Center	275
Первоначальная настройка Kaspersky Security Center	280
Обнаружение устройств в сети	322
Лицензирование	340
Приложения "Лаборатории Касперского". Централизованное развертывание	357
Приложения "Лаборатории Касперского": лицензирование и активация	388
Настройка защиты сети	401
Обновление Kaspersky Security Center и управляемых приложений	455
Управление приложениями сторонних производителей на клиентских устройствах	498
Мониторинг и отчеты	592
Настройка точек распространения и шлюзов соединений	685
Другие повседневные задачи	699
Экспорт событий в SIEM-системы	879
Использование SNMP для отправки статистики приложениям сторонних производителей	900
Приложения	913

О Kaspersky Security Center

В этом разделе представлена информация о назначении, ключевых возможностях и компонентах приложения Kaspersky Security Center, а также способы приобретения Kaspersky Security Center.

Информация в справке может отличаться от информации в документах, входящих в состав комплекта документов к приложению. В этом случае актуальной считается информация в справке. Перейти в справку можно по ссылкам, встроенным в интерфейс приложения, или по ссылке из документации. Справка может обновляться без уведомления. При необходимости вы можете переключаться между онлайн-справкой и офлайн-справкой (см. раздел "Переключение между онлайн-справкой и офлайн-справкой" на стр. [878](#)).

Приложение Kaspersky Security Center предназначено для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Приложение предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе приложений "Лаборатории Касперского".

Приложение Kaspersky Security Center адресовано администраторам сетей организаций и сотрудникам, отвечающим за защиту устройств в организациях.

При помощи Kaspersky Security Center вы можете:

- Формировать иерархию Серверов администрирования для управления сетью собственной организации, а также сетями удаленных офисов или организаций-клиентов.
Под *организациями-клиентами* здесь подразумеваются организации, антивирусную защиту которых обеспечивает поставщик услуг.
- Формировать иерархию групп администрирования для управления набором клиентских устройств как единым целым.
- Управлять системой антивирусной безопасности, построенной на основе приложений "Лаборатории Касперского".
- Централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку приложений "Лаборатории Касперского" и других производителей программного обеспечения.
- Удаленно управлять приложениями "Лаборатории Касперского" и других производителей, установленными на клиентских устройствах: устанавливать обновления, искать и закрывать уязвимости.
- Централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.
- Получать статистику и отчеты о работе приложений и устройств.
- Получать уведомления о критических событиях в работе приложений "Лаборатории Касперского".
- Управлять мобильными устройствами.
- Управлять шифрованием информации, хранящейся на жестких дисках устройств и съемных дисках, и доступом пользователей к зашифрованным данным.
- Проводить инвентаризацию оборудования, подключенного к сети организации.

- Централизованно работать с файлами, помещенными приложениями безопасности на карантин или в резервное хранилище, а также с файлами, обработка которых отложена приложениями безопасности.

Вы можете приобрести Kaspersky Security Center через "Лабораторию Касперского" (например, на сайте <https://www.kaspersky.ru>) или через компании-партнеров.

Если вы покупаете Kaspersky Security Center через "Лабораторию Касперского", вы можете скачать приложение с нашего сайта. Информация, необходимая для активации приложения, высылается вам по электронной почте после оплаты.

Updates functionality (including providing anti-virus signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

В этом разделе

Аппаратные и программные требования.....	29
Совместимые приложения и решения "Лаборатории Касперского"	29
Лицензии и возможности Kaspersky Security Center	29
О совместимости компонентов Kaspersky Security Center	33
Сравнение версий Kaspersky Security Center: на базе Windows и на базе Linux.....	35

Лицензии и возможности Kaspersky Security Center

Kaspersky Security Center требует лицензии на некоторые его функции.

В таблице ниже показано, какая лицензия охватывает какие функции Kaspersky Security Center.

Чтобы использовать функции Kaspersky Security Center, необходимо активировать Сервер администрирования, добавив лицензионный ключ Сервера администрирования.

Необходимо вручную добавить лицензионный ключ для каждого Сервера администрирования.

Таблица 2. Лицензии и возможности Kaspersky Security Center

Функции Kaspersky Security Center	Системное администрирование https://www.kaspersky.com/small-to-medium-business-security/systems-management	Kaspersky Endpoint Security для бизнеса Стандартный https://www.kaspersky.com/small-to-medium-business-security/endpoint-select	Kaspersky Endpoint Security для бизнеса Расширенный https://www.kaspersky.com/small-to-medium-business-security/endpoint-advanced	Kaspersky Total Security для бизнеса https://www.kaspersky.com/small-to-medium-business-security/total	Kaspersky Hybrid Cloud Security Standard https://www.kaspersky.com/enterprise-security/cloud-security	Kaspersky Hybrid Cloud Security Enterprise https://www.kaspersky.com/enterprise-security/cloud-security	Kaspersky EDR Optimum https://www.kaspersky.com/enterprise-security/edr-security-software-solution
Поиск уязвимости (см. стр. 498)	✓	✓	✓	✓	✓	✓	✓
Управление патчами (см. раздел "Установка обновлений приложений сторонних производителей" на стр. 498)	✓	—	✓	✓	—	✓	✓
Управление доступом на основе ролей (см. раздел "Настройка прав. Пользовательские роли" на стр. 809)	✓	✓	✓	✓	✓	✓	✓

Функции Kaspersky Security Center	Системное администрирование https://www.kaspersky.com/small-to-medium-business-security/systems-management	Kaspersky Endpoint Security для бизнеса Стандартный https://www.kaspersky.com/small-to-medium-business-security/endpoint-select	Kaspersky Endpoint Security для бизнеса Расширенный https://www.kaspersky.com/small-to-medium-business-security/endpoint-advanced	Kaspersky Total Security для бизнеса https://www.kaspersky.com/small-to-medium-business-security/total	Kaspersky Hybrid Cloud Security Standard https://www.kaspersky.com/enterprise-security/cloud-security	Kaspersky Hybrid Cloud Security Enterprise https://www.kaspersky.com/enterprise-security/cloud-security	Kaspersky EDR Optimum https://www.kaspersky.com/enterprise-security/edr-security-software-solution
Установка операционных систем и приложений (см. стр. 843)	✓	—	✓	✓	—	✓	✓
Управление мобильными устройствами (то есть управление iOS- и Android-устройствами пользователей)	✓	✓	✓	✓	—	—	✓

Функции Kaspersky Security Center	Системное администрирование https://www.kaspersky.com/small-to-medium-business-security/systems-management	Kaspersky Endpoint Security для бизнеса Стандартный https://www.kaspersky.com/small-to-medium-business-security/endpoint-select	Kaspersky Endpoint Security для бизнеса Расширенный https://www.kaspersky.com/small-to-medium-business-security/endpoint-advanced	Kaspersky Total Security для бизнеса https://www.kaspersky.com/small-to-medium-business-security/total	Kaspersky Hybrid Cloud Security Standard https://www.kaspersky.com/enterprise-security/cloud-security	Kaspersky Hybrid Cloud Security Enterprise https://www.kaspersky.com/enterprise-security/cloud-security	Kaspersky EDR Optimum https://www.kaspersky.com/enterprise-security/edr-security-software-solution
Настройка облачного окружения для работы в облачных окружениях, таких как AWS, Microsoft Azure или Google Cloud	—	—	—	—	✓	✓	—
Экспорт событий в SIEM-системы: Syslog (см. раздел "Об экспорте событий в формате Syslog" см. стр. 891)	✓	✓	✓	✓	✓	✓	✓

Функции Kaspersky Security Center	Системное администрирование https://www.kaspersky.com/small-to-medium-business-security/systems-management	Kaspersky Endpoint Security для бизнеса Стандартный https://www.kaspersky.com/small-to-medium-business-security/endpoint-select	Kaspersky Endpoint Security для бизнеса Расширенный https://www.kaspersky.com/small-to-medium-business-security/endpoint-advanced	Kaspersky Total Security для бизнеса https://www.kaspersky.com/small-to-medium-business-security/total	Kaspersky Hybrid Cloud Security Standard https://www.kaspersky.com/enterprise-security/cloud-security	Kaspersky Hybrid Cloud Security Enterprise https://www.kaspersky.com/enterprise-security/cloud-security	Kaspersky EDR Optimum https://www.kaspersky.com/enterprise-security/edr-security-software-solution
Экспорт событий в SIEM-системы: QRadar by IBM и ArcSight от Micro Focus (см. раздел "Об экспорте событий в форматах CEF и LEEF" см. стр. 891)	✓	—	✓	✓	—	✓	✓

См. также:

Особенности лицензирования Kaspersky Security Center и управляемых приложений.....	355
Приложения "Лаборатории Касперского": лицензирование и активация	388
Настройка интерфейса	320

О совместимости компонентов Kaspersky Security Center

В таблице ниже вы можете найти информацию о совместимости компонентов Kaspersky Security Center.

Таблица 3. Совместимость компонентов Kaspersky Security Center

Компонент	Совместим с
Главный Сервер администрирования Kaspersky Security Center 15.1	- Консоль администрирования Kaspersky Security Center 15.1 - Kaspersky Security Center 15.1 Web Console. Рекомендуется использовать последние версии Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console. В противном случае функциональность Kaspersky Security Center может быть ограничена. Вы можете установить и обновить Сервер администрирования Kaspersky Security Center и Kaspersky Security Center Web Console независимо друг от друга. В этом случае убедитесь, что версия установленного приложения Kaspersky Security Center Web Console совместима с версией Сервера администрирования, к которому вы подключаетесь: - Агент администрирования Kaspersky Security Center версий: 15.1, 15, 14.2, 14.
Kaspersky Security Center 15.1 Web Console.	Сервер администрирования Kaspersky Security Center версий: 15.1 и 14.2. Рекомендуется использовать последние версии Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console. В противном случае функциональность Kaspersky Security Center может быть ограничена. Вы можете установить и обновить Сервер администрирования Kaspersky Security Center и Kaspersky Security Center Web Console независимо друг от друга. В этом случае убедитесь, что версия установленного приложения Kaspersky Security Center Web Console совместима с версией Сервера администрирования, к которому вы подключаетесь:
Главный Сервер администрирования Kaspersky Security Center 15.1.	Подчиненные Серверы администрирования: - Kaspersky Security Center 14 Windows. - Kaspersky Security Center 14.2 Windows. - Kaspersky Security Center 15.1 Windows. - Kaspersky Security Center 14.2 Linux. - Kaspersky Security Center 15 Linux. - Kaspersky Security Center 15.1 Linux.

Сравнение версий Kaspersky Security Center: на базе Windows и на базе Linux

"Лаборатории Касперского" предлагает приложение Kaspersky Security Center в качестве локального решения для двух платформ – Windows и Linux. В решении для Windows вы устанавливаете Сервер администрирования на устройство с операционной системой Windows. Решение на базе Linux имеет версию Сервера администрирования, предназначенную для установки на устройство с операционной системой Linux. Эта справка содержит информацию о Kaspersky Security Center Windows. Для получения подробной информации о решении на базе Linux см. онлайн-справку Kaspersky Security Center Linux <https://support.kaspersky.com/KSCLinux/14.2/en-US/5022.htm>.

Таблица ниже позволяет сравнить основные возможности Kaspersky Security Center как решения на базе Windows и как решения на базе Linux.

Таблица 4. Сравнение возможностей приложения Kaspersky Security Center на базе Windows и на базе Linux

Функция или свойство	Kaspersky Security Center 15.1	
	Решение на базе Windows	Решение на базе Linux
Расположение Сервера администрирования	В локальной инфраструктуре	В локальной инфраструктуре
Расположение системы управления базами данных (СУБД)	В локальной инфраструктуре	В локальной инфраструктуре
Операционная система для установки Сервера администрирования	Windows	Linux
Тип Консоли администрирования	Локальная и веб-интерфейс	Веб-интерфейс
Операционная система для установки Консоли администрирования с веб-интерфейсом	Windows или Linux	Linux
Иерархия Серверов администрирования	✓	✓
Иерархия групп администрирования	✓	✓
Опрос сети	✓	✓ (по IP-диапазонам, контроллерам доменов, Samba 4 Active Directory, Microsoft Active Directory)
Максимальное количество управляемых устройств	100 000	20 000

Функция или свойство	Kaspersky Security Center 15.1	
	Решение на базе Windows	Решение на базе Linux
Защита устройств под управлением Windows, macOS и Linux	✓	✓ (защита устройств только с операционными системами Linux и Windows)
Защита мобильных устройств	✓	—
Защита виртуальных машин	✓	—
Защита публичной облачной инфраструктуры	✓	—
Управление безопасностью устройств	✓	✓
Управление безопасностью, ориентированной на пользователя	✓	✓
Политики приложений	✓	✓
Задачи для приложений "Лаборатории Касперского"	✓	✓
Kaspersky Security Network	✓	✓
Прокси-сервер KSN	✓	✓
Kaspersky Private Security Network	✓	✓
Централизованное распространение лицензионных ключей приложений "Лаборатории Касперского"	✓	✓
Автоматическое обновление антивирусных баз	✓	✓
Поддержка виртуальных Серверов администрирования	✓	✓
Установка обновлений приложений сторонних производителей и поиск уязвимостей в приложениях сторонних производителей	✓	— (только с помощью задачи удаленной установки)

Функция или свойство	Kaspersky Security Center 15.1	
	Решение на базе Windows	Решение на базе Linux
Уведомления о событиях, произошедших на управляемых устройствах	✓	✓
Создание учетных записей пользователей, контроль учетных записей	✓	✓
Вход в консоль с использованием доменной аутентификации	✓	✓ (единый вход (SSO) временно не поддерживается)
Интеграция с SIEM-системами	✓	✓ (только с использованием Syslog)
Мониторинг состояния политик и задач	✓	✓
Развертывание отказоустойчивого кластера Kaspersky Security Center	✓	✓
Установка Сервера администрирования на отказоустойчивом кластере Windows Server	✓	—
Использование SNMP для отправки статистики Сервера администрирования приложениям сторонних производителей	✓	—
Удаленная диагностика клиентских устройств	✓	✓
Удаленное подключение к рабочему столу клиентского устройства	✓	—
Работа с ревизиями объектов	✓	—
Автоматическое обновление приложений "Лаборатории Касперского"	✓	—
Развертывание операционных систем на клиентских устройствах	✓	—

Функция или свойство	Kaspersky Security Center 15.1	
	Решение на базе Windows	Решение на базе Linux
Веб-сервер для публикации инсталляционных пакетов и других файлов	✓	—
Просмотр и работа с алертами, зарегистрированными Kaspersky Endpoint Detection and Response Optimum	✓	—
Использовать Сервер администрирования в роли WSUS-сервера	✓	—
Интеграция с Kaspersky Managed Detection and Response	✓	—
Поддержка Адаптивного контроля аномалий	✓	—
Поддержка кластеров и массивов серверов в группах администрирования	✓	✓
Управление сторонними лицензиями	✓	—

Основные понятия

Этот раздел содержит развернутые определения основных понятий, относящихся к приложению Kaspersky Security Center.

В этом разделе

Сервер администрирования	39
Удаление иерархии Серверов администрирования	41
Виртуальный Сервер администрирования	41
Сервер мобильных устройств	42
Веб-сервер	43
Агент администрирования	43
Группы администрирования	44
Управляемое устройство	45
Нераспределенное устройство	45
Рабочее место администратора	45
Плагин управления	46
Веб-плагин управления	46
Политики	47
Профили политик	48
Задачи	48
Область действия задачи	50
Взаимосвязь политики и локальных параметров приложения	51
Точка распространения	51
Шлюз соединения	54

Сервер администрирования

Компоненты Kaspersky Security Center позволяют осуществлять удаленное управление приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

Устройства, на которых установлен компонент Сервер администрирования, называются *Серверами администрирования* (далее также *Серверами*). Серверы администрирования должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Сервер администрирования устанавливается на устройство в качестве службы со следующим набором атрибутов:

- под именем "Сервер администрирования Kaspersky Security Center";

- с автоматическим типом запуска при старте операционной системы;
- с учетной записью **LocalSystem** либо учетной записью пользователя в соответствии с выбором, сделанным при установке Сервера администрирования.

Сервер администрирования выполняет следующие функции:

- хранение структуры групп администрирования;
- хранение информации о конфигурации клиентских устройств;
- организация хранилищ дистрибутивов приложений;
- удаленная установка приложений на клиентские устройства и удаление приложений;
- обновление баз и модулей приложений "Лаборатории Касперского";
- управление политиками и задачами на клиентских устройствах;
- хранение информации о событиях, произошедших на клиентских устройствах;
- формирование отчетов о работе приложений "Лаборатории Касперского";
- распространение лицензионных ключей на клиентские устройства, хранение информации о ключах;
- отправка уведомлений о ходе выполнения задач (например, об обнаружении вирусов на клиентском устройстве).

Правило именования Серверов администрирования в интерфейсе приложения

В интерфейсе Консоли администрирования и Kaspersky Security Center Web Console Серверы администрирования могут иметь следующие имена:

- Имя устройства Сервера администрирования, например: "*имя_устройства*" или "Сервер администрирования: *имя_устройства*".
- IP-адрес устройства Сервера администрирования, например: "*IP_адрес*" или "Сервер администрирования: *IP_адрес*".
- Подчиненные Серверы администрирования и виртуальные Серверы администрирования имеют собственные имена, которые вы указываете при подключении виртуального или подчиненного Сервера администрирования к главному Серверу администрирования.
- Если вы используете приложение Kaspersky Security Center Web Console, установленное на устройство под управлением Linux, то приложение отображает имена Серверов администрирования, которые вы указали как доверенные в файле ответов.

Вы можете подключиться к Серверу администрирования с помощью Консоли администрирования (см. раздел "Сервер администрирования и Консоль администрирования" на стр. [107](#)) или с помощью Kaspersky Security Center Web Console.

См. также:

Основной сценарий установки.....	56
Установка Kaspersky Security Center.....	206
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104

Удаление иерархии Серверов администрирования

Серверы администрирования могут образовывать иерархию. Каждый Сервер администрирования может иметь несколько подчиненных Серверов администрирования (далее также *подчиненных Серверов*) на разных уровнях иерархии. Уровень вложенности подчиненных Серверов не ограничен. При этом в состав групп администрирования главного Сервера будут входить клиентские устройства всех подчиненных Серверов. Таким образом, независимые участки компьютерной сети могут управляться различными Серверами администрирования, которые, в свою очередь, управляются главным Сервером.

Частным случаем подчиненных Серверов администрирования являются *виртуальные Серверы администрирования* (см. раздел "*Виртуальный Сервер администрирования*" на стр. [41](#)).

Иерархию Серверов администрирования можно использовать для следующих целей:

- Ограничение нагрузки на Сервер администрирования (по сравнению с одним установленным в сети Сервером).
- Сокращение трафика внутри сети и упрощение работы с удаленными офисами. Нет необходимости устанавливать соединение между главным Сервером и всеми устройствами сети, которые могут находиться, например, в других регионах. Достаточно установить на каждом участке сети подчиненный Сервер администрирования, распределить устройства в группах администрирования подчиненных Серверов и обеспечить подчиненным Серверам соединение с главным Сервером по быстрым каналам связи.
- Разделение ответственности между администраторами антивирусной безопасности. При этом сохраняются все возможности централизованного управления и мониторинга состояния антивирусной безопасности сети организации.

Каждое устройство, включенное в иерархию групп администрирования, может быть подключено только к одному Серверу администрирования. Вам нужно самостоятельно проверять подключение устройств к Серверам администрирования. Для этого можно использовать функцию поиска устройств по сетевым атрибутам в группах администрирования различных Серверов.

См. также:

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования[111](#)

Виртуальный Сервер администрирования

Виртуальный Сервер администрирования (далее также *виртуальный Сервер*) – компонент приложения Kaspersky Security Center, предназначенный для управления сетью организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.

- Виртуальный Сервер администрирования при работе использует основную базу данных главного Сервера администрирования. Задачи резервного копирования и восстановления данных, а также задачи проверки и загрузки обновлений, не поддерживаются на виртуальном Сервере администрирования.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Кроме того, виртуальный Сервер администрирования имеет следующие ограничения:

- В окне свойств виртуального Сервера ограничен набор разделов.
- Для удаленной установки приложений "Лаборатории Касперского" на клиентские устройства, работающие под управлением виртуального Сервера, необходимо, чтобы на одном из клиентских устройств был установлен Агент администрирования для связи с виртуальным Сервером. При первом подключении к виртуальному Серверу администрирования это устройство автоматически назначается точкой распространения и выполняет роль шлюза соединений клиентских устройств с виртуальным Сервером администрирования.
- Виртуальный Сервер администрирования может опрашивать сеть только через точки распространения.
- Чтобы перезапустить виртуальный Сервер, работоспособность которого была нарушена, Kaspersky Security Center перезапускает главный Сервер администрирования и все виртуальные Серверы.
- Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Администратор виртуального Сервера обладает всеми правами в рамках этого виртуального Сервера.

Сервер мобильных устройств

Сервер мобильных устройств – это компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.

Kaspersky Security Center включает Сервер iOS MDM в качестве Сервера мобильных устройств. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими сервис Apple Push Notifications (APNs).

Серверы мобильных устройств Kaspersky Security Center позволяют управлять следующими объектами:

- Отдельным мобильным устройством.
- Несколькими мобильными устройствами.
- Несколькими мобильными устройствами, подключенными к кластеру серверов, одновременно. При подключении к кластеру серверов Сервер мобильных устройств, установленный на этом кластере, отображается в Консоли администрирования как один сервер.

Веб-сервер

Веб-сервер Kaspersky Security Center (далее также *Веб-сервер*) – это компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных инсталляционных пакетов, iOS MDM-профилей, а также файлов из папки общего доступа.

При создании автономный инсталляционный пакет автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных инсталляционных пакетов. При необходимости вы можете отменить публикацию автономного пакета или повторно опубликовать его на Веб-сервере.

При создании iOS MDM-профиль для мобильного устройства пользователя также автоматически публикуется на Веб-сервере. Опубликованный профиль автоматически удаляется с Веб-сервера после успешной установки на мобильное устройство пользователя.

Папка общего доступа используется для размещения информации, доступной всем пользователям, устройства которых находятся под управлением Сервера администрирования. Если у пользователя нет прямого доступа к папке общего доступа, ему можно передать информацию из этой папки с помощью Веб-сервера.

Для передачи пользователям информации из папки общего доступа с помощью Веб-сервера администратору требуется создать в папке общего доступа вложенную папку `public` и поместить в нее информацию.

Синтаксис ссылки для передачи информации пользователю выглядит следующим образом:

```
https://<имя Веб-сервера>:<порт HTTPS>/public/<объект>
```

где

- `<имя Веб-сервера>` – имя Веб-сервера Kaspersky Security Center.
- `<порт HTTPS>` – HTTPS-порт Веб-сервера, заданный администратором. HTTPS-порт можно задать в разделе **Веб-сервер** окна свойств Сервера администрирования. По умолчанию установлен порт 8061.
- `<объект>` – вложенная папка или файл, доступ к которым требуется открыть для пользователя.

Администратор может передать сформированную ссылку пользователю любым удобным способом, например, по электронной почте.

По полученной ссылке пользователь может загрузить на локальное устройство предназначенную для него информацию.

Агент администрирования

Взаимодействие между Сервером администрирования и устройствами обеспечивается *Агентом администрирования* – компонентом Kaspersky Security Center. Агент администрирования требуется установить на все устройства, на которых управление работой приложений "Лаборатории Касперского" выполняется с помощью Kaspersky Security Center.

Агент администрирования устанавливается на устройстве в качестве службы со следующим набором атрибутов:

- под именем "Агент администрирования Kaspersky Security Center";

- с автоматическим типом запуска при старте операционной системы;
- с помощью учетной записи LocalSystem.

Устройство, на которое установлен Агент администрирования, называется *управляемым устройством* или *устройством*.

Агент администрирования можно установить на устройство под управлением операционной системы Windows, Linux или Mac. Вы можете активировать компонент следующими способами:

- Инсталляционный пакет в хранилище Сервера администрирования (необходимо, чтобы был установлен Сервер администрирования).
- Инсталляционный пакет находится на веб-серверах "Лаборатории Касперского" (см. раздел "Работа с плагинами управления" см. стр. [368](#)).

Нет необходимости устанавливать Агент администрирования на устройства, на которых установлен Сервер администрирования, поскольку серверная версия Агента администрирования устанавливается автоматически совместно с Сервером администрирования.

Название процесса, который запускает Агент администрирования, – *klagent.exe*.

Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (*периодический сигнал*) равным 15 минут на 10 000 управляемых устройств.

См. также:

Параметры политики Агента администрирования.....	789
Развертывание Агента администрирования и приложения безопасности	163

Группы администрирования

Группа администрирования (далее также *группа*) – это набор управляемых устройств, объединенных по какому-либо признаку с целью управления устройствами группы как единым целым Kaspersky Security Center.

Для всех управляемых устройств в группе администрирования устанавливаются:

- Единые параметры работы приложений – с помощью групповых политик.
- Единый режим работы всех приложений – с помощью создания групповых задач с определенным набором параметров. Примеры групповых задач включают создание и установку общего инсталляционного пакета, обновление баз и модулей приложений, проверку устройства по требованию и включение постоянной защиты.

Управляемое устройство может входить в состав только одной группы администрирования.

Для Серверов администрирования и групп администрирования можно создавать иерархии с любым уровнем вложенности. На одном уровне иерархии могут располагаться подчиненные и виртуальные Серверы администрирования, группы и управляемые устройства. Можно переводить устройства из одной группы в другую, не перемещая их физически. Например, если сотрудник предприятия перешел с позиции бухгалтера на позицию разработчика, вы можете перевести компьютер этого сотрудника из группы администрирования "Бухгалтеры" в группу администрирования "Разработчики". Таким образом, устройство будет автоматически переданы параметры приложений, необходимые для разработчика.

См. также:

Управление группами администрирования [742](#)

Управляемое устройство

Управляемое устройство – это компьютер под управлением Windows, Linux или macOS, на котором установлен Агент администрирования, или мобильное устройство, на котором установлено приложение безопасности "Лаборатории Касперского". Вы можете управлять такими устройствами с помощью задач и политик для приложений, установленных на устройствах. Вы также можете формировать отчеты для управляемых устройств.

Вы можете настроить управляемое немобильное устройство, чтобы оно выполняло функции точки распространения и шлюза соединений.

Устройство может находиться под управлением только одного Сервера администрирования. Один Сервер администрирования может обслуживать до 100 000 устройств, включая мобильные устройства.

Нераспределенное устройство

Нераспределенное устройство – это устройство в сети, которое не включено ни в одну из групп администрирования. Вы можете выполнять действия с нераспределенными устройствами, например, перемещать их в группы администрирования, устанавливая на них приложения.

Когда в сети обнаруживается новое устройство, оно помещается в группу администрирования Нераспределенные устройства. Можно настроить правила автоматического распределения устройств по группам администрирования в момент обнаружения.

Рабочее место администратора

Рабочее место администратора — устройство, на котором установлена Консоль администрирования или которое вы используете для работы с Kaspersky Security Center Web Console. С этих устройств администраторы могут осуществлять удаленное централизованное управление приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

В результате установки Консоли администрирования на вашем устройстве появится значок для запуска Консоли администрирования. Найдите его в меню **Пуск** → **Приложения** → **Kaspersky Security Center**.

Количество рабочих мест администратора не ограничивается. С каждого рабочего места администратора можно управлять группами администрирования сразу нескольких Серверов администрирования в сети. Рабочее место администратора можно подключить к Серверу администрирования (как к физическому, так и к виртуальному) любого уровня иерархии.

Рабочее место администратора можно включить в состав группы администрирования в качестве клиентского устройства.

В пределах групп администрирования любого Сервера одно и то же устройство может быть одновременно и клиентом Сервера администрирования, и Сервером администрирования, и рабочим местом администратора.

Плагин управления

Управление приложениями «Лаборатории Касперского» через Консоль администрирования выполняется при помощи специального компонента – *плагина управления*. В состав каждого приложения «Лаборатории Касперского», которым можно управлять при помощи Kaspersky Security Center, входит плагин управления.

С помощью плагина управления приложением в Консоли администрирования можно выполнять следующие действия:

- создавать и редактировать политики и параметры приложения, а также параметры задач этой приложения;
- получать информацию о задачах приложения, событиях в ее работе, а также о статистике работы приложения, получаемой с клиентских устройств.

Вы можете загрузить плагины управления с веб-сайта Службы технической поддержки "Лаборатории Касперского" <https://support.kaspersky.com/9333>.

См. также:

Работа с плагинами управления	368
Веб-плагин управления	46

Веб-плагин управления

Веб-плагин управления – это специальный компонент, используемый для удаленного управления приложениями "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console. Веб-плагин управления также называется *плагином управления*. Плагин управления представляет собой интерфейс между Kaspersky Security Center Web Console и определенным приложением "Лаборатории Касперского". С помощью плагина управления можно настраивать задачи и политики для приложения.

Вы можете загрузить веб-плагины управления с веб-сайта Службы технической поддержки «Лаборатории Касперского» <https://support.kaspersky.com/9333>.

Плагин управления предоставляет следующие возможности:

- Интерфейс для создания и изменения задач и параметров приложения.
- Интерфейс для создания и изменения политик и профилей политик (см. раздел "Политики и профили политик" см. стр. [431](#)) для удаленной централизованной настройки приложений "Лаборатории Касперского" и устройств.
- Передачу событий, сформированных приложениями.
- Функции Kaspersky Security Center Web Console для отображения оперативных данных и событий приложения, а также статистики, полученной от клиентских устройств.

См. также:

Плагин управления	46

Политики

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования (см. раздел "Группы администрирования" см. стр. 44) и ее подгруппе. Вы можете установить несколько приложений "Лаборатории Касперского" (см. раздел "Совместимые приложения и решения "Лаборатории Касперского"" на стр. 29) на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов (см. таблицу ниже):

Таблица 5. Статус политики

Состояние	Описание
Активная	Это текущая политика, которая применяется к устройству. Для приложения "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики приложения "Лаборатории Касперского" применяются к устройству.
Неактивная	Политика, которая в настоящее время не применяется к устройству.
Для автономных пользователей	Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

Политики действуют по следующим правилам:

- Для одного приложения можно настроить несколько политик с различными значениями.
- Для одного приложения может быть активна только одна политика.
- Вы можете активировать неактивную политику при возникновении определенного события. Например, в период вирусных атак можно включить параметры для усиленной антивирусной защиты.
- Политика может иметь дочерние политики.

Вы можете использовать политики для подготовки к экстренным ситуациям, например, к вирусной атаке. Например, если происходит атака через флеш-накопители USB, можно активировать политику, блокирующую доступ к флеш-накопителям. В этом случае текущая активная политика автоматически становится неактивной.

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

Профиль политики – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. **Эффективные параметры** – это набор параметров политики, параметров профиля политики и параметров локального приложения, которые в настоящее время применяются к устройству.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей.

См. также:

Основной сценарий установки.....	56
Политики и профили политик	431

Профили политик

Может возникнуть необходимость создать несколько копий одной политики для разных групп администрирования; может также возникнуть необходимость централизованно изменить параметры этих политик. Эти копии могут различаться одним или двумя параметрами. Например, все бухгалтеры в организации работают под управлением одной и той же политики, но старшим бухгалтерам разрешено использовать флеш-накопители USB, а младшим бухгалтерам не разрешено. В этом случае применение политик к устройствам только через иерархию групп администрирования может оказаться неудобным.

Чтобы избежать создания нескольких копий одной политики, Kaspersky Security Center позволяет создавать *профили политик*. Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики.

Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве. При активации профиля изменяются параметры "базовой" политики, которые исходно действовали на устройстве. Эти параметры принимают значения, указанные в профиле.

См. также:

Политики и профили политик	431

Задачи

Kaspersky Security Center управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения, только если для этого приложения установлен плагин управления.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных;
- синхронизация обновлений Windows Update;
- создание инсталляционного пакета на основе образа операционной системы эталонного устройства.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.
Локальные задачи могут быть изменены не только администратором средствами Консоли администрирования, но и пользователем удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.
- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.
Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.
- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в журналах событий Microsoft Windows и Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

См. также:

Основной сценарий установки.....	56
Управление задачами	414
Создание задачи	416

Область действия задачи

Область задачи – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Область *локальной задачи* – само устройство.
- Область *задачи Сервера администрирования* – Сервер администрирования.
- Область *групповой задачи* – перечень устройств, входящих в группу.

При создании *глобальной задачи* можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя.

- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования. Данные должны быть занесены в базу при подключении этих устройств или в результате обнаружения устройств.

- Указать выборку устройств.

С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка устройств является наиболее гибким способом задания области действия задачи.

Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запускаются на устройствах, не имеющих связи с Сервером администрирования. Задачи, область действия которых задается другим способом, запускаются непосредственно на устройствах и не зависят от наличия связи устройства с Сервером администрирования.

Задачи для выборок устройств будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования. Задачи, область действия которых задается другим способом, запускаются по локальному времени устройства.

Взаимосвязь политики и локальных параметров приложения

Вы можете при помощи политик устанавливать одинаковые значения параметров работы приложения для всех устройств, входящих в состав группы.

Переопределить значения параметров, заданные политикой, для отдельных устройств в группе можно при помощи локальных параметров приложения. При этом можно установить значения только тех параметров, изменение которых не запрещено политикой (параметр не закрыт замком).

Значение параметра, которое использует приложение на клиентском устройстве, определяется наличием замка (🔒) у параметра в политике:

- Если на изменение параметра наложен запрет, на всех клиентских устройствах используется одно и то же заданное политикой значение.
- Если запрет не наложен, то на каждом клиентском устройстве приложение использует локальное значение параметра, а не то, которое указано в политике. При этом значение параметра может изменяться через локальные параметры приложения.

Таким образом, при выполнении задачи на клиентском устройстве приложение использует параметры, заданные двумя разными способами:

- параметрами задачи и локальными параметрами приложения, если в политике не был установлен запрет на изменение параметра;
- политикой группы, если в политике был установлен запрет на изменение параметра.

Локальные параметры приложения изменяются после первого применения политики в соответствии с параметрами политики.

См. также:

Политики и профили политик[431](#)

Точка распространения

Точка распространения (ранее называлась «агент обновлений») – это устройство с установленным Агентом администрирования, который используется для распространения обновлений, удаленной установки приложений, получения информации об устройствах в сети. Точка распространения может выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства группы (в том числе и с помощью широковещательной рассылки по протоколу UDP). Обновления могут быть получены как с Сервера администрирования, так и с серверов обновлений "Лаборатории Касперского". В последнем случае для точки распространения должна быть создана задача обновления (см. раздел "Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства" см. стр. [482](#)).

Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Точки распространения ускоряют распространение обновлений и позволяют высвободить ресурсы Сервера администрирования.

- Распространять политики и групповые задачи с помощью широковещательной рассылки по протоколу UDP.
- Выполнять роль шлюза соединений с Сервером администрирования для устройств группы администрирования (см. раздел "Об использовании точки распространения в качестве шлюза соединений" на стр. [695](#)).

Если нет возможности создать прямое соединение между управляемыми устройствами группы и Сервером администрирования, точку распространения можно назначить шлюзом соединений этой группы с Сервером администрирования. В этом случае управляемые устройства подключаются к шлюзу соединений, который, в свою очередь, подключается к Серверу администрирования.

Наличие точки распространения, работающей в режиме шлюза соединений не исключает прямого соединения управляемых устройств с Сервером администрирования. Если шлюз соединений недоступен, а прямое соединение с Сервером администрирования технически возможно, управляемые устройства напрямую подключаются к Серверу.

- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.
- Выполнять удаленную установку приложений сторонних производителей и приложений "Лаборатории Касперского" средствами операционной системы точки распространения. Обратите внимание, что точка распространения может выполнять установку на клиентские устройства без Агента администрирования.

Эта функция позволяет удаленно передавать инсталляционные пакеты Агента администрирования на клиентские устройства, расположенные в сетях, к которым у Сервера администрирования нет прямого доступа.

- Выступать в роли прокси-сервера, участвующего в Kaspersky Security Network (KSN).

Можно включить прокси-сервер KSN на стороне точки распространения (см. раздел "Назначение устройства точкой распространения вручную" на стр. [491](#)), чтобы устройство выполняло роль прокси-сервера KSN. В этом случае на устройстве запустится служба прокси-сервера KSN (ksnproxy) (см. раздел "Изменения в системе после установки Kaspersky Security Center" на стр. [271](#)).

Передача файлов от Сервера администрирования точке распространения осуществляется по протоколу HTTP или, если настроено использование SSL-соединения, по протоколу HTTPS. Использование протокола HTTP или HTTPS обеспечивает более высокую производительность по сравнению с использованием протокола SOAP за счет сокращения трафика.

Устройства с установленным Агентом администрирования могут быть назначены точками распространения вручную администратором (см. раздел "Назначение устройства точкой распространения вручную" на стр. [491](#)) или автоматически Сервером администрирования. Полный список точек распространения для указанных групп администрирования отображается в отчете со списком точек распространения.

Областью действия точки распространения является группа администрирования, для которой она назначена администратором, а также ее подгруппы всех уровней вложенности. Если в иерархии групп

администрирования назначено несколько точек распространения, Агент администрирования управляемого устройства подключается к наиболее близкой по иерархии точке распространения.

Областью действия точек распространения также может являться сетевое местоположение. Сетевое местоположение используется для формирования вручную набора устройств, на которые точка распространения будет распространять обновления. Определение сетевого местоположения доступно только для устройств под управлением операционной системы Windows.

Если точки распространения назначаются автоматически Сервером администрирования, то Сервер назначает точки распространения по широковебательным доменам, а не по группам администрирования. Это происходит после того, как становятся известны широковебательные домены. Агент администрирования обменивается с другими Агентами администрирования своей подсети сообщениями и отправляет Серверу администрирования информацию о себе и краткую информацию о других Агентах администрирования. На основании этой информации Сервер администрирования может сгруппировать Агенты администрирования по широковебательным доменам. Широковещательные домены становятся известны Серверу администрирования после того, как опрошено более 70% Агентов администрирования в группах администрирования. Сервер администрирования опрашивает широковебательные домены каждые два часа. После того как точки распространения назначены по широковебательным доменам, их невозможно назначить снова по группам администрирования.

Если администратор вручную назначает точки распространения, их можно назначать группам администрирования или сетевым местоположениям.

Агенты администрирования с активным профилем соединения не участвуют в определении широковебательного домена. Kaspersky Security Center присваивает каждому Агенту администрирования уникальный адрес многоадресной IP-рассылки, который не пересекается с другими адресами. Это позволяет избежать превышения нагрузки на сеть, которое возникло бы из-за пересечения адресов.

Если на одном участке сети или в группе администрирования назначаются две точки распространения или более, одна из них становится активной точкой распространения, остальные назначаются резервными. Активная точка распространения загружает обновления и инсталляционные пакеты непосредственно с Сервера администрирования, резервные точки распространения обращаются за обновлениями только к активной точке распространения. В этом случае файлы загружаются только один раз с Сервера администрирования и далее распределяются между точками распространения. Если активная точка распространения по каким-либо причинам становится недоступной, одна из резервных точек распространения назначается активной. Сервер администрирования назначает точку распространения резервной автоматически.

Статус точки распространения (*Активный/Резервный*) отображается флажком в отчете утилиты klnagchk (см. раздел "Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита klnagchk" на стр. 757).

Для работы точки распространения требуется не менее 4 ГБ свободного места на диске. Если объем свободного места на диске точки распространения меньше 2 ГБ, Kaspersky Security Center создает проблему безопасности с уровнем важности *Предупреждение*. Проблема безопасности будет опубликована

в свойствах устройства в разделе **Проблемы безопасности**.

При работе задач удаленной установки на устройстве с точкой распространения потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть больше размера всех устанавливаемых инсталляционных пакетов.

При работе задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с точкой распространения потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть как минимум в два раза больше размера всех устанавливаемых патчей.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

См. также:

Настройка точек распространения и шлюзов соединений	685
О точках распространения	147
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455

Шлюз соединения

Шлюз соединения – это Агент администрирования, работающий в особом режиме. Шлюз соединения принимает соединения от других Агентов администрирования и туннелирует их к Серверу администрирования через собственное соединение с Сервером. В отличие от обычного Агента администрирования, шлюз соединения ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования.

Шлюз соединения может принимать соединения от 10 000 устройств.

Существует два варианта использования шлюзов соединения:

- Рекомендуется установить шлюз соединения в демилитаризованной зоне (DMZ). Для других Агентов администрирования, установленных на автономных устройствах (см. раздел "О подключении автономных устройств" см. стр. [300](#)), необходимо специально настроить подключение к Серверу администрирования через шлюз соединения.

Шлюз соединения не изменяет и не обрабатывает данные, передаваемые от Агентов администрирования на Сервер администрирования. Шлюз соединения не записывает эти данные в буфер и, следовательно, не может принимать данные от Агента администрирования и затем передавать их на Сервер администрирования. Если Агент администрирования пытается подключиться к Серверу администрирования через шлюз соединения, но шлюз соединения не может подключиться к Серверу администрирования, Агент администрирования воспринимает это как недоступный Сервер администрирования. Все данные остаются на Агенте администрирования (не на шлюзе соединения).

Шлюз соединения не может подключиться к Серверу администрирования через другой шлюз соединения. Это означает, что Агент администрирования не может одновременно быть шлюзом соединения и использовать шлюз соединения для подключения к Серверу администрирования.

Все шлюзы соединения включены в список точек распространения в свойствах Сервера администрирования.

- Вы также можете использовать шлюзы соединения в сети. Например, автоматически назначаемые точки распространения также становятся шлюзами соединений в своей области действия. Однако во внутренней сети шлюзы соединения не дают значительных преимуществ. Они уменьшают количество сетевых подключений, принимаемых Сервером администрирования, но не уменьшают объем входящих данных. Даже без шлюзов соединения все устройства могли подключаться к Серверу администрирования.

См. также:

Настройка точек распространения и шлюзов соединений	685
Об использовании точки распространения в качестве шлюза соединений	695

Архитектура приложения

Этот раздел описывает архитектуру и основные понятия Kaspersky Security Center.

Приложение Kaspersky Security Center включает в себя следующие основные компоненты:

- **Сервер администрирования** (далее также *Сервер*). Осуществляет функции централизованного хранения информации об установленных в сети организации приложениях и управления ими.
- **Агент администрирования** (далее также *Агент*). Координирует взаимодействие Сервера администрирования и приложений "Лаборатории Касперского", установленных на узле сети (рабочей станции или сервере). Этот компонент является единым для всех приложений, разработанных для систем Microsoft Windows. Для приложений "Лаборатории Касперского" для операционных систем UNIX и подобных им и macOS существуют отдельные версии Агента администрирования.
- **Консоль администрирования** (далее также *Консоль*). Предоставляет пользовательский интерфейс к административным службам Сервера и Агента. Консоль администрирования выполнена в виде компонента расширения к Microsoft Management Console (MMC). Консоль администрирования позволяет подключаться к удаленному Серверу администрирования через интернет.
- **Сервер мобильных устройств**. Предоставляет доступ к мобильным устройствам и позволяет управлять ими с помощью Консоли администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.

См. также:

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности:
дополнительные сведения[104](#)

Основной сценарий установки

Следуя основному сценарию, вы можете развернуть Сервер администрирования, а также установить на устройства сети Агент администрирования и приложения безопасности. Вы можете использовать этот сценарий и для ознакомления с приложением, и для установки приложения с целью дальнейшей работы.

Установка Kaspersky Security Center включает следующие шаги:

17. Подготовка
18. Установка Kaspersky Security Center и приложений безопасности "Лаборатории Касперского" на устройстве с Сервером администрирования.
19. Удаленное развертывание приложений безопасности "Лаборатории Касперского" на клиентских устройствах.

Развертывание Kaspersky Security Center в облачном окружении и развертывание Kaspersky Security Center для поставщиков услуг описаны в соответствующих разделах справки.

Рекомендуется отвести на установку Сервера администрирования не менее часа, а на выполнение сценария целиком – не менее одного рабочего дня. На компьютер, который будет выполнять роль Сервера

администрирования Kaspersky Security Center, также рекомендуется установить приложение безопасности, например, Kaspersky Security для Windows Server или Kaspersky Endpoint Security.

После завершения сценария в сети организации будет развернута защита из следующим способом:

- Для Сервера администрирования будет установлена СУБД.
- Сервер администрирования Kaspersky Security Center будет установлен.
- Все необходимые политики и задачи будут созданы, а также будут настроены заданные по умолчанию параметры политик и задач.
- На управляемые устройства будут установлены приложения безопасности (например, Kaspersky Endpoint Security для Windows) и Агент администрирования.
- Группы администрирования будут созданы (возможно, объединенные в иерархию).
- При необходимости будет развернута защита мобильных устройств.
- При необходимости будут назначены точки распространения.

Установка Kaspersky Security Center происходит поэтапно:

Подготовка

а. Получение необходимых файлов

Убедитесь, что у вас есть лицензионный ключ (код активации) для Kaspersky Security Center или лицензионные ключи (коды активации) для приложений безопасности "Лаборатории Касперского".

Распакуйте архив, полученный от вашего поставщика. Этот архив содержит лицензионные ключи (файлы формата KEY), коды активации (см. раздел "О коде активации" на стр. [345](#)) и список приложений "Лаборатории Касперского", которые могут быть активированы каждым из этих лицензионных ключей.

Если вы хотите попробовать Kaspersky Security Center, вы можете получить пробную тридцатидневную версию на веб-сайте "Лаборатории Касперского" <https://www.kaspersky.com/small-to-medium-business-security>.

Подробную информацию о лицензировании приложений безопасности "Лаборатории Касперского", которые не входят в состав Kaspersky Security Center, вы можете найти в документации к этим приложениям.

б. Выбор структуры защиты организации

Ознакомьтесь с компонентами Kaspersky Security Center (см. раздел "Архитектура приложения" на стр. [56](#)). Выберите структуру защиты (см. раздел "Выбор структуры защиты организации" на стр. [136](#)) и конфигурацию сети (см. раздел "Типовые конфигурации Kaspersky Security Center" на стр. [137](#)), наиболее подходящие для вашей организации. Исходя из конфигурации сети и пропускной способности каналов связи определите, какое количество Серверов администрирования необходимо использовать и как их разместить по офисам (см. раздел "Планирование развертывания Kaspersky Security Center" на стр. [133](#)), если вы работаете с распределенной сетью.

Для достижения и сохранения оптимальной производительности при различных условиях работы, пожалуйста, учитывайте количество устройств в сети, топологию сети и необходимый вам набор функций Kaspersky Security Center (подробнее см. в Руководстве по масштабированию Kaspersky Security Center).

Определите, будет ли в вашей организации использоваться иерархия Серверов администрирования (см. раздел "Удаление иерархии Серверов администрирования" на стр. [41](#)). Для этого нужно понять, возможно и целесообразно ли обслуживание всех клиентских устройств одним Сервером администрирования или требуется выстроить иерархию Серверов администрирования. Вам также

может потребоваться выстроить иерархию Серверов администрирования, совпадающую с организационной структурой предприятия, сеть которого вы хотите защитить.

Если вам требуется обеспечить защиту мобильных устройств, выполните подготовительные действия по настройке Сервера iOS MDM.

Убедитесь, что устройства, выбранные вами для использования в качестве Серверов администрирования, а также для установки Консоли администрирования, соответствуют аппаратным и программным требованиям (см. стр. [29](#)).

с. Подготовка к использованию пользовательских сертификатов

Если инфраструктура открытых ключей (PKI) вашей организации требует, чтобы вы использовали пользовательские сертификаты, выпущенные определенным доверенным центром сертификации (CA), подготовьте эти сертификаты (см. раздел "О сертификатах Kaspersky Security Center" см. стр. [72](#)) и убедитесь, что они соответствуют всем требованиям (см. раздел "Требования к пользовательским сертификатам, используемым в Kaspersky Security Center" см. стр. [76](#)).

d. Подготовка к лицензированию Kaspersky Security Center

Если вы планируете использовать версию Kaspersky Security Center с поддержкой Управления мобильными устройствами, Интеграцией с SIEM-системами и / или с поддержкой Системного администрирования, убедитесь, что у вас имеется файл ключа либо код активации для лицензирования (см. раздел "Лицензирование" на стр. [340](#)) приложения.

e. Подготовка к лицензированию управляемых приложений безопасности

Во время развертывания защиты вам потребуется предоставить "Лаборатории Касперского" активные лицензионные ключи на те приложения, которыми вы планируете управлять с помощью Kaspersky Security Center (см. список доступных для управления приложений безопасности (см. раздел "Совместимые приложения и решения "Лаборатории Касперского" на стр. [29](#))). Подробнее о лицензировании каждого из приложений безопасности вы можете прочитать в документации к этим приложениям.

f. Выбор аппаратной конфигурации Сервера администрирования и СУБД

Спланируйте аппаратную конфигурацию для СУБД и Сервера администрирования с учетом количества устройств в вашей сети.

g. Выбор СУБД

При выборе СУБД учитывайте количество управляемых устройств, которые будет обслуживать Сервер администрирования. Если в вашей сети менее 10 000 устройств и вы не планируете увеличивать их количество, вы можете выбрать бесплатную СУБД SQL Express или MySQL и установить ее на одном устройстве с Сервером администрирования. Вы можете выбрать СУБД MariaDB, которая позволяет управлять устройствами в количестве до 20 000. Если в вашей сети более 10 000 устройств (или вы планируете расширение сети до такого количества устройств), рекомендуется выбирать платную СУБД SQL и размещать ее на отдельном устройстве. Платная СУБД может работать с несколькими Серверами администрирования, а бесплатная СУБД – только с одним.

Если вы выберете SQL Server, тогда можно перенести данные, хранящиеся в базе данных, в MySQL, в MariaDB или в Azure SQL СУБД. Чтобы выполнить перенос данных, выполните резервное копирование данных и восстановите их в новой СУБД (см. раздел "Резервное копирование и восстановление данных в интерактивном режиме" на стр. [725](#)).

h. Установка СУБД и создание базы данных

Узнайте больше об учетных записях для работы с СУБД (см. раздел "Учетные записи для работы с СУБД" на стр. [207](#)) и установите СУБД.

Перед установкой выберите поддерживаемую СУБД (см. раздел "Аппаратные и программные требования" см. стр. [29](#)). Вы можете выбрать, например, PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL или MariaDB.

Сведения о том, как установить выбранную СУБД, см. в документации к ней.

Если вы установите MariaDB (см. раздел "Настройка сервера MariaDB x64 для работы с Kaspersky Security Center" на стр. [141](#)), MySQL (см. раздел "Настройка сервера MySQL x64 для работы с Kaspersky Security Center" см. стр. [142](#)), PostgreSQL (см. раздел "Настройка сервера PostgreSQL или Postgres Pro для работы с Kaspersky Security Center" см. стр. [143](#)) или Postgres Pro (см. раздел "Настройка сервера PostgreSQL или Postgres Pro для работы с Kaspersky Security Center" см. стр. [143](#)) используйте рекомендуемые параметры, чтобы обеспечить правильную работу СУБД.

Запишите и сохраните параметры СУБД, поскольку они потребуются вам при установке Сервера администрирования. Эти параметры включают имя SQL-сервера, номер порта для подключения к SQL-серверу, имя учетной записи и пароль для доступа к SQL-серверу.

Если вы решили установить СУБД PostgreSQL или Postgres Pro, убедитесь, что вы указали пароль для суперпользователя. Если пароль не указан, Сервер администрирования может не подключиться к базе данных.

По умолчанию инсталлятор Kaspersky Security Center создает базу данных для размещения информации Сервера администрирования (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. [238](#)), однако вы можете отказаться от ее создания и использовать другую базу данных. В этом случае убедитесь, что база данных создана, вы знаете ее имя, а учетная запись, под которой Сервер администрирования получит доступ к этой базе данных, будет иметь для нее роль db_owner.

При необходимости обратитесь за информацией к администратору СУБД.

i. Настройка портов

Убедитесь, что для взаимодействия компонентов согласно выбранной вами структуре защиты (см. раздел "Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения" на стр. [104](#)) открыты необходимые порты (см. раздел "Порты, используемые Kaspersky Security Center" на стр. [63](#)).

Если требуется предоставить доступ к Серверу администрирования из интернета (см. раздел "Предоставление доступа к Серверу администрирования из интернета" на стр. [144](#)), настройте порты и параметры подключения в зависимости от конфигурации сети.

j. Проверка учетных записей

Проверьте наличие у вас прав локального администратора для успешной установки Сервера администрирования Kaspersky Security Center и развертывания защиты на устройствах. Права локального администратора на клиентских устройствах нужны для установки на эти устройства Агента администрирования. После установки Агента администрирования вы сможете с его помощью удаленно устанавливать приложения на устройства, не пользуясь учетной записью с правами администратора устройства.

По умолчанию инсталлятор Kaspersky Security Center создает на устройстве, выбранном для установки Сервера администрирования, три локальные учетные записи, от имени которых будет запускаться Сервер администрирования (см. раздел "Шаг 9. Выбор учетной записи для запуска Сервера администрирования" на стр. [240](#)) и службы Kaspersky Security Center (см. раздел "Шаг 10. Выбор учетной записи для запуска служб Kaspersky Security Center" на стр. [241](#)):

- KL-AK-*: учетная запись службы Сервера администрирования;

- NT Service/KSC*: учетная запись для прочих служб из состава Сервера администрирования;
- KIPxeUser: учетная запись для развертывания операционных систем.

Вы можете отказаться от создания учетных записей для служб Сервера администрирования и других служб. Вместо этого вы можете использовать существующие учетные записи, например учетные записи домена, если планируете установить Сервер администрирования на отказоустойчивом кластере (см. раздел "Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере" на стр. [226](#)) или планируете использовать учетные записи домена вместо локальных учетных записей по другой причине. В этом случае убедитесь, что учетные записи для запуска Сервера администрирования и служб Kaspersky Security Center созданы, являются непривилегированными и обладают необходимыми правами для доступа к СУБД (см. раздел "Учетные записи для работы с СУБД" на стр. [207](#)). (Если вы планируете в дальнейшем разворачивать операционные системы (см. раздел "Развертывание операционных систем на новых устройствах в сети" на стр. [849](#)) на устройствах средствами Kaspersky Security Center, не отказывайтесь от создания учетных записей.)

Установка Kaspersky Security Center и приложений безопасности "Лаборатории Касперского" на устройстве с Сервером администрирования

а. Установка Сервера администрирования, Консоли администрирования, Kaspersky Security Center Web Console и плагинов управления для приложений безопасности

Загрузите Kaspersky Security Center <https://www.kaspersky.com/small-to-medium-business-security/security-center> с сайта "Лаборатории Касперского". Можно загрузить полный пакет, только Kaspersky Security Center Web Console или только Консоль администрирования.

Установите Сервер администрирования (см. раздел "Установка Kaspersky Security Center" на стр. [206](#)) на устройство, которое вы выбрали (либо устройства, если вы планируете (см. раздел "Типовая конфигурация: один офис" на стр. [137](#)) использовать более одного Сервера администрирования). Вы можете выбрать стандартную или выборочную установку Сервера администрирования. Вместе с Сервером администрирования установится Консоль администрирования. Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена.

Стандартная установка (на стр. [229](#)) рекомендуется, если вы хотите ознакомиться с программой Kaspersky Security Center, например, протестировать ее работу на небольшом участке вашей сети. При стандартной установке вы настраиваете только параметры базы данных. Также вы можете установить только набор плагинов управления, заданный по умолчанию, для приложений "Лаборатории Касперского". Вы также можете воспользоваться стандартной установкой, если вы уже имеете опыт работы с Kaspersky Security Center и знаете, как после стандартной установки настроить все необходимые вам параметры.

Выборочная установка (на стр. [234](#)) рекомендуется, если вы планируете настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления приложениями "Лаборатории Касперского" будут установлены. При необходимости вы можете запустить выборочную установку в тихом режиме (см. раздел "Установка Сервера администрирования в тихом режиме" на стр. [264](#)).

Вместе с Сервером администрирования устанавливаются также Консоль администрирования и серверная версия Агента администрирования. Можно также выбрать установку Kaspersky Security Center Web Console (см. раздел "Шаг 3. Установка Kaspersky Security Center Web Console" на стр. [236](#)).

При необходимости можно установить Консоль администрирования (см. раздел "Установка Консоли администрирования на рабочее место администратора" на стр. [270](#)) и Kaspersky Security Center Web

Console на рабочее место администратора независимо для управления Сервером администрирования по сети.

b. Первоначальная настройка и лицензирование

После завершения установки Сервера администрирования при первом подключении к Серверу администрирования автоматически запускается Мастер первоначальной настройки (см. раздел "Мастер первоначальной настройки Сервера администрирования" на стр. [281](#)). Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики (на стр. [47](#)) и задачи (на стр. [48](#)) с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач (см. раздел "Сценарий: настройка защиты сети" на стр. [403](#)).

Если вы планируете использовать функциональность, выходящую за рамки Базовой функциональности (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. [354](#)), активируйте приложение по лицензии. Вы можете выполнить это на одном из шагов (см. раздел "Шаг 2. Выбор способа активации приложения" на стр. [284](#)) мастера первоначальной настройки.

c. Проверка успешности установки Сервера администрирования

После успешного выполнения предыдущих шагов Сервер администрирования установлен и готов к дальнейшей работе.

Убедитесь, что работает Консоль администрирования и что вы можете подключиться через Консоль к Серверу администрирования. Убедитесь также, что на Сервере администрирования имеется задача загрузки обновлений в хранилище Сервера администрирования (в папке **Задачи** дерева консоли (см. раздел "Дерево консоли" на стр. [921](#))) и политика для Kaspersky Endpoint Security (в папке **Политики** дерева консоли).

После завершения проверки, перейдите к шагам ниже.

Удаленное развертывание приложений безопасности "Лаборатории Касперского" на клиентских устройствах

a. Обнаружение устройств в сети

Этот шаг входит в мастер первоначальной настройки (см. раздел "Шаг 12. Обнаружение устройств" на стр. [295](#)). Вы можете также запустить обнаружение устройств (на стр. [324](#)) вручную. В результате Сервер администрирования Kaspersky Security Center получает адреса и имена всех устройств, зарегистрированных в сети. В дальнейшем вы можете с помощью Kaspersky Security Center устанавливать приложения "Лаборатории Касперского" и других производителей на обнаруженные устройства. Kaspersky Security Center запускает обнаружение устройств регулярно, поэтому, если в сети появятся новые устройства, они будут обнаружены автоматически.

b. Установка Агента администрирования и приложений безопасности на устройства в сети

Развертывание защиты (см. раздел "Сценарий: настройка защиты сети" на стр. [403](#)) в сети организации подразумевает установку Агента администрирования и программ безопасности (например, Kaspersky Endpoint Security для Windows) на устройства, которые были обнаружены Сервером администрирования при обнаружении устройств.

Приложения безопасности защищают устройства от вирусов и/или других приложений, представляющих угрозу. Агент администрирования обеспечивает связь устройства с Сервером администрирования. Параметры Агента администрирования автоматически настраиваются по умолчанию.

При необходимости можно установить Агент администрирования в неинтерактивном (тихом) режиме с файлом ответов (см. раздел "Установка в тихом режиме (с файлом ответов)" на стр. [179](#)) или без

него (см. раздел "Установка Агента администрирования в тихом режиме (без файла ответов)" на стр. [180](#)).

Перед тем как установить Агент администрирования и приложения безопасности на устройства в сети, убедитесь, что эти устройства доступны (то есть включены). Вы можете установить Агент администрирования на виртуальные машины, так же как и на физические устройства (см. раздел "Виртуальная инфраструктура" на стр. [187](#)).

Возможна удаленная или локальная установка приложений безопасности и Агента администрирования.

Удаленная установка (см. раздел "Приложения "Лаборатории Касперского". Централизованное развертывание" на стр. [357](#)) – с помощью мастера развертывания защиты вы можете удаленно установить приложение безопасности (например, Kaspersky Endpoint Security для Windows) и Агент администрирования на устройствах, которые были обнаружены Сервером администрирования в сети организации. Как правило, задача удаленной установки успешно развертывает защиту для большинства сетевых устройств. Однако она может возвращать ошибку на некоторых устройствах, если, например, устройство отключено или недоступно по другой причине. В этом случае рекомендуется вручную подключиться к устройству и использовать локальную установку.

Локальная установка (см. раздел "Локальная установка приложений" на стр. [192](#)) – используется на тех устройствах сети, на которых не удалось развернуть защиту с помощью задачи удаленной установки. Чтобы установить защиту на такие устройства, создайте автономный инсталляционный пакет для запуска на этих устройствах локально.

Установка Агента администрирования на устройства с операционными системами Linux и macOS описана в документации для Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Mac соответственно. Несмотря на то, что устройства под управлением операционных систем Linux и macOS считаются менее уязвимыми, чем устройства под управлением Windows, на них также рекомендуется устанавливать приложения безопасности.

После установки убедитесь, что приложение безопасности установлено на управляемые устройства. Для этого запустите Отчет о версиях приложений "Лаборатории Касперского" и ознакомьтесь с его результатами (см. раздел "Просмотр реестра приложений" на стр. [585](#)).

c. Распространение лицензионных ключей на клиентские устройства

Распространите лицензионные ключи (см. раздел "Приложения "Лаборатории Касперского": лицензирование и активация" на стр. [388](#)) на клиентские устройства, чтобы активировать управляемые приложения безопасности на этих устройствах.

d. Настройка защиты мобильных устройств

Этот шаг входит в мастер первоначальной настройки.

Чтобы управлять корпоративными мобильными устройствами, выполните необходимые подготовительные шаги и разверните Управление мобильными устройствами.

e. Создание структуры групп администрирования

В некоторых случаях для развертывания защиты на устройствах сети оптимальным образом может потребоваться разделить устройства на группы администрирования (см. раздел "Группы администрирования" см. стр. [44](#)) с учетом организационной структуры организации. Вы можете создать правила перемещения для распределения устройств по группам или распределить устройства вручную. Для групп администрирования можно назначать групповые задачи, определять область действия политик и назначать точки распространения.

Убедитесь, что все управляемые устройства правильно распределены по соответствующим группам администрирования и что у вас в сети не осталось нераспределенных устройств (см. стр. [323](#)).

f. Назначение точек распространения

Kaspersky Security Center автоматически назначает точки распространения (см. раздел "О точках распространения" на стр. [147](#)) группам администрирования, но при необходимости вы можете назначить их вручную. Точки распространения рекомендуется использовать (см. раздел "Настройка точек распространения и шлюзов соединений" см. стр. [685](#)) в больших сетях для снижения нагрузки на Сервер администрирования, а также в сетях с распределенной структурой для предоставления Серверу администрирования доступа к устройствам или группам устройств, соединенным каналами с низкой пропускной способностью. В качестве точек распространения можно использовать устройства под управлением Linux (см. раздел "Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне" см. стр. [691](#)) и под управлением Windows.

См. также:

Основные понятия	39
Порты, используемые Kaspersky Security Center	63
Схемы трафика данных и использования портов	87
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Архитектура приложения	56
Предоставление доступа к Серверу администрирования из интернета	144
Сценарий: мониторинг и отчеты	593
Сценарий: настройка защиты сети	403

Порты, используемые Kaspersky Security Center

В таблицах ниже перечислены порты, которые должны быть открыты на Серверах администрирования и на клиентских устройствах. Если вы хотите, вы можете изменить номера портов по умолчанию.

В таблице ниже перечислены порты, которые должны быть открыты на Сервере администрирования. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server, порт 1433 для Microsoft SQL Server или порт 5432 для PostgreSQL и Postgres Pro). Подробную информацию см. в документации СУБД.

Таблица 6. Порты, которые должны быть открыты на Сервере администрирования

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
8060	klcsweb	TCP	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов. Вы можете изменить номер порта по умолчанию в разделе Веб-сервер (см. раздел " Настройка параметров Веб-сервера " см. стр. 720) окна свойств Сервера администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.
8061	klcsweb	TCP (TLS)	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов. Вы можете изменить номер порта по умолчанию в разделе Веб-сервер (см. раздел " Настройка параметров Веб-сервера " см. стр. 720) окна свойств Сервера администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.
13000	klserver	TCP (TLS)	Прием подключений от Агентов администрирования и от подчиненных Серверов администрирования; используется также на подчиненных серверах для приема подключений от главного Сервера (например, если подчиненный Сервер находится в демилитаризованной зоне)	Управление клиентскими устройствами и подчиненными Серверами администрирования. Вы можете изменить номер порта по умолчанию для приема подключений от Агентов администрирования при настройке портов подключения (см. раздел "Шаг 12. Настройка параметров подключения к Серверу администрирования" на стр. 242). Вы можете изменить номер порта по умолчанию для приема подключений от подчиненных Серверов администрирования при создании иерархии Серверов администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
13000	klserver	UDP	Прием информации от Агентов администрирования о выключении устройств	Управление клиентскими устройствами. Вы можете изменить номер порта по умолчанию в параметрах политики Агента администрирования в Консоли администрирования (см. раздел "Параметры политики Агента администрирования" см. стр. 789) или в Kaspersky Security Center Web Console.
13291	klserver	TCP (TLS)	Прием подключений от Консоли администрирования к Серверу администрирования	Управление Сервером администрирования. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования в Консоли администрирования.
13299	klserver	TCP (TLS)	Получение соединений от Kaspersky Security Center Web Console к Серверу администрирования; получение соединений от Сервера администрирования через OpenAPI	Kaspersky Security Center Web Console, OpenAPI. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (в подразделе Порты подключения раздела Общие) в Консоли администрирования на основе консоли Microsoft Management Console (MMC), либо при создании иерархии Серверов администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.
14000	klserver	TCP	Прием подключений от Агентов администрирования	Управление клиентскими устройствами. Вы можете изменить номер порта по умолчанию при настройке портов подключения (см. раздел "Шаг 12. Настройка параметров подключения к Серверу администрирования" на стр. 242) при установке Kaspersky Security Center или при подключении клиентского устройства к Серверу администрирования вручную (см. раздел "Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmove" на стр. 750).

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
13111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	TCP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования (см. раздел "Настройка доступа к KPSN" на стр. 874).
15111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	UDP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования (см. раздел "Настройка доступа к KPSN" на стр. 874).
17000	klactprx	TCP (TLS)	Прием подключений для активации приложений от управляемых устройств (кроме мобильных устройств)	Прокси-сервер активации, используемый немобильными устройствами для активации приложений "Лаборатории Касперского" с помощью кодов активации. Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования.
17100 (только если вы управляете мобильными устройствами)	klactprx	TCP (TLS)	Прием подключений для активации приложений от мобильных устройств	Прокси-сервер активации для мобильных устройств. Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования.
19170	klserver	HTTPS (TLS)	Туннелирование соединения с управляемыми устройствами с помощью утилиты klstunnel	Удаленное подключение к управляемым устройствам с помощью Kaspersky Security Center Web Console. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (в подразделе Дополнительные порты раздела Общие) только в Консоли администрирования.
13292 (только если вы управляете мобильными устройствами)	klserver	TCP (TLS)	Прием подключений от мобильных устройств	Управление мобильными устройствами. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
13294 (только если вы управляете мобильными устройствами)	klserver	TCP (TLS)	Прием подключений от устройств с защитой на уровне UEFI	Управление клиентскими устройствами с защитой на уровне UEFI. Вы можете изменить номер порта по умолчанию при подключении мобильных устройств (см. раздел "Шаг 10. Подключение мобильных устройств" на стр. 290) или позже в окне свойств Сервера администрирования (в подразделе Дополнительные порты раздела Общие) в Консоли администрирования или в Kaspersky Security Center Web Console.
13296	klserver	TCP (TLS)	Публикация метрик Kaspersky Security Center для Prometheus	Публикация метрик Kaspersky Security Center, которые в дальнейшем получит Prometheus. Посмотреть метрики можно по ссылке: <a href="https://<адрес_сервера>:13296/metrics">https://<адрес_сервера>:13296/metrics . В поле <адрес_сервера> укажите IP-адрес или доменное имя вашего Сервера администрирования. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования в Консоли администрирования (см. раздел "Шаг 10. Подключение мобильных устройств" на стр. 290).
30522, 30523 (локальные порты)	klagent	TCP	Передача обновлений приложения "Лаборатории Касперского" на управляемые устройства с помощью Агента администрирования с использованием компонента FileTransferBridge.	Управляемые устройства, которые получают обновления приложения "Лаборатории Касперского" с Сервера администрирования (см. раздел "Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"" см. стр. 460), указанного в качестве источника обновлений баз.

В таблице ниже указан порт, который должен быть открыт на Сервере iOS MDM (только если вы управляете мобильными устройствами).

Таблица 7. Порт, используемый Сервером iOS MDM

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
443	klismdmservicesrv	TCP (TLS)	Прием соединений от мобильных устройств iOS	Управление мобильными устройствами. Вы можете изменить номер порта по умолчанию при установке Сервера iOS MDM.

В таблице ниже указан порт, который должен быть открыт на Сервере Kaspersky Security Center Web Console. Это может быть то же устройство, на котором установлен Сервер администрирования, или другое устройство.

Таблица 8. Порт, используемый Сервером Kaspersky Security Center Web Console

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
8080	Node.js: серверный JavaScript	TCP (TLS)	Прием соединений от браузера и передача в Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Вы можете изменить номер порта по умолчанию при установке Kaspersky Security Center Web Console на устройстве под управлением Windows или Linux. Если вы устанавливаете Kaspersky Security Center Web Console на устройство с операционной системой ALT Linux, то необходимо указать номер порта, отличный от 8080, так как порт 8080 используется операционной системой.

В таблице ниже указан порт, который должен быть открыт на управляемых устройствах, на которых установлен Агент администрирования.

Таблица 9. Порты, используемые Агентом администрирования

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
15000	klagent	UDP	Сигналы управления от Сервера администрирования или точки распространения к Агентам администрирования	Управление клиентскими устройствами. Вы можете изменить номер порта по умолчанию в параметрах политики Агента администрирования в Консоли администрирования (см. раздел "Параметры политики Агента администрирования" см. стр. 789) или в Kaspersky Security Center Web Console.
15000	klagent	Широковещательная рассылка UDP	Получение данных о других Агентах администрирования в том же широковещательном домене (далее данные отправляются на Сервер администрирования)	Доставка обновлений и инсталляционных пакетов.
15001	klagent	UDP	Получение многоадресных запросов от точек распространения (если используется)	Получение обновлений и инсталляционных пакетов от точки распространения. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. раздел "Назначение устройства точкой распространения вручную" на стр. 491) или в Kaspersky Security Center Web Console.

Обратите внимание, что процесс klagent также может запрашивать свободные порты из динамического диапазона портов операционной системы конечного устройства. Операционная система назначает эти порты процессу klagent автоматически, поэтому процесс klagent может использовать некоторые порты, используемые другим программным обеспечением. Если процесс klagent влияет на работу этого программного обеспечения, измените параметры порта в программном обеспечении или измените динамический диапазон портов по умолчанию в вашей операционной системе, чтобы исключить порт, используемый этим программным обеспечением.

Обратите внимание, что рекомендации по совместимости Kaspersky Security Center со сторонним программным обеспечением носят справочный характер и могут быть неприменимы к новым версиям стороннего программного обеспечения. Описанные рекомендации по настройке портов основаны на опыте Службы технической поддержки и наших лучших практиках.

В таблице ниже указаны порты, которые должны быть открыты на управляемом устройстве с установленным Агентом администрирования, выполняющим роль точки распространения. Перечисленные порты должны быть открыты на устройствах, которые выполняют роль точек распространения, в дополнение к портам, используемым Агентами администрирования (см. таблицу выше).

Таблица 10. Порты, используемые Агентом администрирования, который работает в качестве точки распространения

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
13000	klagent	TCP (TLS)	Прием подключений от Агентов администрирования и от Kaspersky Security Center когда точка распространения выполняет роль шлюза соединения в демилитаризованной зоне (см. раздел "Об использовании точки распространения в качестве шлюза соединений" на стр. 695). Если в качестве точки распространения указано устройство с установленным Сервером администрирования, для SSL-соединения по умолчанию используется порт 13001 вместо 13000.	Управление клиентскими устройствами, доставка обновлений и инсталляционных пакетов. Подробнее см. в раздел: Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (на стр. 113). Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. раздел "Назначение устройства точкой распространения вручную" на стр. 491) или в Kaspersky Security Center Web Console.
13111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	TCP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. раздел "Назначение устройства точкой распространения вручную" на стр. 491) или в Kaspersky Security Center Web Console.
15111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	UDP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. раздел "Назначение устройства точкой распространения вручную" на стр. 491) или в Kaspersky Security Center Web Console.

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
17111 (только если на устройстве запущена служба прокси-сервера KSN)	kspnproxy	HTTPS	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. раздел "Назначение устройства точкой распространения вручную" на стр. 491) или в Kaspersky Security Center Web Console.
13295 (только если вы используете точку распространения в качестве push-сервера)	klagent	TCP (TLS)	Прием подключений от клиентских устройств	Push-сервер. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. раздел "Использование точки распространения в качестве извещающего сервера" на стр. 697) или в Kaspersky Security Center Web Console.

См. также:

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Основной сценарий установки.....	56

Сертификаты для работы с Kaspersky Security Center

Этот раздел содержит информацию о сертификатах Kaspersky Security Center и описывает, как выпустить пользовательский сертификат для Сервера администрирования.

В этом разделе

О сертификатах Kaspersky Security Center.....	72
О сертификате Сервера администрирования.....	75
Требования к пользовательским сертификатам, используемым в Kaspersky Security Center	76
Сценарий: задание пользовательского сертификата Сервера администрирования	78
Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert.....	81
Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmove	83
Перевыпуск сертификата Веб-сервера	84

О сертификатах Kaspersky Security Center

Kaspersky Security Center использует следующие типы сертификатов для обеспечения безопасного взаимодействия между компонентами приложения:

- сертификат Сервера администрирования;
- мобильный сертификат;
- сертификат Сервера iOS MDM;
- сертификат Веб-сервера Kaspersky Security Center;
- сертификат Kaspersky Security Center Web Console.

По умолчанию Kaspersky Security Center использует самоподписанные сертификаты (то есть выданные самим Kaspersky Security Center). Если требуется, вы можете заменить самоподписанные сертификаты пользовательскими сертификатами, в соответствии со стандартами безопасности вашей организации. После того как Сервер администрирования проверит соответствие пользовательского сертификата всем применимым требованиям, этот сертификат приобретает такую же область действия, что и самоподписанный сертификат. Единственное отличие состоит в том, что пользовательский сертификат не перевыпускается автоматически по истечении срока действия. Вы заменяете сертификаты на пользовательские с помощью утилиты klsetsrvcert (см. раздел "Сценарий: задание пользовательского сертификата Сервера администрирования" на стр. [78](#)) или в Консоли администрирования в свойствах Сервера администрирования, в зависимости от типа сертификата. При использовании утилиты klsetsrvcert необходимо указать тип сертификата, используя одно из следующих значений:

- C – общий сертификат для портов 13000 и 13291;
- CR – общий резервный сертификат для портов 13000 и 13291;
- M – мобильный сертификат для порта 13292;
- MR – мобильный резервный сертификат для порта 13292;
- MCA – мобильный сертификат, полученный от аккредитованного центра сертификации для автоматической генерации пользовательских сертификатов.

Вам не нужно загружать утилиту klsetsrvcert. Утилита входит в состав комплекта поставки Kaspersky Security Center. Утилита несовместима с предыдущими версиями Kaspersky Security Center.

Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

Сертификаты Сервера администрирования

Сертификат Сервера администрирования необходим для аутентификации Сервера администрирования, а также для безопасного взаимодействия Сервера администрирования и Агента администрирования на управляемых устройствах или между главным Сервером администрирования и подчиненными Серверами. При первом подключении Консоли администрирования к Серверу администрирования вам будет предложено подтвердить использование текущего сертификата Сервера администрирования. Такое подтверждение также требуется при каждой замене сертификата Сервера администрирования, после каждой переустановки Сервера администрирования и при подключении подчиненного Сервера администрирования к главному Серверу администрирования. Этот сертификат называется общим ("C").

Общий сертификат ("C") создается автоматически при установке компонента Сервера администрирования. Сертификат состоит из двух частей:

- Файл klserver.cer; по умолчанию он находится на устройстве, на котором установлен компонент Сервера администрирования, в папке C:\ProgramData\KasperskyLab\adminkit\1093\cert.
- Секретный ключ находится в защищенном хранилище Windows (Windows Protected Storage).

Также существует общий резервный сертификат ("CR"). Kaspersky Security Center автоматически генерирует этот сертификат за 90 дней до истечения срока действия общего сертификата. Общий резервный сертификат впоследствии используется для замены сертификата Сервера администрирования. Когда истекает срок действия общего сертификата, общий резервный сертификат используется для поддержания связи с экземплярами Агента администрирования, установленными на управляемых устройствах. С этой целью общий резервный сертификат автоматически становится новым общим сертификатом за 24 часа до истечения срока действия старого общего сертификата.

Вы также можете создать резервную копию сертификата Сервера администрирования отдельно от других параметров Сервера администрирования, чтобы перенести Сервер администрирования с одного устройства на другое без потери данных.

Мобильные сертификаты

Мобильный сертификат ("M") необходим для аутентификации Сервера администрирования на мобильных устройствах. Вы настраиваете использование мобильного сертификата на шаге мастера первоначальной настройки.

Также существует мобильный резервный сертификат ("MR"): он используется для замены мобильного сертификата. Kaspersky Security Center автоматически генерирует этот сертификат за 60 дней до истечения срока действия общего сертификата. Когда истекает срок действия мобильного сертификата, мобильный резервный сертификат используется для поддержания связи с Агентами администрирования, установленными на управляемых мобильных устройствах. С этой целью мобильный резервный сертификат автоматически становится новым мобильным сертификатом за 24 часа до истечения срока действия старого мобильного сертификата.

Если сценарий подключения требует использования сертификата клиента на мобильных устройствах (подключение с двусторонней SSL-аутентификация), вы генерируете эти сертификаты с помощью доверенного центра сертификации для автоматически сгенерированных пользовательских сертификатов ("MCA"). Кроме того, мастер первоначальной настройки позволяет вам начать использовать

пользовательские сертификаты, выпущенные другим аккредитованным центром сертификации, а интеграция с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

сертификат Сервера iOS MDM;

Сертификат Сервера iOS MDM необходим для аутентификации Сервера администрирования на мобильных устройствах под управлением операционной системы iOS. Взаимодействие с этими устройствами осуществляется через протокол Apple Mobile Device Management (MDM), в котором не используется Агент администрирования. Вместо этого вы устанавливаете специальный iOS MDM-профиль, содержащий клиентский сертификат, на каждом устройстве, чтобы обеспечить двустороннюю SSL-аутентификацию.

Кроме того, мастер первоначальной настройки позволяет вам начать использовать пользовательские сертификаты, выпущенные другим аккредитованным центром сертификации, а интеграция с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

Клиентские сертификаты передаются на устройства iOS, когда вы загружаете эти iOS MDM-профили. Пользовательский сертификат Сервера iOS MDM уникален для каждого управляемого устройства iOS. Вы генерируете все клиентские сертификаты Сервера iOS MDM с помощью аккредитованного центра сертификации для автоматически сгенерированных пользовательских сертификатов ("MCA").

сертификат Веб-сервера Kaspersky Security Center;

Специальный тип сертификата использует Веб-сервер Kaspersky Security Center (далее также Веб-сервер) – компонент Сервера администрирования Kaspersky Security Center. Этот сертификат необходим для публикации инсталляционных пакетов Агента администрирования, которые вы впоследствии загружаете на управляемые устройства, а также для публикации iOS MDM-профилей, приложений iOS и инсталляционных пакетов Kaspersky Security для мобильных устройств. Для этого Веб-сервер может использовать различные сертификаты.

Если поддержка мобильных устройств отключена, Веб-сервер использует один из следующих сертификатов в порядке приоритета:

1. Пользовательский сертификат Веб-сервера, который вы указали вручную с помощью Консоли администрирования.
2. Общий сертификат Сервера администрирования ("C").

Если поддержка мобильных устройств включена, Веб-сервер использует один из следующих сертификатов в порядке приоритета:

1. Пользовательский сертификат Веб-сервера, который вы указали вручную с помощью Консоли администрирования.
2. Пользовательский мобильный сертификат.
3. Самоподписанный мобильный сертификат ("M").
4. Общий сертификат Сервера администрирования ("C").

Сертификат Kaspersky Security Center Web Console

Сервер Kaspersky Security Center Web Console (далее также Web Console) имеет собственный сертификат. Когда вы открываете сайт, браузер проверяет, является ли ваше соединение надежным. Сертификат Web Console позволяет аутентифицировать Web Console и используется для шифрования трафика между браузером и Web Console.

Когда вы открываете Web Console, браузер может информировать вас о том, что подключение к Web Console не является приватным и что сертификат Web Console недействителен. Это предупреждение

появляется потому, что сертификат Kaspersky Security Center Web Console является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить это предупреждение, можно выполнить одно из следующих действий:

- Заменить сертификат Kaspersky Security Center Web Console на пользовательский сертификат (рекомендуемый параметр). Создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам (см. раздел "Требования к пользовательским сертификатам, используемым в Kaspersky Security Center" см. стр. [76](#)).
- Добавить сертификат Web Console в список доверенных сертификатов браузера. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.

См. также:

Требования к пользовательским сертификатам, используемым в Kaspersky Security Center	76
Сценарий: задание пользовательского сертификата Сервера администрирования	78
Основной сценарий установки.....	56
Аутентификация Сервера при подключении Консоли администрирования	708
Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования	111
Резервное копирование и восстановление данных в интерактивном режиме	725
Мастер первоначальной настройки Сервера администрирования.....	281
Веб-сервер	43

О сертификате Сервера администрирования

Выполняются две операции с использованием *сертификата Сервера администрирования*: аутентификация Сервера администрирования при подключении Консоли администрирования и обмен данными с устройствами. Сертификат используется также для аутентификации, когда главные Серверы администрирования подключены к подчиненным Серверам администрирования.

Сертификаты, выписанные "Лабораторией Касперского"

Сертификат Сервера администрирования автоматически создается при установке компонента Сервер администрирования и хранится в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\admindkit\1093\cert.

Сертификат Сервера администрирования действителен в течение пяти лет, если сертификат был сгенерирован Сервером администрирования версии 12.2 или более ранней. В противном случае срок действия сертификата ограничен 397 днями. Новый сертификат генерируется Сервером администрирования как резервный сертификат, за 90 дней до срока окончания действия текущего сертификата. Затем новый сертификат автоматически замещает текущий сертификат за один день до окончания его срока действия. Все Агенты администрирования на клиентских устройствах автоматически настраиваются на аутентификацию с Сервером администрирования с использованием нового сертификата.

Пользовательские сертификаты

При необходимости можно назначить Серверу администрирования пользовательский сертификат. Например, это может понадобиться для лучшей интеграции с существующей PKI вашей организации или для требуемой настройки полей сертификата.

Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "Ошибка аутентификации Сервера администрирования". Чтобы устранить эту ошибку, вам потребуется восстановить соединение после замены сертификата (см. раздел "Сценарий: задание пользовательского сертификата Сервера администрирования" на стр. [78](#)).

В случае если сертификат Сервера администрирования утерян, для его восстановления необходимо провести переустановку компонента Сервер администрирования и восстановление данных (см. раздел "Резервное копирование и восстановление данных Сервера администрирования" на стр. [723](#)).

Требования к пользовательским сертификатам, используемым в Kaspersky Security Center

В таблице ниже представлены требования к пользовательским сертификатам, предъявляемые к различным компонентам Kaspersky Security Center (см. раздел "О сертификатах Kaspersky Security Center" см. стр. [72](#)).

Таблица 11. Требования для сертификатов Kaspersky Security Center

Тип сертификата	Требования	Комментарии
Общий сертификат, Общий резервный сертификат ("C", "CR")	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Отсутствует. Используемые ключи: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация Сервера, аутентификация клиента.	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом, отличным от "None", но не должно быть меньше 1.

Тип сертификата	Требования	Комментарии
Мобильный сертификат, Мобильный резервный сертификат ("M", "MR")	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Отсутствует. Используемые ключи: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (EKU) (необязательно): аутентификация Сервера.	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом, отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1.
Сертификат, выпущенный аккредитованным центром сертификации (CA), для автоматически генерируемых пользовательских сертификатов (MCA)	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Отсутствует. Используемые ключи: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация Сервера, аутентификация клиента.	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1.
Сертификат Веб-сервера	Расширенное использование ключа (EKU): аутентификация Сервера. Контейнер PKCS #12 / PEM, из которого указывается сертификат, включает всю цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля <code>subjectAltName</code> является допустимым. Сертификат соответствует действующим требованиям браузеров, предъявляемым к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	—

Тип сертификата	Требования	Комментарии
Сертификат Kaspersky Security Center Web Console	Контейнер PEM, из которого указывается сертификат, включает всю цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля <code>subjectAltName</code> является допустимым. Сертификат соответствует действующим требованиям браузеров к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	Зашифрованные сертификаты не поддерживаются Kaspersky Security Center Web Console.

См. также:

О сертификате Сервера администрирования.....	75
Сценарий: задание пользовательского сертификата Сервера администрирования.....	78
Основной сценарий установки.....	56

Сценарий: задание пользовательского сертификата Сервера администрирования

Вы можете назначить пользовательский сертификат Сервера администрирования, например, для лучшей интеграции с существующей инфраструктурой открытых ключей (PKI) вашей организации или для пользовательской конфигурации параметров сертификата. Целесообразно заменять сертификат сразу после инсталляции Сервера администрирования, до завершения работы мастера первоначальной настройки.

Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

Предварительные требования

Новый сертификат должен быть создан в формате PKCS#12 (например, с помощью PKI организации) и должен быть выпущен доверенным центром сертификации (CA). Также новый сертификат должен включать в себя всю цепочку доверия и закрытый ключ, который должен храниться в файле с расширением `pfx` или `p12`. Для нового сертификата должны быть соблюдены требования, перечисленные в таблице ниже.

Таблица 12. Требования к сертификатам Сервера администрирования

Тип сертификата	Требования
Общий сертификат, общий резервный сертификат ("C", "CR")	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Отсутствует. Значение ограничения длины пути может быть целым числом отличным от "None", но не меньше 1. Используемые ключи: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (Extended Key Usage, ECU) (необязательно): аутентификация Сервера и аутентификация клиента. ECU необязательно, но если оно содержится в вашем сертификате, данные аутентификации Сервера и клиента должны быть указаны в ECU.
Мобильный сертификат, мобильный резервный сертификат ("M", "MR")	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Отсутствует. Значение ограничения длины пути может быть целым числом, отличным от "None", если общий сертификат имеет значение ограничения длины пути не менее 1. Используемые ключи: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (ECU): аутентификация Сервера. ECU необязательно, но если оно содержится в вашем сертификате, данные аутентификации Сервера должны быть указаны в ECU.

Тип сертификата	Требования
Сертификат, выпущенный аккредитованным центром сертификации (CA), для автоматически генерируемых пользовательских сертификатов (MCA)	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Отсутствует. Значение ограничения длины пути может быть целым числом, отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1. Используемые ключи: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (англ. Extended Key Usage, ECU): аутентификация клиента. ECU необязателен, но если он содержится в вашем сертификате, данные аутентификации клиента должны быть указаны в ECU.

Сертификаты, выпущенные доверенным центром сертификации (англ. certificate authority, CA), не имеют разрешения на подписывание сертификатов. Чтобы использовать такие сертификаты, убедитесь, что на точках распространения или шлюзах соединения в вашей сети установлен Агент администрирования версии 13 или выше. В противном случае вы не сможете использовать сертификаты без разрешения на подпись.

Этапы

Указание сертификата Сервера администрирования состоит из следующих этапов:

а. Замена сертификата Сервера администрирования

Используйте для этой цели утилиту командной строки `klsetsrvcert` (см. раздел "Замена сертификата Сервера администрирования с помощью утилиты `klsetsrvcert`" на стр. [81](#)).

б. Указание нового сертификата и восстановление связи Агентов администрирования с Сервером администрирования

При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "Ошибка аутентификации Сервера администрирования". Чтобы указать новый сертификат и восстановить соединение, используйте командную строку утилиты `klmover` (см. раздел "Подключение Агентов администрирования к Серверу администрирования с помощью утилиты `klmover`" на стр. [83](#)).

с. Указание нового сертификата в параметрах Kaspersky Security Center Web Console

После замены сертификата укажите это в параметрах Kaspersky Security Center Web Console. Иначе Kaspersky Security Center Web Console не сможет подключиться к Серверу администрирования.

Результаты

После завершения сценария сертификат Сервера администрирования будет заменен, Сервер Агент администрирования на управляемых устройствах аутентифицирует Сервер с использованием нового сертификата.

См. также:

О сертификатах Kaspersky Security Center.....	72
О сертификате Сервера администрирования.....	75
Требования к пользовательским сертификатам, используемым в Kaspersky Security Center	76
Основной сценарий установки.....	56

Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert

► Чтобы заменить сертификат Сервера администрирования:

В командной строке выполните следующую команду:

```
klsetsrvcert [-t <type> {-i <inputfile> [-p <password>] [-o <chkopt>] |  
-g <dnsname>}] [-f <time>] [-r <calistfile>] [-l <logfile>]
```

Вам не нужно загружать утилиту klsetsrvcert. Утилита входит в состав комплекта поставки Kaspersky Security Center. Она несовместима с предыдущими версиями Kaspersky Security Center.

Описание параметров утилиты klsetsrvcert представлено в таблице ниже.

Таблица 13. Значения параметров утилиты klsetsrvcert

Параметр	Значение
-t <type>	Тип сертификата, который следует заменить. Возможные значения параметра <type>: - С – заменить общий сертификат для портов 13000 и 13291. - CR – заменить общий резервный сертификат для портов 13000 и 13291. - М – заменить сертификат для мобильных устройств порта 13292. - MR – заменить мобильный резервный сертификат для порта 13292. - MCA – мобильный сертификат, полученный от аккредитованного центра сертификации для автоматической генерации пользовательских сертификатов.
-f <time>	Расписание замены сертификата использует формат "ДД-ММ-ГГГГ ЧЧ:ММ" (для портов 13000 и 13291). Используйте этот параметр, если вы хотите заменить общий или общий резервный сертификат до истечения срока его действия. Укажите время, когда управляемые устройства должны синхронизироваться с Сервером администрирования с использованием нового сертификата.
-i <inputfile>	Контейнер с сертификатом и закрытый ключ в формате PKCS#12 (файл с расширением p12 или pfx).
-p <password>	Пароль, при помощи которого защищен p12-контейнер. Сертификат и закрытый ключ хранятся в контейнере, поэтому для расшифровки файла с контейнером требуется пароль.
-o <chkopt>	Параметры проверки сертификата (разделенные точкой с запятой). Чтобы использовать пользовательский сертификат без разрешения на подпись, в утилите klsetsrvcert укажите -o NoCA. Это полезно для сертификатов, выпущенных доверенным центром сертификации (англ. certificate authority, CA). Чтобы изменить длину ключа шифрования для сертификатов типа С или CR, укажите -o RsaKeyLen:<key length> в утилите klsetsrvcert, где параметр <key length> – это требуемая длина ключа. Иначе используется текущая длина ключа сертификата.
-g <dnsname>	Сертификат будет создан с указанным DNS-именем.
-r <calistfile>	Список доверенных корневых сертификатов, подписанных доверенным центром сертификации, в формате PEM.
-l <logfile>	Файл вывода результатов. По умолчанию вывод осуществляется в стандартный поток вывода.

Например, для указания пользовательского сертификата Сервера администрирования (см. раздел "О сертификатах Kaspersky Security Center" см. стр. [72](#)), используйте следующую команду:

```
klsetsrvcert -t C -i <inputfile> -p <password> -o NoCA
```

После замены сертификата все Агенты администрирования, подключенные к Серверу администрирования по протоколу SSL, теряют связь. Чтобы восстановить связь, используйте командную строку утилиты klmove (см. раздел "Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmove" на стр. [83](#)).

Чтобы не потерять соединения Агентов администрирования, используйте следующие команды:

1. Чтобы установить новый сертификат,

```
klsetsrvcert.exe -t CR -i <inputfile> -p <password> -o NoCA
```

2. Чтобы указать дату применения нового сертификата,

```
klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
```

где дата "DD-MM-YYYY hh:mm" на 3–4 недели больше текущей. Сдвиг времени замены сертификата на новый позволит распространить новый сертификат на все Агенты администрирования.

См. также:

Сценарий: задание пользовательского сертификата Сервера администрирования [78](#)

Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover

После замены сертификата Сервера администрирования с помощью утилиты командной строки klsetsrvcert (см. раздел "Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert" на стр. [81](#)) вам необходимо установить SSL-соединение между Агентами администрирования и Сервером администрирования, так как соединение разорвано.

- Чтобы указать новый сертификат Сервера администрирования и восстановить соединение:

В командной строке выполните следующую команду:

```
klmover [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossll] [-cert <путь к файлу сертификата>]
```

Для запуска утилиты требуются права администратора.

Эта утилита автоматически копируется в папку установки Агента администрирования при установке Агента администрирования на клиентское устройство.

Чтобы злоумышленники не могли вывести устройства из-под контроля вашего Сервера администрирования, настоятельно рекомендуется включить защиту паролем для запуска утилиты klmover. Чтобы включить защиту паролем, в параметрах политики Агента администрирования выберите параметр **Использовать пароль деинсталляции**.

Утилита klmover требует прав локального администратора. Защиту паролем для запуска утилиты klmover можно не устанавливать для устройств, работающих без прав локального администратора.

При включении параметра **Использовать пароль деинсталляции** также включается защита паролем средствами Cleaner (cleaner.exe).

Описание параметров утилиты klmover представлено в таблице ниже.

Таблица 14. Значения параметров утилиты klmover

Параметр	Значение
-address <адрес Сервера>	Адрес Сервера администрирования для подключения. В качестве адреса можно указать IP-адрес, NetBIOS- или DNS-имя.
-pn <номер порта>	Номер порта, по которому будет осуществляться незашифрованное подключение к Серверу администрирования. По умолчанию установлен порт 14000.
-ps <номер SSL-порта>	Номер SSL-порта, по которому осуществляется зашифрованное подключение к Серверу администрирования с использованием протокола SSL. По умолчанию установлен порт 13000.
-noss1	Использовать незашифрованное подключение к Серверу администрирования. Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному SSL-протоколу.
-cert <путь к файлу сертификата>	Использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования.
-virtserv	Имя виртуального Сервера администрирования.
-cloningmode	Режим клонирования диска Агента администрирования. Используйте один из следующих параметров для настройки режима клонирования диска: -cloningmode – запрос состояния режима клонирования диска. -cloningmode 1 – включить режим клонирования диска. -cloningmode 0 – выключить режим клонирования диска.

Например, чтобы подключить Агент администрирования к Серверу администрирования, выполните следующую команду:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

См. также:

Сценарий: задание пользовательского сертификата Сервера администрирования[78](#)

Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover ..[750](#)

Перевыпуск сертификата Веб-сервера

Сертификат Веб-сервера используемый в Kaspersky Security Center необходим для публикации инсталляционных пакетов Агента администрирования, которые вы впоследствии загружаете на управляемые устройства, а также для публикации iOS MDM-профилей, приложений для iOS и инсталляционных пакетов Kaspersky Security для мобильных устройств. В зависимости от текущей конфигурации приложения в качестве сертификата Веб-сервера могут использоваться различные сертификаты (подробнее см. О сертификатах Kaspersky Security Center (см. стр. [72](#))).

Вам может потребоваться перевыпустить сертификат Веб-сервера, чтобы обеспечить соответствие требованиям безопасности вашей организации или для поддержания постоянного соединения ваших управляемых устройств перед началом обновления приложения (см. раздел "Обновление предыдущей версии Kaspersky Security Center" см. стр. 276). Kaspersky Security Center предоставляет два способа перевыпуска сертификата Веб-сервера. Выбор между двумя способами зависит от того, подключены ли у вас мобильные устройства и управляются ли они через мобильный протокол (то есть с помощью мобильного сертификата).

Если вы никогда не указывали пользовательский сертификат в качестве сертификата Веб-сервера в окне **Веб-сервер** свойств Сервера администрирования, мобильный сертификат действует как сертификат Веб-сервера. В этом случае перевыпуск сертификата Веб-сервера выполняется путем перевыпуска самого мобильного протокола.

► Чтобы перевыпустить сертификат Веб-сервера, когда у вас нет мобильных устройств, управляемых через мобильный протокол:

1. В дереве консоли, в контекстном меню требуемого Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервер администрирования выберите раздел **Параметры подключения к Серверу администрирования**.
3. В списке подразделов выберите подраздел **Сертификаты**.
4. Если вы планируете и дальше использовать сертификат, выданный Kaspersky Security Center:
 - a. В группе параметров **Аутентификация Сервера администрирования мобильными устройствами** выберите параметр **Сертификат выпущен средствами Сервера администрирования** и нажмите на кнопку **Перевыпустить**.
 - b. В открывшемся окне **Перевыпуск сертификата** в группе параметров **Адрес подключения и Срок активации** выберите соответствующие параметры и нажмите на кнопку **ОК**.
 - c. В появившемся окне нажмите на кнопку **Да**.

Если вы планируете использовать собственный сертификат, выполните следующее:

- d. Проверьте, соответствует ли ваш пользовательский сертификат требованиям Kaspersky Security Center (см. раздел "Требования к пользовательским сертификатам, используемым в Kaspersky Security Center" см. стр. 76) и требованиям к доверенным сертификатам Apple <https://support.apple.com/en-us/HT210176>. При необходимости измените сертификат.
- e. Выберите параметр **Другой сертификат** и нажмите на кнопку **Обзор**.
- f. В открывшемся окне **Сертификат** в поле **Тип сертификата** выберите тип вашего сертификата и укажите расположение сертификата и параметры:
 - Если вы выбрали **Контейнер PKCS#12**, нажмите на кнопку **Обзор** рядом с полем **Файл сертификата** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль (если есть)**.
 - Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ (.prk, .pem)** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль (если есть)**. Нажмите на кнопку **Обзор** рядом с полем **Открытый ключ (.cer)** и укажите открытый ключ на жестком диске.
- g. В окне **Сертификат** нажмите на кнопку **ОК**.

h. В появившемся окне нажмите на кнопку **Да**.

Мобильный сертификат перевыпущен для использования в качестве сертификата Веб-сервера.

► *Чтобы перевыпустить сертификат Веб-сервера, когда у вас есть мобильные устройства, управляемые через мобильный протокол:*

1. Создайте пользовательский сертификат и подготовьте его для использования в Kaspersky Security Center. Проверьте, соответствует ли ваш пользовательский сертификат требованиям Kaspersky Security Center (см. раздел "Требования к пользовательским сертификатам, используемым в Kaspersky Security Center" см. стр. [76](#)) и требованиям к доверенным сертификатам Apple <https://support.apple.com/en-us/HT210176>. При необходимости измените сертификат.

Для создания сертификата можно использовать утилиту `kliossrvcertgen.exe`
<https://support.kaspersky.com/10890#block1>.

2. В дереве консоли, в контекстном меню требуемого Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервер администрирования выберите раздел **Веб-сервер**.
4. В меню **По протоколу HTTPS** выберите параметр **Задать другой сертификат**.
5. В меню **По протоколу HTTPS** нажмите на кнопку **Изменить**.
6. В открывшемся окне **Сертификат** в поле **Тип сертификата** выберите тип вашего сертификата:
 - Если вы выбрали **Контейнер PKCS#12**, нажмите на кнопку **Обзор** рядом с полем **Файл сертификата** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль (если есть)**.
 - Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ (.prk, .pem)** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль (если есть)**. Нажмите на кнопку **Обзор** рядом с полем **Открытый ключ (.cer)** и укажите открытый ключ на жестком диске.
7. В окне **Сертификат** нажмите на кнопку **ОК**.
8. При необходимости в окне свойств Сервера администрирования в поле **HTTPS-порт Веб-сервера** измените номер HTTPS-порта для Веб-сервера. Нажмите на кнопку **ОК**.

Сертификат Веб-сервера перевыпущен.

Схемы трафика данных и использования портов

В этом разделе приведены схемы трафика данных между компонентами Kaspersky Security Center, управляемыми приложениями безопасности и внешними серверами для различных конфигураций. Схемы содержат номера портов, которые должны быть доступны на локальных устройствах.

В этом разделе

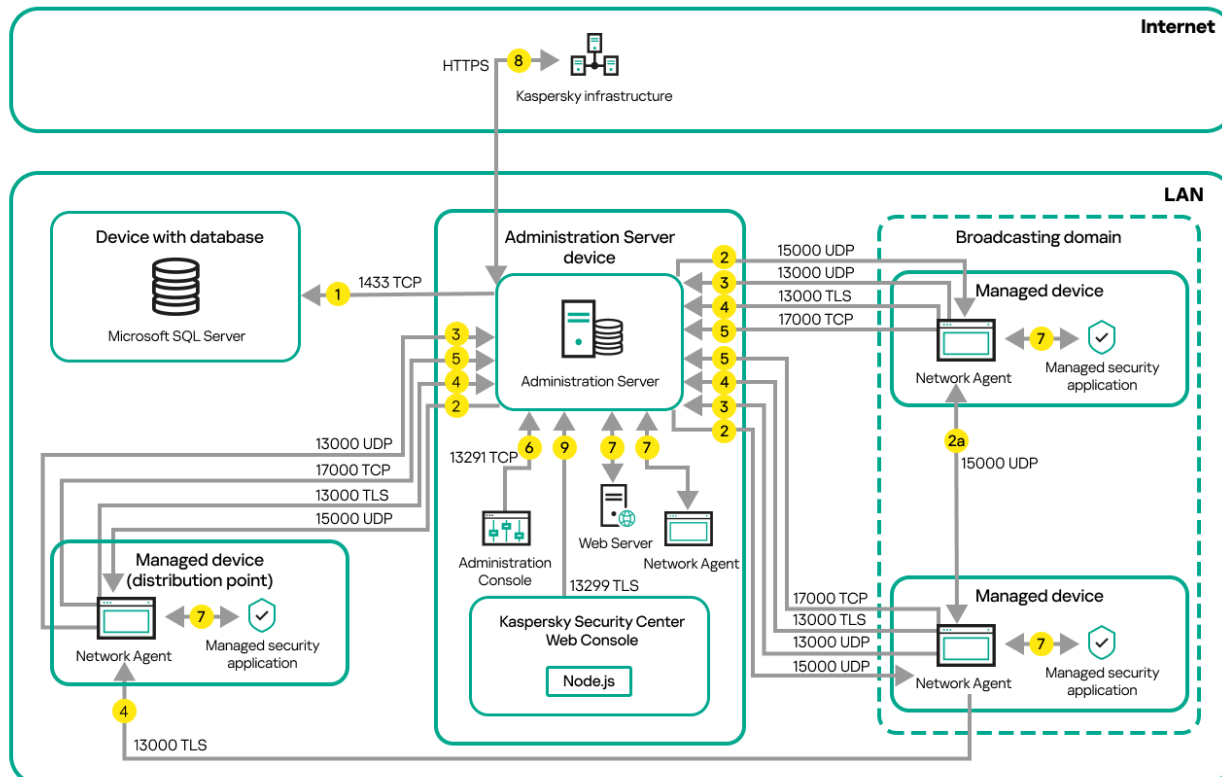
Сервер администрирования и управляемые устройства в локальной сети (LAN).....	88
Главный Сервер администрирования в локальной сети (LAN) и два подчиненных Сервера администрирования	90
Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование обратного прокси-сервера	93
Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения.....	96
Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете	101
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104

См. также:

Основной сценарий установки	56

Сервер администрирования и управляемые устройства в локальной сети (LAN)

На рисунке ниже показан трафик данных, если Kaspersky Security Center развернут только в локальной сети (LAN).



На рисунке показано как разные управляемые устройства подключаются к Серверу администрирования различными способами: напрямую или с помощью точки распространения. Точки распространения уменьшают нагрузку на Сервер администрирования при распространении обновлений и для оптимизации трафика в сети. Однако точки распространения нужны только в том случае, если количество управляемых устройств достаточно велико (см. раздел "Расчет количества и конфигурации точек распространения" на стр. [149](#)). Если количество управляемых устройств мало, все управляемые устройства могут получать обновления непосредственно с Сервера администрирования.

Стрелки указывают направление трафика: каждая стрелка проведена от устройства, которое инициирует соединение, к устройству, которое "отвечает" на вызов. Указаны номер порта и название протокола, используемые для передачи данных. Каждая стрелка пронумерована и содержит следующую информацию о соответствующем трафике данных:

1. Сервер администрирования передает данные в базу данных (см. раздел "Сервер администрирования и СУБД" на стр. [106](#)). Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000 (см. раздел "Сервер администрирования и клиентское устройство: Управление приложением безопасности" на стр. [108](#)).

Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).

Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь с Сервером администрирования на эти устройства не отправляются напрямую.

3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. раздел "Сервер администрирования и клиентское устройство: Управление приложением безопасности" на стр. [108](#)) и от подчиненных Серверов администрирования (см. раздел "Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования" на стр. [111](#)) через TLS-порт 13000.

Если вы используете Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключение от Агентов администрирования по не TLS-порту 14000. Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, но рекомендуется использовать TLS-порт 13000.

Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.
6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291 (см. раздел "Сервер администрирования и Консоль администрирования" на стр. [107](#)). Консоль администрирования может быть установлена на том же устройстве или на другом.
7. Приложения на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно управлять этими данными вручную.

9. Сервер Kaspersky Security Center Web Console передает данные на Сервер администрирования, который может быть установлен на том же устройстве или на другом, через TLS-порт 13299 (см. раздел "Сервер администрирования и Kaspersky Security Center Web Console" на стр. [115](#)).

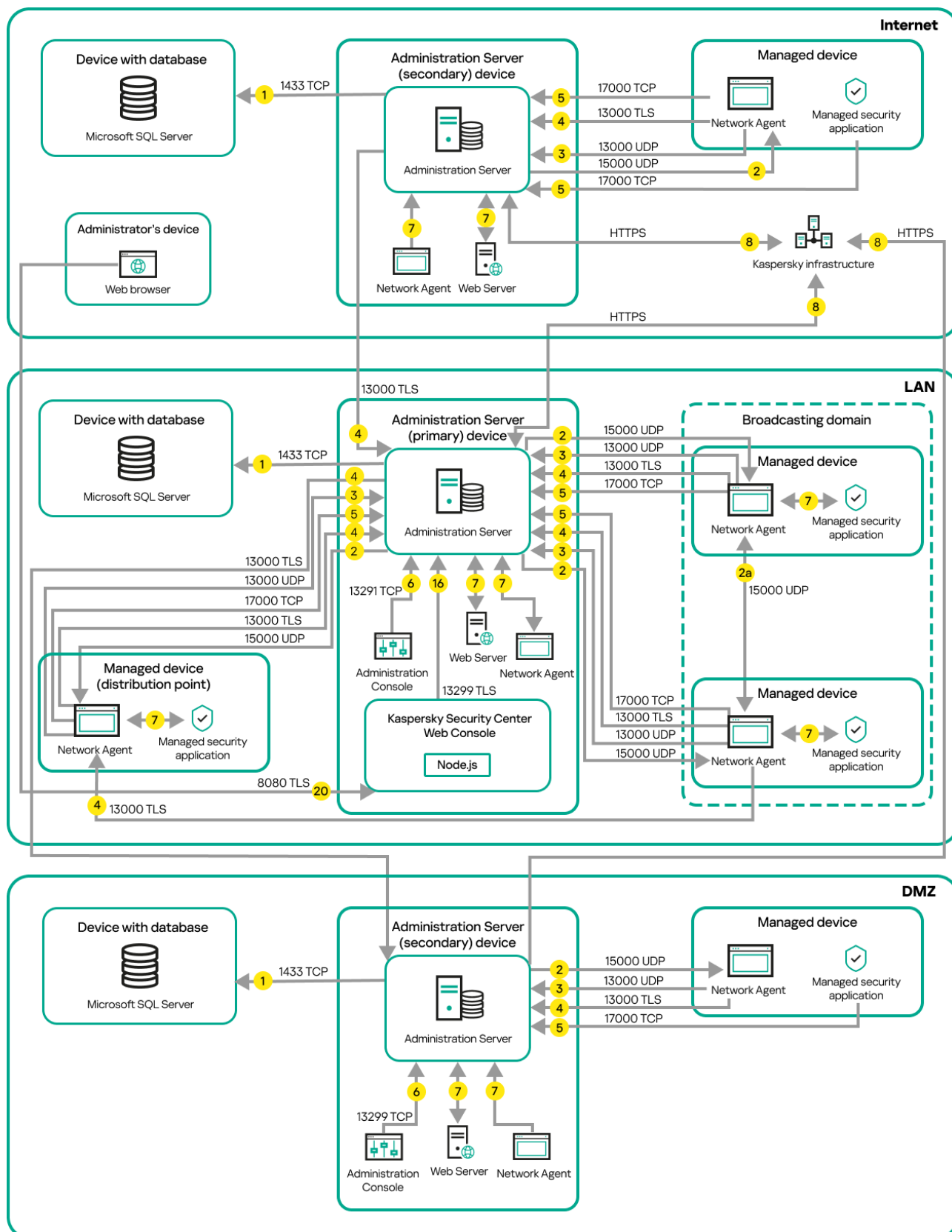
См. также:

Типовая конфигурация: один офис	137
Порты, используемые Kaspersky Security Center	63

Главный Сервер администрирования в локальной сети (LAN) и два подчиненных Сервера администрирования

На рисунке показана иерархия Серверов администрирования: главный Сервер администрирования расположен внутри локальной сети (LAN). Подчиненный Сервер администрирования находится в

демилитаризованной зоне (DMZ); другой подчиненный Сервер администрирования расположен в интернете.



Стрелки указывают направление трафика: каждая стрелка проведена от устройства, которое инициирует соединение, к устройству, которое "отвечает" на вызов. Указаны номер порта и название протокола, используемые для передачи данных. Каждая стрелка пронумерована и содержит следующую информацию о соответствующем трафике данных:

1. Сервер администрирования передает данные в базу данных (см. раздел "Сервер администрирования и СУБД" на стр. [106](#)). Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000 (см. раздел "Сервер администрирования и клиентское устройство: Управление приложением безопасности" на стр. [108](#)).

Агенты администрирования отправляют запросы друг другу в пределах одного широковебательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковебательного домена и для автоматического назначения точек распространения (если этот параметр включен).

Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь с Сервером администрирования на эти устройства не отправляются напрямую.

3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. раздел "Сервер администрирования и клиентское устройство: Управление приложением безопасности" на стр. [108](#)) и от подчиненных Серверов администрирования (см. раздел "Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования" на стр. [111](#)) через TLS-порт 13000.

Если вы используете Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключение от Агентов администрирования по не TLS-порту 14000. Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, но рекомендуется использовать TLS-порт 13000.

Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.
6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291 (см. раздел "Сервер администрирования и Консоль администрирования" на стр. [107](#)). Консоль администрирования может быть установлена на том же устройстве или на другом.
7. Приложения на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно управлять этими данными вручную.

9. Сервер Kaspersky Security Center Web Console передает данные на Сервер администрирования, который может быть установлен на том же устройстве или на другом, через TLS-порт 13299.

9а. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080 (см. раздел "Сервер администрирования и Kaspersky Security Center Web Console" на стр. [115](#)). Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

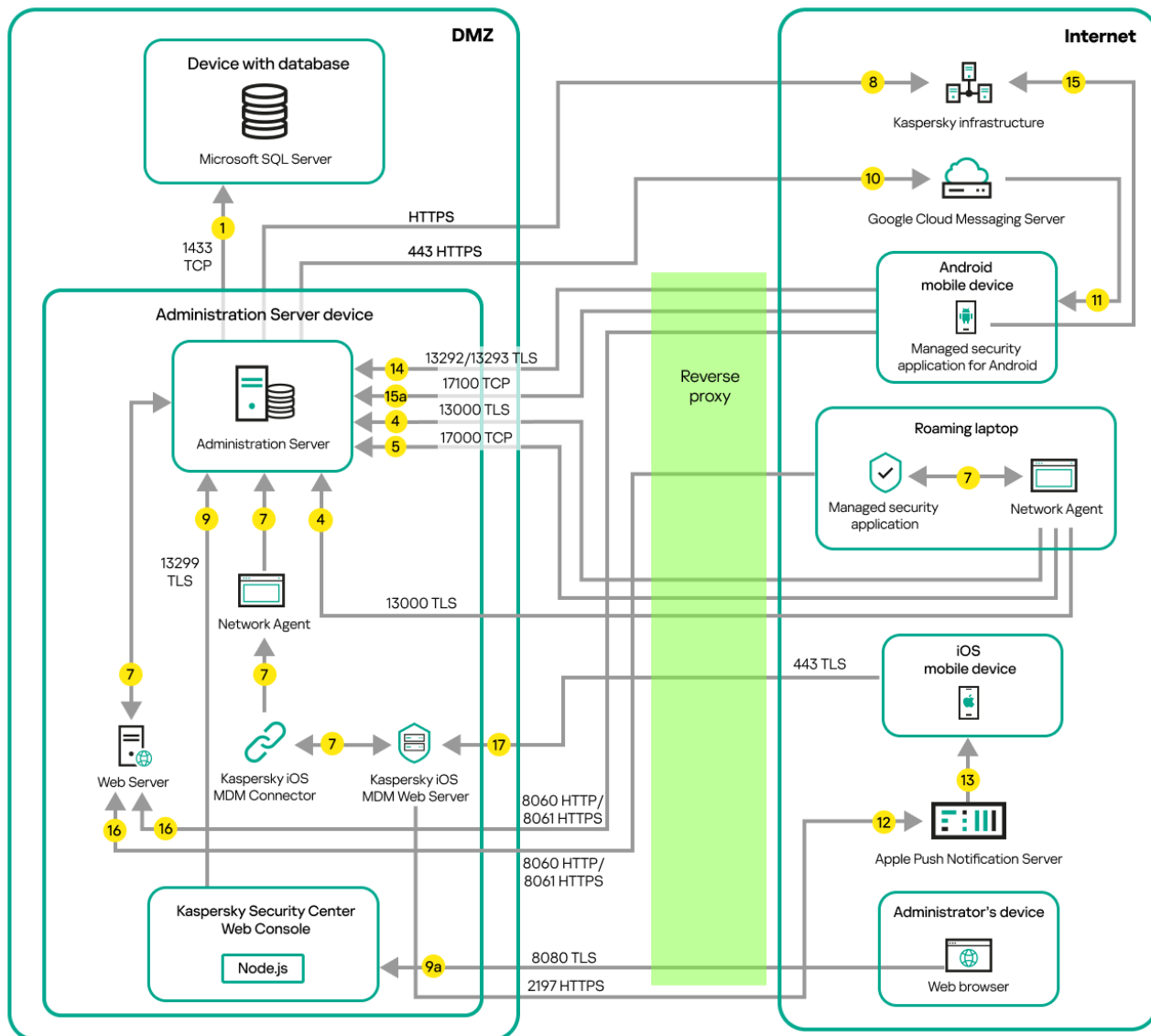
См. также:

Иерархия Серверов администрирования.....	150
Порты, используемые Kaspersky Security Center.....	63

Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование обратного прокси-сервера

На рисунке ниже показан трафик данных, когда Сервер администрирования находится внутри локальной сети (LAN), а управляемые устройства, включая мобильные устройства, находятся в интернете. На рисунке

ниже используется выбранный вами обратный прокси-сервер. Дополнительную информацию см. в документации к приложению.



Эта схема разворачивания рекомендуется, если вы не хотите, чтобы мобильные устройства подключались напрямую к Серверу администрирования, и не хотите назначать шлюз соединения в демилитаризованной зоне (DMZ).

Стрелки указывают направление трафика: каждая стрелка проведена от устройства, которое инициирует соединение, к устройству, которое "отвечает" на вызов. Указаны номер порта и название протокола, используемые для передачи данных. Каждая стрелка пронумерована и содержит следующую информацию о соответствующем трафике данных:

1. Сервер администрирования передает данные в базу данных (см. раздел "Сервер администрирования и СУБД" на стр. [106](#)). Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.

2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000 (см. раздел "Сервер администрирования и клиентское устройство: Управление приложением безопасности" на стр. [108](#)).

Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).

Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь с Сервером администрирования на эти устройства не отправляются напрямую.

3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. раздел "Сервер администрирования и клиентское устройство: Управление приложением безопасности" на стр. [108](#)) и от подчиненных Серверов администрирования (см. раздел "Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования" на стр. [111](#)) через TLS-порт 13000.

Если вы используете Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключение от Агентов администрирования по не TLS-порту 14000. Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, но рекомендуется использовать TLS-порт 13000.

Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.
6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291 (см. раздел "Сервер администрирования и Консоль администрирования" на стр. [107](#)). Консоль администрирования может быть установлена на том же устройстве или на другом.
7. Приложения на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно управлять этими данными вручную.

9. Сервер Kaspersky Security Center Web Console передает данные на Сервер администрирования, который может быть установлен на том же устройстве или на другом, через TLS-порт 13299.

9а. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080 (см. раздел "Сервер администрирования и Kaspersky Security Center Web Console" на стр. [115](#)). Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

10. Только для мобильных устройств Android: данные от Сервера администрирования передаются службам Google. Это соединение используется для уведомления мобильных устройств Android о том, что требуется их подключение к Серверу администрирования. Затем push-уведомления отправляются на мобильные устройства.
11. Только для мобильных устройств Android: push-уведомления от серверов Google отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств о том, что требуется их подключение к Серверу администрирования.
12. Только для мобильных устройств iOS: данные от Сервера iOS MDM передаются на серверы Apple Push Notification. Затем push-уведомления отправляются на мобильные устройства.
13. Только для мобильных устройств iOS: push-уведомления от серверов Apple отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств iOS о том, что требуется их подключение к Серверу администрирования.
14. Только для мобильных устройств: управляемое приложение передает данные на Сервер администрирования через TLS-порт 13292/13293 (см. раздел "Активация и управление приложением безопасности на мобильном устройстве" на стр. [116](#)) напрямую или через обратный прокси-сервер.
15. Только для мобильных устройств: данные от мобильного устройства передаются к инфраструктуре "Лаборатории Касперского".

15а. Если мобильное устройство не имеет доступа в интернет, данные передаются на Сервер администрирования через порт 17100 (см. раздел "Активация и управление приложением безопасности на мобильном устройстве" на стр. [116](#)), а Сервер администрирования передает их инфраструктуре "Лаборатории Касперского". Однако этот сценарий используется очень редко.
16. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер (на стр. [43](#)), который находится на том же устройстве, на котором установлен Сервер администрирования.
17. Только для мобильных устройств iOS: данные от мобильных устройств передаются по TLS-порту 443 на Сервер iOS MDM, который находится на том же устройстве, на котором установлен Сервер администрирования или шлюз соединения.

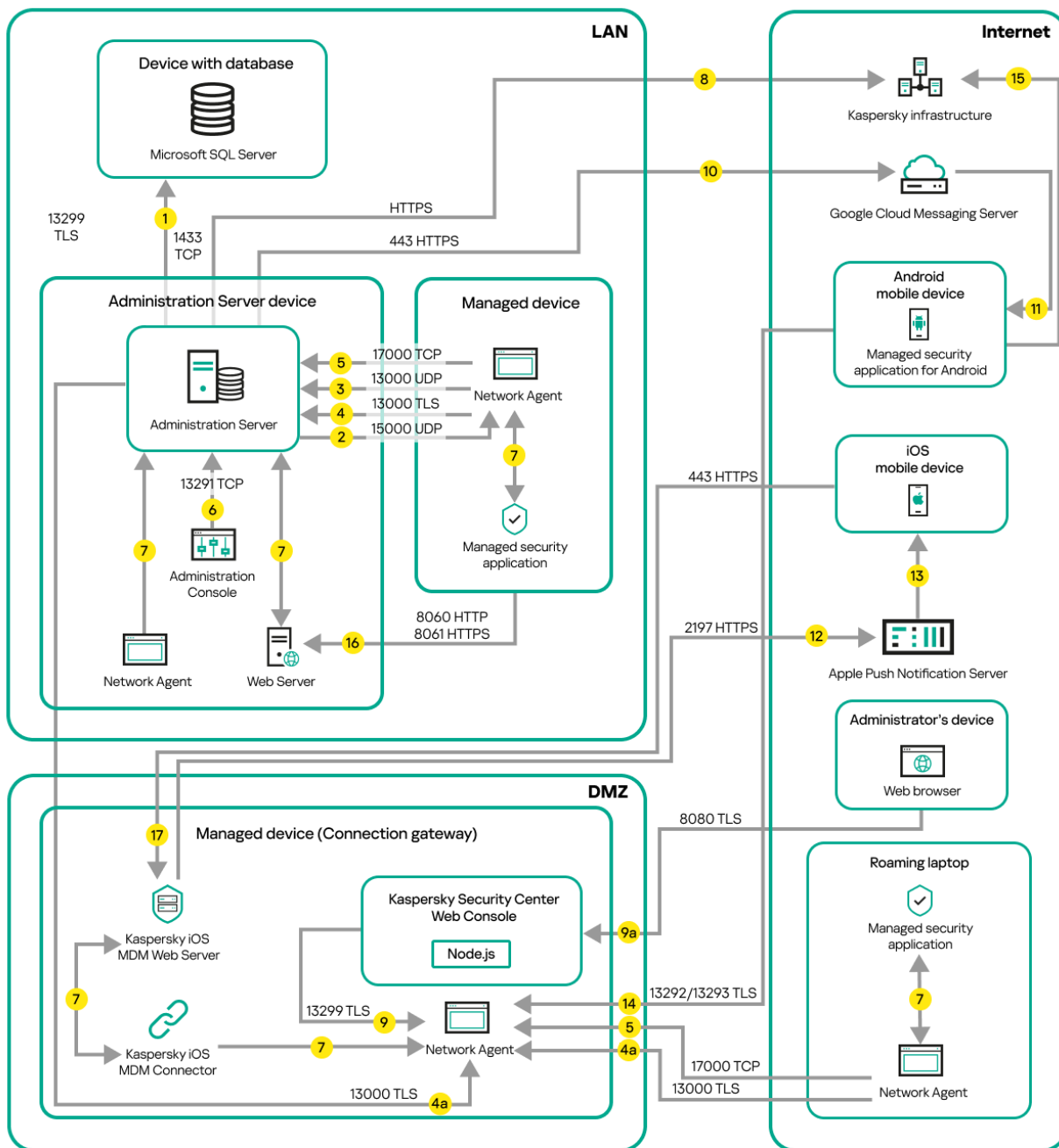
См. также:

Порты, используемые Kaspersky Security Center [63](#)

Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения

На рисунке ниже показан трафик данных, когда Сервер администрирования находится внутри локальной сети (LAN), а управляемые устройства, включая мобильные устройства, находятся в интернете. Шлюз соединения используется.

Эта схема разворачивания рекомендуется, если вы не хотите, чтобы мобильные устройства подключались непосредственно к Серверу администрирования, и не хотите использовать обратный прокси-сервер или корпоративный сетевой экран.



На этом рисунке управляемые устройства подключены к Серверу администрирования через шлюз соединений, который расположен в демилитаризованной зоне (DMZ). Обратный прокси-сервер или корпоративный сетевой экран не используются.

Стрелки указывают направление трафика: каждая стрелка проведена от устройства, которое инициирует соединение, к устройству, которое "отвечает" на вызов. Указаны номер порта и название протокола, используемые для передачи данных. Каждая стрелка пронумерована и содержит следующую информацию о соответствующем трафике данных:

1. Сервер администрирования передает данные в базу данных (см. раздел "Сервер администрирования и СУБД" на стр. [106](#)). Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000 (см. раздел "Сервер администрирования и клиентское устройство: Управление приложением безопасности" на стр. [108](#)).

Агенты администрирования отправляют запросы друг другу в пределах одного широковебательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковебательного домена и для автоматического назначения точек распространения (если этот параметр включен).

Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь с Сервером администрирования на эти устройства не отправляются напрямую.

3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. раздел "Сервер администрирования и клиентское устройство: Управление приложением безопасности" на стр. [108](#)) и от подчиненных Серверов администрирования (см. раздел "Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования" на стр. [111](#)) через TLS-порт 13000.

Если вы используете Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключение от Агентов администрирования по не TLS-порту 14000. Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, но рекомендуется использовать TLS-порт 13000.

Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

4а. Шлюз соединений (см. раздел "Шлюз соединения" см. стр. [54](#)) в демилитаризованной зоне также принимает подключение от Сервера администрирования по TLS-порту 13000 (см. раздел "Сервер администрирования и два устройства в демилитаризованной зоне: шлюз соединений и клиентское устройство" см. стр. [114](#)). Так как шлюз соединения в демилитаризованной зоне не может получить доступ к портам Сервера администрирования, Сервер администрирования создает и поддерживает постоянное сигнальное соединение со шлюзом соединения. Сигнальное соединение не используется для передачи данных; оно используется только для отправки приглашения к сетевому взаимодействию. Когда шлюзу соединения необходимо подключиться к Серверу, он уведомляет Сервер через это сигнальное соединение, а затем Сервер создает необходимое соединение для передачи данных.

Внешние устройства также подключаются к шлюзу соединения через TLS-порт 13000 (см. раздел "Сервер администрирования и два устройства в демилитаризованной зоне: шлюз соединений и клиентское устройство" см. стр. [114](#)).

5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.
6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291 (см. раздел "Сервер

администрирования и Консоль администрирования" на стр. [107](#)). Консоль администрирования может быть установлена на том же устройстве или на другом.

7. Приложения на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно управлять этими данными вручную.

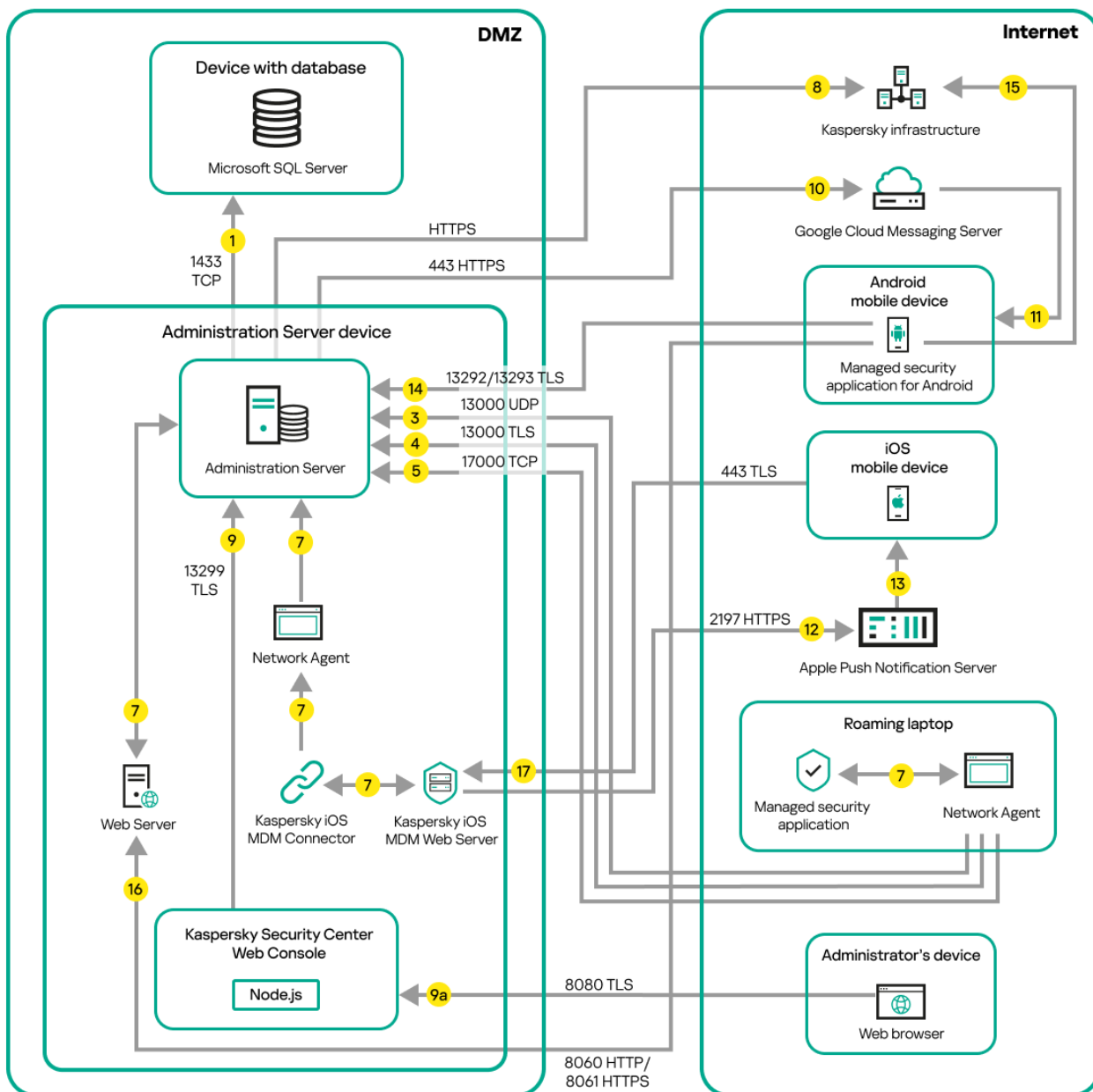
9. Сервер Kaspersky Security Center Web Console передает данные на Сервер администрирования, который может быть установлен на том же устройстве или на другом, через TLS-порт 13299.
 - 9а. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080 (см. раздел "Сервер администрирования и Kaspersky Security Center Web Console" на стр. [115](#)). Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.
10. Только для мобильных устройств Android: данные от Сервера администрирования передаются службам Google. Это соединение используется для уведомления мобильных устройств Android о том, что требуется их подключение к Серверу администрирования. Затем push-уведомления отправляются на мобильные устройства.
11. Только для мобильных устройств Android: push-уведомления от серверов Google отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств о том, что требуется их подключение к Серверу администрирования.
12. Только для мобильных устройств iOS: данные от Сервера iOS MDM передаются на серверы Apple Push Notification. Затем push-уведомления отправляются на мобильные устройства.
13. Только для мобильных устройств iOS: push-уведомления от серверов Apple отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств iOS о том, что требуется их подключение к Серверу администрирования.
14. Только для мобильных устройств: управляемое приложение передает данные на Сервер администрирования через TLS-порт 13292/13293 (см. раздел "Активация и управление приложением безопасности на мобильном устройстве" на стр. [116](#)) напрямую или через обратный прокси-сервер.
15. Только для мобильных устройств: данные от мобильного устройства передаются к инфраструктуре "Лаборатории Касперского".
 - 15а. Если мобильное устройство не имеет доступа в интернет, данные передаются на Сервер администрирования через порт 17100 (см. раздел "Активация и управление приложением безопасности на мобильном устройстве" на стр. [116](#)), а Сервер администрирования передает их инфраструктуре "Лаборатории Касперского". Однако этот сценарий используется очень редко.
16. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер (на стр. [43](#)), который находится на том же устройстве, на котором установлен Сервер администрирования.
17. Только для мобильных устройств iOS: данные от мобильных устройств передаются по TLS-порту 443 на Сервер iOS MDM, который находится на том же устройстве, на котором установлен Сервер администрирования или шлюз соединения.

См. также:

Порты, используемые Kaspersky Security Center	63
Об использовании точки распространения в качестве шлюза соединений	695

Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете

На рисунке ниже показан трафик данных, когда Сервер администрирования расположен в демилитаризованной зоне, а управляемые устройства расположены в интернете, включая мобильные устройства.



На этом рисунке шлюз соединения не используется: мобильные устройства подключаются к Серверу администрирования напрямую.

Стрелки указывают направление трафика: каждая стрелка проведена от устройства, которое инициирует соединение, к устройству, которое "отвечает" на вызов. Указаны номер порта и название протокола, используемые для передачи данных. Каждая стрелка пронумерована и содержит следующую информацию о соответствующем трафике данных:

1. Сервер администрирования передает данные в базу данных (см. раздел "Сервер администрирования и СУБД" на стр. [106](#)). Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000 (см. раздел "Сервер администрирования и клиентское устройство: Управление приложением безопасности" на стр. [108](#)).

Агенты администрирования отправляют запросы друг другу в пределах одного широковебательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковебательного домена и для автоматического назначения точек распространения (если этот параметр включен).

Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь с Сервером администрирования на эти устройства не отправляются напрямую.

3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. раздел "Сервер администрирования и клиентское устройство: Управление приложением безопасности" на стр. [108](#)) и от подчиненных Серверов администрирования (см. раздел "Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования" на стр. [111](#)) через TLS-порт 13000.

Если вы используете Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключение от Агентов администрирования по не TLS-порту 14000. Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, но рекомендуется использовать TLS-порт 13000.

Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.
6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291 (см. раздел "Сервер администрирования и Консоль администрирования" на стр. [107](#)). Консоль администрирования может быть установлена на том же устройстве или на другом.
7. Приложения на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно управлять этими данными вручную.

9. Сервер Kaspersky Security Center Web Console передает данные на Сервер администрирования, который может быть установлен на том же устройстве или на другом, через TLS-порт 13299.

9а. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080 (см. раздел "Сервер администрирования и Kaspersky Security Center Web Console" на стр. [115](#)). Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

10. Только для мобильных устройств Android: данные от Сервера администрирования передаются службам Google. Это соединение используется для уведомления мобильных устройств Android о том, что требуется их подключение к Серверу администрирования. Затем push-уведомления отправляются на мобильные устройства.
11. Только для мобильных устройств Android: push-уведомления от серверов Google отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств о том, что требуется их подключение к Серверу администрирования.
12. Только для мобильных устройств iOS: данные от Сервера iOS MDM передаются на серверы Apple Push Notification. Затем push-уведомления отправляются на мобильные устройства.
13. Только для мобильных устройств iOS: push-уведомления от серверов Apple отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств iOS о том, что требуется их подключение к Серверу администрирования.
14. Только для мобильных устройств: управляемое приложение передает данные на Сервер администрирования через TLS-порт 13292/13293 (см. раздел "Активация и управление приложением безопасности на мобильном устройстве" на стр. [116](#)) напрямую или через обратный прокси-сервер.
15. Только для мобильных устройств: данные от мобильного устройства передаются к инфраструктуре "Лаборатории Касперского".

15а. Если мобильное устройство не имеет доступа в интернет, данные передаются на Сервер администрирования через порт 17100 (см. раздел "Активация и управление приложением безопасности на мобильном устройстве" на стр. [116](#)), а Сервер администрирования передает их инфраструктуре "Лаборатории Касперского". Однако этот сценарий используется очень редко.
16. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер (на стр. [43](#)), который находится на том же устройстве, на котором установлен Сервер администрирования.
17. Только для мобильных устройств iOS: данные от мобильных устройств передаются по TLS-порту 443 на Сервер iOS MDM, который находится на том же устройстве, на котором установлен Сервер администрирования или шлюз соединения.

См. также:

Порты, используемые Kaspersky Security Center	63
Доступ из интернета: Сервер администрирования в демилитаризованной зоне	145

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения

В этом разделе приведены схемы взаимодействия между компонентами в составе Kaspersky Security Center и управляемыми приложениями безопасности. На схемах приведены номера портов, которые должны быть доступны, и имена процессов, открывающих порты.

В этом разделе

Условные обозначения в схемах взаимодействия	104
Сервер администрирования и СУБД	106
Сервер администрирования и Консоль администрирования	107
Сервер администрирования и клиентское устройство: Управление приложением безопасности	108
Обновление программного обеспечения на клиентском устройстве с помощью точки распространения	109
Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования	111
Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне	112
Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство	113
Сервер администрирования и два устройства в демилитаризованной зоне: шлюз соединений и клиентское устройство	114
Сервер администрирования и Kaspersky Security Center Web Console	115
Активация и управление приложением безопасности на мобильном устройстве	116

См. также:

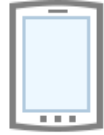
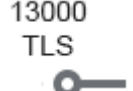
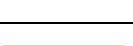
Основной сценарий установки ... [56](#)

Условные обозначения в схемах взаимодействия

В таблице ниже приведены условные обозначения, использованные в схемах.

Таблица 15. Условные обозначения

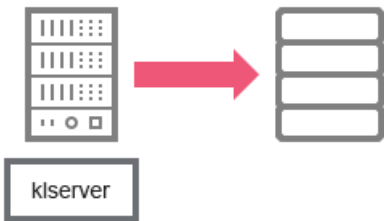
Иконка	Значение
	Сервер администрирования

Иконка	Значение
	Подчиненный Сервер администрирования
	СУБД
	Клиентское устройство, на котором установлены Агент администрирования и приложение семейства Kaspersky Endpoint Security (либо другое приложение безопасности, которое может управлять Kaspersky Security Center)
	Шлюз соединения
	Точка распространения
	Мобильное клиентское устройство с установленным приложением Kaspersky Security для мобильных устройств
	Браузер на устройстве пользователя
	Процесс, запущенный на устройстве и открывающий какой-либо порт
	Порт и его номер
	Трафик TCP (направление стрелки обозначает направление трафика)
	Трафик UDP (направление стрелки обозначает направление трафика)
	Вызов COM
	Транспорт СУБД

Иконка	Значение
	Границы демилитаризованной зоны

Сервер администрирования и СУБД

Данные от Сервера администрирования поступают в базу данных SQL Server, MySQL или MariaDB.

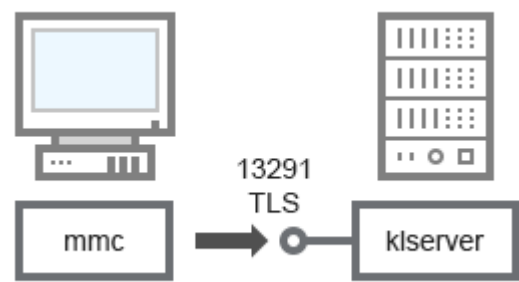


Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.

См. также:

Условные обозначения в схемах взаимодействия	104
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Порты, используемые Kaspersky Security Center	63
Выбор СУБД для Сервера администрирования	139

Сервер администрирования и Консоль администрирования



Пояснения к схеме см. в таблице ниже.

Таблица 16. Сервер администрирования и Консоль администрирования (трафик)

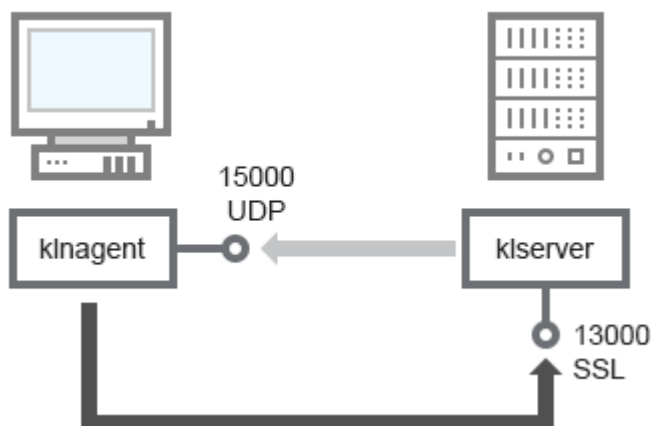
Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Сервер администрирования	13291	klserver	TCP	Да	Прием подключений от Консоли администрирования

См. также:

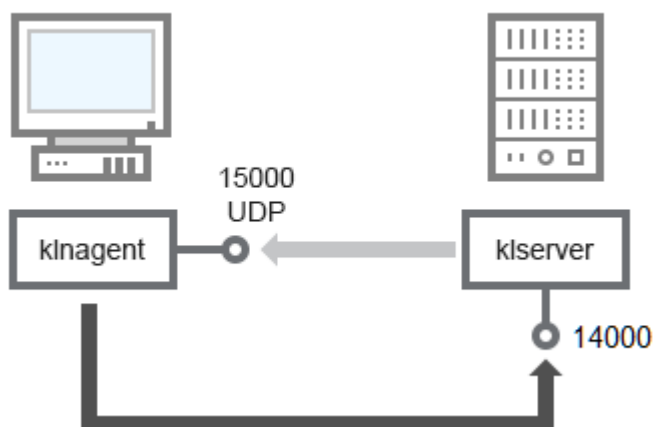
Условные обозначения в схемах взаимодействия	104
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Порты, используемые Kaspersky Security Center	63

Сервер администрирования и клиентское устройство: Управление приложением безопасности

Сервер администрирования принимает подключения от Агентов администрирования по защищенному порту 13000 (см. рис. ниже).



Если вы использовали Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключения от Агентов администрирования по незащищенному порту 14000 (см. рис. ниже). Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, однако рекомендуется использовать защищенный порт 13000.



Пояснения к схемам см. в таблице ниже.

Таблица 17. Сервер администрирования и клиентское устройство: управление приложением

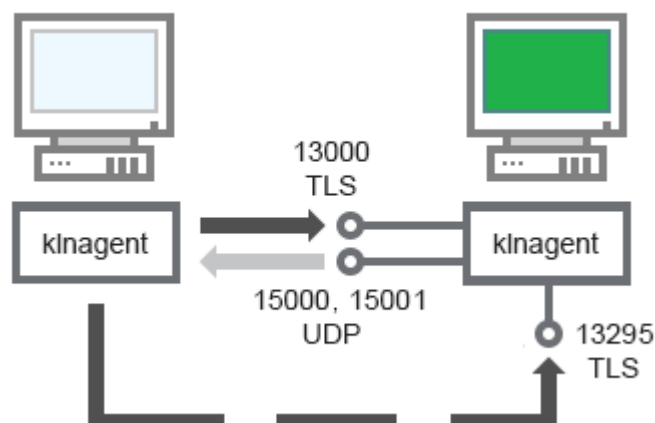
Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (только для TCP)	Назначение порта
Агент администрирования	15000	klagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования
Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от Агентов администрирования
Сервер администрирования	14000	klserver	TCP	Нет	Прием подключений от Агентов администрирования

См. также:

Условные обозначения в схемах взаимодействия	104
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Порты, используемые Kaspersky Security Center	63

Обновление программного обеспечения на клиентском устройстве с помощью точки распространения

Клиентское устройство подключается к точке распространения через порт 13000 и, если вы используете точку распространения в качестве push-сервера, также через порт 13295; точка распространения выполняет многоадресную рассылку Агентам администрирования через порт 15000 (см. рисунок ниже). Обновления и инсталляционные пакеты поступают с точки распространения через порт 15001.



Пояснения к схеме см. в таблице ниже.

Таблица 18. Обновление программного обеспечения с помощью точки распространения

(трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (только для TCP)	Назначение порта
Агент администрирования	15000	klagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования
Агент администрирования	15001	klagent	UDP	Нет значения	Получение обновлений и инсталляционных пакетов от точки распространения
Точка распространения	13000	klagent	TCP	Да	Прием подключений от Агентов администрирования
Точка распространения	13295	klagent	TCP	Да	Получение подключений от клиентских устройств (push-сервера)

См. также:

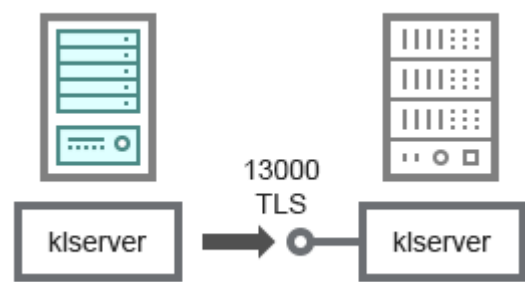
Условные обозначения в схемах взаимодействия	104
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Порты, используемые Kaspersky Security Center	63

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования

На схеме (см. рис. ниже) показано, как используется порт 13000 для взаимодействия Серверов администрирования, объединенных в иерархию.

При объединении Серверов в иерархию (см. раздел "Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования" на стр. 700) необходимо, чтобы порт 13291 обоих Серверов был доступен. Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования (см. раздел "Сервер администрирования и Консоль администрирования" на стр. 107).

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Консоль администрирования, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13291 главного Сервера был доступен.



Пояснения к схеме см. в таблице ниже.

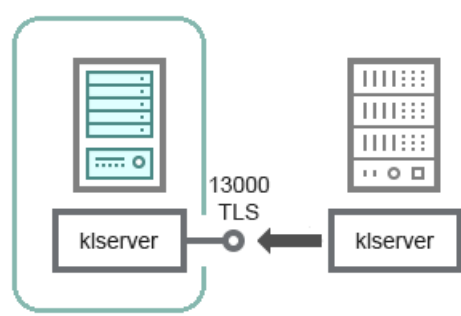
Таблица 19. Иерархия Серверов администрирования (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Главный Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от подчиненных Серверов администрирования

См. также:

Условные обозначения в схемах взаимодействия	104
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Порты, используемые Kaspersky Security Center	63
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования	700

Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне



На схеме показана иерархия Серверов администрирования, в которой подчиненный Сервер, находящийся в демилитаризованной зоне, принимает подключение от главного Сервера (пояснения к схеме см. в таблице ниже). При объединении Серверов в иерархию (см. раздел "Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования" на стр. 700) необходимо, чтобы порт 13291 обоих Серверов был доступен. Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования (см. раздел "Сервер администрирования и Консоль администрирования" на стр. 107).

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Консоль администрирования, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13291 главного Сервера был доступен.

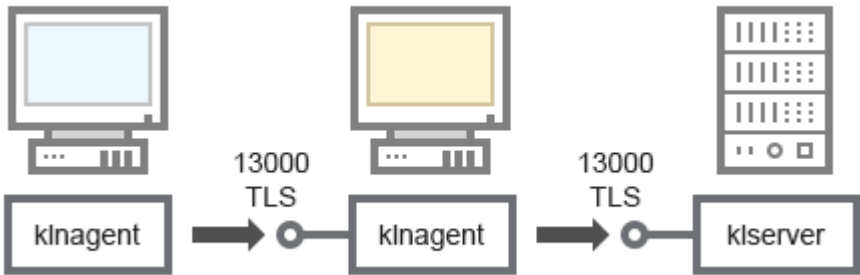
Таблица 20. Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Подчиненный Сервер администрирования	13000	kserver	TCP	Да	Прием подключений от главного Сервера администрирования

См. также:

Условные обозначения в схемах взаимодействия	104
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Порты, используемые Kaspersky Security Center	63
Настройка подключения Консоли администрирования к Серверу администрирования	296
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования	700

Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство



Пояснения к схеме см. в таблице ниже.

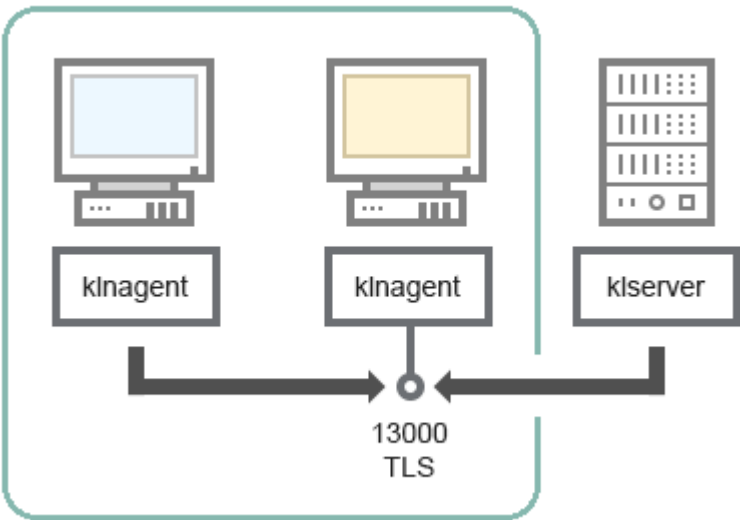
Таблица 21. Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от Агентов администрирования
Агент администрирования	13000	klnagent	TCP	Да	Прием подключений от Агентов администрирования

См. также:

Условные обозначения в схемах взаимодействия	104
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Порты, используемые Kaspersky Security Center	63

Сервер администрирования и два устройства в демилитаризованной зоне: шлюз соединений и клиентское устройство



Пояснения к схеме см. в таблице ниже.

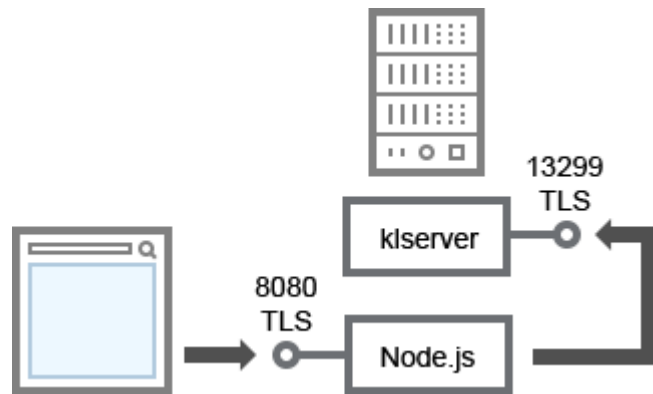
Таблица 22. Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Агент администрирования	13000	klnagent	TCP	Да	Прием подключений от Агентов администрирования

См. также:

Условные обозначения в схемах взаимодействия	104
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Порты, используемые Kaspersky Security Center	63

Сервер администрирования и Kaspersky Security Center Web Console



Пояснения к схеме см. в таблице ниже.

Таблица 23. Сервер администрирования и Kaspersky Security Center Web Console (трафик)

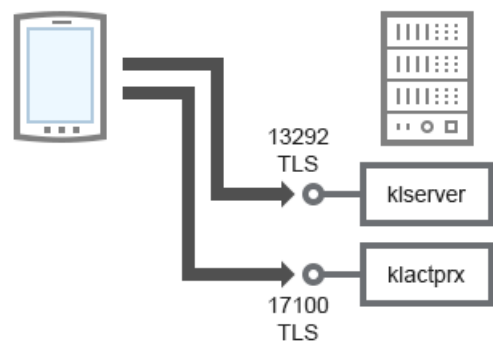
Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Сервер администрирования	13299	klservice	TCP	Да	Получение соединений от Kaspersky Security Center Web Console к Серверу администрирования через OpenAPI
Сервер Kaspersky Security Center Web Console или Сервер администрирования	8080	Node.js: серверный JavaScript	TCP	Да	Получение соединений от Kaspersky Security Center Web Console

Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

См. также:

Условные обозначения в схемах взаимодействия	104
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Порты, используемые Kaspersky Security Center	63

Активация и управление приложением безопасности на мобильном устройстве



Пояснения к схеме см. в таблице ниже.

Таблица 24. Активация и управление приложением безопасности на мобильном устройстве (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Сервер администрирования	13292	klservice	TCP	Да	Прием подключений от Консоли администрирования к Серверу администрирования
Сервер администрирования	17100	klactprx	TCP	Да	Прием подключений для активации приложений от мобильных устройств

См. также:

Условные обозначения в схемах взаимодействия	104
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Порты, используемые Kaspersky Security Center	63

Лучшие практики развертывания

Kaspersky Security Center является распределенным приложением. В состав Kaspersky Security Center входят следующие приложения:

- Сервер администрирования – центральный компонент, ответственный за управление устройствами организации и хранение данных в СУБД.
- Консоль администрирования – основной инструмент администратора. Консоль администрирования поставляется вместе с Сервером администрирования, но может быть также установлена отдельно на одно или несколько устройств администратора.
- Агент администрирования – служит для управления установленным на устройстве приложением безопасности, а также для получения информации об устройстве и передаче этой информации на

Сервер администрирования. Агенты администрирования устанавливаются на устройства организации.

Развертывание Kaspersky Security Center в сети организации осуществляется следующим образом:

- установка Сервера администрирования;
- установка Консоли администрирования на устройстве администратора;
- установка Агента администрирования и приложения безопасности на устройства организации.

Руководство по усилению защиты

Приложение Kaspersky Security Center предназначено для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Приложение предоставляет администратору доступ к детальной информации об уровне безопасности сети организации. Kaspersky Security Center позволяет настраивать все компоненты защиты, построенной на основе приложений "Лаборатории Касперского".

Сервер администрирования Kaspersky Security Center имеет полный доступ к управлению защитой клиентских устройств и является важнейшим компонентом системы защиты организации. Поэтому для Сервера администрирования требуются усиленные меры защиты.

В Руководстве по усилению защиты описаны рекомендации и особенности настройки Kaspersky Security Center и его компонентов для снижения рисков его компрометации.

Руководство по усилению защиты содержит следующую информацию:

- выбор схемы развертывания Сервера Администрирования;
- настройка безопасного подключения к Серверу Администрирования;
- настройка учетных записей для работы с Сервером администрирования;
- управление защитой Сервера администрирования;
- управление защитой клиентских устройств;
- настройка защиты управляемых приложений;
- обслуживание Сервера администрирования;
- передача информации в сторонние системы;
- рекомендации по безопасности сторонних информационных систем.

Развертывание Сервера администрирования

Архитектура Сервера администрирования

В общем случае на выбор архитектуры централизованного управления влияют расположение защищаемых устройств, доступы из смежных сетей, схемы обновления баз и другие параметры.

На начальном этапе проработки архитектуры мы рекомендуем ознакомиться с компонентами Kaspersky Security Center (см. раздел "Архитектура приложения" на стр. [56](#)) и их взаимодействием между собой, а также со схемами трафика данных и использования портов (см. раздел "Схемы трафика данных и использования портов" на стр. [87](#)).

На основании этой информации нужно сформировать архитектуру, определяющую:

- расположение Сервера администрирования и подключение к сети;
- организацию рабочих мест администраторов и способы подключения к Серверу администрирования;
- способ установки Агента администрирования и приложения защиты;
- использование точек распространения;
- использование виртуальных Серверов администрирования;
- использование иерархии Серверов администрирования;
- схему обновления антивирусных баз;
- другие информационные потоки.

Выбор устройства для Сервера администрирования

Сервер администрирования рекомендуется устанавливать на выделенный сервер в инфраструктуре. Если на сервере отсутствует стороннее программное обеспечение, это позволит настроить параметры безопасности с учетом требований Kaspersky Security Center и без зависимости от требований стороннего программного обеспечения.

Сервер администрирования может быть развернут как на физическом сервере, так и на виртуальной машине. Убедитесь, что выбранное устройство соответствует аппаратным и программным требованиям (см. стр. [29](#)).

Расположение Сервера администрирования

Устройства, управляемые Сервером администрирования, могут располагаться:

- в локальном сегменте сети;
- в интернете;
- в демилитаризованной зоне (DMZ).

При этом Сервер администрирования также может быть расположен в следующих сегментах: технологическом, корпоративном, сегментах демилитаризованной зоны (DMZ).

При использовании Kaspersky Security Center для управления защитой изолированного сегмента сети, рекомендуется разворачивать Сервер администрирования в сегменте демилитаризованной зоны (DMZ) (см. раздел "Схемы трафика данных и использования портов" на стр. [87](#)). Это позволит организовать полноценное сегментирование сетей и минимизировать возможные обращения в защищаемый сегмент, сохранив при этом возможности по управлению устройствами и доставке обновлений.

Ограничение установки Сервера администрирования на контроллер домена, терминальный сервер или пользовательское устройство

Категорически не рекомендуется устанавливать Сервер администрирования на контроллер домена, терминальный сервер или пользовательское устройство.

Рекомендуется предусмотреть функциональное разделение ключевых устройств сети. Это позволит сохранить работоспособность разных систем при выходе устройства из строя или при его компрометации. В это же время такой подход позволит реализовать различные политики безопасности для каждого устройства.

Например, ограничения безопасности, применяемые к контроллеру домена <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack>, могут значительно снизить производительность Сервера администрирования и привести к невозможности использования некоторых его функций. Если привилегированный доступ к контроллеру домена получит

злоумышленник, он может изменить, повредить или уничтожить базу данных Active Directory Domain Services (AD DS). При этом также будут скомпрометированы все системы и учетные записи, управляемые Active Directory.

Учетные записи для установки и запуска Сервера администрирования

Рекомендуется запустить установку Сервера администрирования под учетной записью локального администратора, чтобы избежать использования учетных записей домена для доступа к базе данных Сервера администрирования. Набор необходимых учетных записей и их прав (см. раздел "Учетные записи для работы с СУБД" на стр. [207](#)) зависит от выбранного типа СУБД, местоположения СУБД и способа создания базы данных Сервера администрирования.

Группы пользователей KLAadmins и KLOperators создаются автоматически во время установки Kaspersky Security Center. Этим группам предоставляются права на подключение к Серверу администрирования и на работу с его объектами.

В зависимости от того, под какой учетной записью проводится установка Kaspersky Security Center, группы KLAadmins и KLOperators создаются следующим образом:

- Если установка проводится под учетной записью пользователя, входящего в домен, группы создаются на устройстве с Сервером администрирования и в домене, в который входит устройство с Сервером администрирования.
- Если установка проводится под учетной записью системы, группы создаются только на устройстве с Сервером администрирования.

Чтобы избежать создания групп KLAadmins и KLOperators в домене и, как следствие, **присвоения прав для управления Сервером администрирования вне устройства, на котором он установлен**, рекомендуется проводить установку Kaspersky Security Center под локальной учетной записью.

При установке Сервера администрирования выберите учетную запись, под которой Сервер администрирования будет запускаться как служба. По умолчанию приложение создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования (klserver).

Служба Сервера администрирования при необходимости может запускаться под выбранной учетной записью. При этом учетная запись должна обладать различными правами для подключения к СУБД. Для обеспечения безопасности используйте непривилегированную учетную запись для запуска службы Сервера администрирования.

Во избежание некорректных параметров доступа для учетной записи Сервера администрирования рекомендуется создавать ее автоматически (см. раздел "Шаг 9. Выбор учетной записи для запуска Сервера администрирования" на стр. [240](#)).

Исключение Сервера администрирования из домена

Если вы используете Сервер администрирования для защиты групп устройств важных систем, не рекомендуется включать в домен устройство Сервера администрирования (если оно используется). Это позволит разграничить права управления Kaspersky Security Center и избежать получения доступа к управлению в случае компрометации домена.

Обратите внимание, если вы установите Сервер администрирования на устройство, входящее в рабочую группу, будут недоступны следующие сценарии работы с Сервером администрирования:

- Использование отказоустойчивого кластера Kaspersky Security Center (см. раздел "Об отказоустойчивом кластере Kaspersky Security Center" см. стр. [246](#)).
- Использование отказоустойчивого кластера Windows Server (см. раздел "Установка Сервера администрирования на отказоустойчивом кластере Windows Server" на стр. [254](#)).

- Использование SQL Server на отдельном устройстве.

Использовать SQL Сервер на отдельном устройстве можно, только если Сервер администрирования и SQL Server включены в домен.

- Удаленная установка средствами Сервера администрирования (см. раздел "Удаленная установка средствами Сервера администрирования с помощью групповых политик Active Directory" см. стр. [227](#)) с помощью групповых политик Active Directory

Если необходимо установить Сервер администрирования на устройство, входящее в рабочую группу, во избежание установки Сервера администрирования вы можете использовать Kaspersky Security Center Linux вместо Kaspersky Security Center Windows.

Безопасность соединения

Использование TLS

Рекомендуется запретить небезопасные подключения к Серверу администрирования. Например, при настройке Сервера администрирования, рекомендуется не включать подключения по HTTP-протоколу к Серверу администрирования.

Обратите внимание, что по умолчанию часть HTTP-портов Сервера администрирования (см. раздел "Порты, используемые Kaspersky Security Center" на стр. [63](#)) закрыта. Оставшийся порт используется Веб-сервером Kaspersky Security Center (8060). Этот порт можно ограничить параметрами сетевого экрана устройства с Сервером администрирования.

Строгие параметры TLS

Рекомендуется использовать протокол TLS версии 1.2 или выше и ограничить или запретить использование небезопасных алгоритмов шифрования.

Вы можете настроить протоколы шифрования (см. раздел "Шифрование подключения TLS" см. стр. [317](#)) (TLS), используемые Сервером администрирования. При этом учитывайте, что на момент выпуска определенной версии Сервера администрирования параметры протокола шифрования по умолчанию настроены так, чтобы обеспечить безопасную передачу данных.

Ограничение доступа к базе данных Сервера администрирования

Рекомендуется ограничить доступ к базе данных Сервера администрирования. Например, вы можете разрешить доступ только с устройства с Сервером администрирования. Это позволит снизить вероятность взлома базы Сервера администрирования данных через известные уязвимости.

Вы можете настроить параметры в соответствии с руководством по эксплуатации используемой базы данных, а также предусмотреть закрытые порты на сетевых экранах.

Запрет удаленной аутентификации с учетными записями Windows

Запрет на SSPI-подключения с удаленных адресов возможен с помощью специального флага LP_RestrictRemoteOsAuth. Этот флаг позволяет запретить удаленную аутентификацию на Сервере администрирования для учетных записей Windows, локальных или доменных.

Чтобы переключить флаг LP_RestrictRemoteOsAuth в режим запрета SSPI-подключений с удаленных адресов:

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Выполните следующую команду в командной строке, чтобы указать значение флага LP_RestrictRemoteOsAuth:

```
klscflag.exe -fset -pv .core/.independent -s KLLIM -n  
LP_RestrictRemoteOsAuth -t d -v 1
```

3. Перезапустите службу Сервера администрирования.

Флаг LP_RestrictRemoteOsAuth не работает, если удаленная аутентификация выполняется через Kaspersky Security Center Web Console или Консоль администрирования, установленную на том же устройстве, что и Сервер администрирования.

Аутентификация Microsoft SQL Server

Если вы используете Microsoft SQL Server в качестве СУБД Сервера администрирования (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. [238](#)), нужно защитить от несанкционированного доступа данные Kaspersky Security Center, передаваемые в базу данных или получаемые от нее, а также данные, хранящиеся в этой базе данных. Для этого требуется настроить использование безопасного соединения между Kaspersky Security Center и SQL Server. Самый надежный способ обеспечить безопасную связь – это установить Kaspersky Security Center и SQL Server на одном устройстве и использовать механизм совместной памяти для обоих приложений. Во всех других случаях рекомендуется использовать сертификат SSL/TLS для аутентификации экземпляра SQL Server (см. раздел "Сценарий: аутентификация Microsoft SQL Server" см. стр. [224](#)).

Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования

По умолчанию пользователи могут войти в Kaspersky Security Center с любого устройства, на котором установлена Kaspersky Security Center Web Console или Консоль администрирования на основе Microsoft Management Console (MMC). Настроить Сервер администрирования (см. раздел "Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования" на стр. [708](#)) можно таким образом, чтобы пользователи могли подключаться к нему только с устройств с разрешенными IP-адресами. В этом случае, если злоумышленник похитит учетную запись Kaspersky Security Center, он сможет подключиться к Kaspersky Security Center только с тех IP-адресов, которые добавлены в разрешенные.

Учетные записи и авторизация

Перед выполнением шагов ниже, создайте резервную копию данных Сервера администрирования Kaspersky Security Center с помощью задачи Резервное копирование данных Сервера администрирования (см. раздел "Резервное копирование и восстановление параметров Сервера администрирования" на стр. [721](#)) или с помощью утилиты klbackup. Сохраните резервную копию данных в надежном месте.

Использование двухэтапной проверки Сервера администрирования

Kaspersky Security Center предоставляет пользователям Kaspersky Security Center Web Console и Консоли администрирования возможность использовать **двухэтапную проверку** на основе стандарта RFC 6238 (TOTP: Time-Based One-Time Password algorithm).

Если для вашей учетной записи включена двухэтапная проверка, каждый раз при входе в Kaspersky Security Center Web Console или в Консоль администрирования вы вводите свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Если вы используете доменную аутентификацию для

своей учетной записи, вам необходимо ввести только дополнительный одноразовый код безопасности. Для того чтобы получить одноразовый код безопасности, вам нужно установить приложение для аутентификации на своем компьютере или мобильном устройстве.

Существуют как программные, так и аппаратные аутентификаторы (токены), поддерживающие стандарт RFC 6238. Например, к программным аутентификаторам относятся Google Authenticator, Microsoft Authenticator, FreeOTP.

Категорически не рекомендуется устанавливать приложение для аутентификации на том же устройстве, с которого выполняется подключение к Серверу администрирования. Например, вы можете установить приложение для аутентификации на мобильном устройстве.

Использование двухфакторной аутентификации операционной системы

Для авторизации на устройстве с Сервером администрирования рекомендуется использовать многофакторную аутентификацию (MFA) с использованием токена, смарт-карты или другого способа.

Запрет на сохранение пароля администратора

При использовании Консоли администрирования не рекомендуется сохранять пароль администратора в диалоговом окне подключения к Серверу администрирования.

Также при работе с Сервером администрирования через Kaspersky Security Center Web Console не рекомендуется сохранять пароль администратора в браузере на устройстве пользователя.

Авторизация внутреннего пользователя

По умолчанию пароль внутренней учетной записи пользователя Сервера администрирования (см. раздел "Изменение учетной записи внутреннего пользователя" на стр. [806](#)) должен соответствовать следующим требованиям:

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп списка ниже:
 - верхний регистр (A-Z);
 - нижний регистр (A-Z) (a-z);
 - числа (0-9);
 - специальные символы (@ # \$ % ^ & * - _ ! + = [] { } | : ' , . ? / \ ` ~ " () ;)
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить количество попыток ввода пароля (см. раздел "Изменение количества попыток ввода пароля" см. стр. [807](#)).

Пользователь Kaspersky Security Center может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

Отдельная группа администрирования для устройства с Сервером администрирования

Для Сервера администрирования рекомендуется создать выделенную группу администрирования (см. раздел "Создание групп администрирования" на стр. [743](#)). Предоставьте этой группе особые права доступа и создайте политику безопасности для нее.

Чтобы избежать умышленного понижения уровня защиты Сервера администрирования рекомендуется ограничить список учетных записей, которые могут управлять этой группой администрирования.

Группы KLAAdmins и KLOperators

Группы пользователей KLAAdmins и KLOperators (см. раздел "Права доступа к Серверу администрирования и его объектам" на стр. [706](#)) создаются автоматически во время установки Kaspersky Security Center. Группе KLAAdmins предоставлены все права. Группе KLOperators предоставлены права на Чтение и Выполнение. Набор прав, предоставленных группе KLAAdmins, **недоступен для изменения**.

С помощью стандартных средств администрирования операционной системы можно просмотреть группы KLAAdmins и KLOperators и внести изменения в состав этих групп.

При разработке регламентов работы с Сервером администрирования нужно определить, потребуется ли специалисту информационной безопасности полный доступ (и включение в группу KLAAdmins) для решения штатных задач.

Большинство базовых задач администрирования могут быть распределены между подразделениями организации (или разными сотрудниками одного подразделения) и, как следствие, между различными учетными записями. Также может быть выполнено разграничение по доступу к группам администрирования в Kaspersky Security Center. В результате можно реализовать такую модель использования, при которой авторизация под учетными записями из группы KLAAdmins будет нестандартным поведением, что можно рассматривать как инцидент.

Если установка Kaspersky Security Center проводилась под системной учетной записью, группы создаются только на устройстве с Сервером администрирования. В этом случае рекомендуем убедиться, что в группу включены только учетные записи, созданные во время установки Kaspersky Security Center. Не рекомендуется добавлять в группу KLAAdmins другие группы пользователей (локальные и/или доменные), которые были созданы автоматически во время установки Kaspersky Security Center. Также следует ограничить права на изменение этой группы. Группа KLAAdmins должна включать единичные непривилегированные учетные записи.

Если установка выполнялась под учетной записью пользователя, входящего в домен, группы KLAAdmins и KLOperators создаются как на Сервере администрирования, так и в домене, в который входит Сервер администрирования. Рекомендуется применить аналогичный подход как и в случае с установкой под системной учетной записью.

Ограничить членство в роли "Главный администратор"

Рекомендуется ограничить членство пользователей в роли "Главный администратор".

По умолчанию после установки Сервера администрирования роль "Главный администратор" присвоена группе локальных администраторов устройства и созданной группе KLAAdmins. Это удобно для управления, но критично с точки зрения безопасности, так как роль "Главный администратор" имеет очень широкий набор привилегий – назначение этой роли пользователям должно быть строго регламентировано.

Локальных администраторов можно исключить из списка пользователей, имеющих права администратора Kaspersky Security Center. Роль "Главный администратор" невозможно удалить из группы KLAAdmins. В нее можно включить учетные записи группы KLAAdmins (см. раздел "Права доступа к Серверу администрирования и его объектам" на стр. [706](#)), которые будут использоваться для управления Сервером администрирования.

В случае использования доменной аутентификации, рекомендуется ограничить привилегии учетных записей администраторов домена в Kaspersky Security Center. По умолчанию этим учетным записям присвоена роль "Главный администратор". Также администратор домена может включить свою учетную запись в группу KLAAdmins с целью получения роли "Главный администратор". Чтобы этого избежать, в параметрах безопасности Kaspersky Security Center можно добавить группу "Администраторы домена" ("Domain Admins") и определить для нее запрещающие правила. Эти правила будут приоритетнее разрешающих.

Также можно использовать предопределенные роли пользователей (см. раздел "Права доступа к функциям приложения" на стр. [810](#)) с уже настроенным набором прав.

Настройка прав доступа к функциям приложения

Рекомендуется использовать возможности гибкой настройки прав доступа (см. раздел "Настройка прав. Пользовательские роли" на стр. [809](#)) пользователей и групп пользователей к разным функциям Сервера администрирования.

Управление доступом на основе ролей позволяет создавать типовые роли пользователей с заранее настроенным набором прав и присваивать эти роли пользователям в зависимости от их служебных обязанностей.

Основные преимущества ролевой модели управления доступом:

- простота администрирования;
- иерархия ролей;
- принцип наименьшей привилегии;
- разделение обязанностей.

Вы можете воспользоваться встроенными ролями и присвоить их определенным сотрудникам на основе должностей либо создать полностью новые роли.

При настройке ролей требуется уделить особое внимание привилегиям, связанным с изменением состояния защиты устройства и удаленной установкой стороннего программного обеспечения:

- Управление группами администрирования.
- Операции с Сервером администрирования.
- Удаленная установка.
- Изменение параметров хранения событий и отправки уведомлений.

Эта привилегия позволяет настроить уведомления, которые запускают скрипт или исполняемый модуль на устройстве с Сервером администрирования при возникновении события.

Отдельная учетная запись для удаленной установки приложений

Помимо базового разграничения прав доступа, рекомендуется ограничить возможность удаленной установки приложений для всех учетных записей (кроме "Главного администратора" или иной специализированной учетной записи).

Рекомендуется использовать отдельную учетную запись для удаленной установки приложений. Вы можете назначить роль (см. раздел "Назначение роли пользователю или группе безопасности" на стр. [838](#)) или разрешения (см. раздел "Назначение прав пользователям или группам пользователей" на стр. [838](#)) отдельной учетной записи.

Обеспечение безопасности привилегированного доступа Windows

Рекомендуется рассмотреть рекомендации Microsoft по обеспечению безопасности привилегированного доступа. Чтобы просмотреть эти рекомендации, перейдите в раздел Обеспечение безопасности привилегированного доступа <https://learn.microsoft.com/en-us/security/compass/overview>. Одной из ключевых рекомендаций является развертывание рабочих станций с привилегированным доступом (PAW) <https://learn.microsoft.com/en-us/security/compass/privileged-access-devices#paw-phased-implementation>.

Использование управляемых учетных записей служб (MSA) и групповых управляемых учетных записей служб (gMSA) для запуска служб Сервера администрирования

В Active Directory существует специальный тип учетных записей для безопасного запуска служб – MSA/gMSA <https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview>. Kaspersky Security Center поддерживает управляемые учетные записи службы (см. раздел "Шаг 9. Выбор учетной записи для запуска Сервера администрирования" на стр. [240](#)) (MSA) и групповые управляемые учетные записи службы (gMSA). Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования.

Регулярный аудит всех пользователей

Рекомендуется проводить регулярный аудит всех пользователей на устройстве, где установлен Сервер администрирования. Это позволит реагировать на некоторые типы угроз безопасности, связанные с возможной компрометацией устройства.

Управление защитой Сервера администрирования

Выбор приложения защиты Сервера администрирования

Выбор приложения для защиты устройства, на котором установлен Сервер администрирования, зависит от типа развертывания Сервера администрирования и общей стратегии защиты.

Если вы разворачиваете Сервер администрирования на выделенном устройстве, рекомендуется выбрать приложение Kaspersky Endpoint Security для защиты устройства с Сервером администрирования. Это позволит применить все имеющиеся технологии для защиты устройства, в том числе модули поведенческого анализа.

Если Сервер администрирования устанавливается на уже существующее в инфраструктуре устройство, использованное ранее для выполнения других задач, рекомендуются следующие приложения защиты:

- Kaspersky Industrial CyberSecurity for Nodes. Это приложение рекомендуется устанавливать на устройства, входящие в промышленную сеть. Kaspersky Industrial CyberSecurity for Nodes – это приложение, имеющее сертификаты совместимости с различными производителями промышленного программного обеспечения.
- Рекомендованные решения безопасности. Если Сервер администрирования установлен на устройство с другим программным обеспечением, нужно ознакомиться с рекомендациями производителя программного обеспечения по использованию антивирусных решений (возможно, уже существуют рекомендации по выбору приложения защиты, и, вероятно, вам потребуется выполнить настройку доверенной зоны).

Создание отдельной политики безопасности для защиты приложения

Для приложения защиты Сервера администрирования нужно создать отдельную политику безопасности. Эта политика должна отличаться от политики безопасности для клиентских устройств. Такой подход позволит задать максимально подходящие параметры безопасности для Сервера администрирования, не влияя при этом на уровень защиты других устройств.

Рекомендуется разделить устройства на группы, определив устройство с Сервером администрирования в отдельную группу администрирования, для которой вы затем можете создать специальную политику безопасности.

Модули защиты

Если отсутствуют особые рекомендации от производителя стороннего программного обеспечения, установленного на том же устройстве, что и Сервер администрирования, рекомендуется активировать и настроить все доступные модули защиты (после проверки их работы в течение определенного времени).

Настройка сетевого экрана устройства с Сервером администрирования

На устройстве с Сервером администрирования рекомендуется настроить сетевой экран таким образом, чтобы ограничить число устройств, с которых администраторы могут подключаться к Серверу администрирования через Консоль администрирования либо Kaspersky Security Center Web Console.

По умолчанию Сервер администрирования использует порт (см. раздел "Порты, используемые Kaspersky Security Center" на стр. [63](#)) 13291 для подключения к Консоли администрирования и порт 13299 для подключения к Kaspersky Security Center Web Console. Рекомендуется ограничить число устройств, с которых Сервер администрирования может управляться по этим портам.

Запрет на запуск панели управления

Если вы установили Сервер администрирования на устройство под управлением Microsoft Windows и используете приложение с модулем контроля запуска приложений, можно запретить запуск панели управления (control.exe) для непривилегированных пользователей, например для группы администраторов.

В таком случае, после создания указанных запрещающих правил контроля запуска приложений, пользователи с правами предустановленной роли Администратора потеряют возможность контролировать другие учетные записи сети, в том числе изменять имена учетных записей и пароли.

Управление защитой клиентских устройств

Ограничение добавления лицензионных ключей в инсталляционные пакеты

Инсталляционные пакеты хранятся в папке общего доступа Сервера администрирования, во вложенной папке Packages. Если лицензионные ключи будут добавлены в инсталляционный пакет, они могут быть доступны на чтение всем пользователям, имеющим права на чтение этой папки общего доступа.

Для того чтобы избежать компрометации лицензионного ключа, не рекомендуется добавлять лицензионные ключи в инсталляционные пакеты.

Рекомендуется использовать автоматическое распространение лицензионных ключей на управляемые устройства (см. раздел "Лицензирование управляемых приложений" см. стр. [389](#)), выполнять развертывание с помощью задачи Добавление лицензионного ключа для управляемого приложения, и добавлять код активации или файл ключа на устройства вручную.

Правила автоматического перемещения устройств между группами администрирования

Рекомендуется ограничить использование правил автоматического перемещения устройств (см. раздел "Создание правил автоматического перемещения устройств в группы администрирования" на стр. [335](#)) между группами администрирования.

Использование правил автоматического перемещения может привести к тому, что на устройство будут распространены политики, предоставляющие более широкий набор привилегий, чем было до перемещения.

Перемещение клиентского устройства в другую группу администрирования может привести к распространению на него параметров политик. Эти параметры политик могут быть нежелательны к распространению на гостевые и недоверенные устройства.

Эта рекомендация, не относится к первоначальному распределению устройств по группам администрирования (см. раздел "Настройка защиты управляемых приложений" на стр. [127](#)).

Требования к безопасности к устройствам с точками распространения и шлюзам соединений

Устройства с установленным Агентом администрирования могут использоваться в качестве точки распространения и выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства в группе.
- Выполнять удаленную установку приложений сторонних производителей и приложений "Лаборатории Касперского" на клиентские устройства.
- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.

Размещение точек распространения в сети организации используется для следующего:

- уменьшение нагрузки на Сервер администрирования;
- оптимизация трафика;
- предоставление Серверу администрирования доступа к устройствам в труднодоступных частях сети.

С учетом доступных возможностей рекомендуется защитить, в том числе физически, устройства, выполняющие роль точек распространения, от любого типа несанкционированного доступа.

Ограничение автоматического назначения точек распространения

Для упрощения администрирования и сохранения работоспособности сети рекомендуется воспользоваться автоматическим назначением точек распространения. Однако в промышленных и небольших сетях рекомендуется избегать автоматического назначения точек распространения, так как на точки распространения могут быть, например, переданы конфиденциальные сведения учетных записей, используемых для работы задач принудительной удаленной установки средствами операционной системы.

В промышленных и небольших сетях вы можете назначить точки распространения вручную.

При необходимости вы также можете просмотреть Отчет о работе точек распространения (см. раздел "Права доступа к функциям приложения" на стр. [810](#)).

Настройка защиты управляемых приложений

Политики управляемых приложений

Рекомендуется создать политику (см. раздел "Политики" на стр. [47](#)) для каждого вида используемого приложения и компонента Kaspersky Security Center (Агент администрирования, Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Agent и другие). Эта групповая политика должна применяться ко всем управляемым устройствам (корневой группе администрирования) или к отдельной группе, в которую автоматически попадают новые управляемые устройства в соответствии с настроенными правилами перемещения.

Установка пароля на выключение защиты и удаление приложения

Чтобы злоумышленники не могли отключить приложения безопасности "Лаборатории Касперского", рекомендуется установить пароль для выключения защиты и удаления приложений безопасности "Лаборатории Касперского". Вы можете установить пароль, например, для Kaspersky Endpoint Security

для Windows <https://support.kaspersky.com/KESWin/12.6/en-US/123303.htm>, Kaspersky Security для Windows Servers, Агента администрирования и других программ «Лаборатории Касперского». После включения защиты паролем рекомендуется заблокировать эти параметры, закрыв их "замком".

Указание пароля для ручного подключения клиентского устройства к Серверу администрирования (утилита klmover)

Утилита klmover позволяет вручную подключить клиентское устройство к Серверу администрирования. При установке на клиентское устройство Агента администрирования утилита автоматически копируется в папку установки Агента администрирования.

Чтобы злоумышленники не могли вывести устройства из-под контроля вашего Сервера администрирования, настоятельно рекомендуется включить защиту паролем для запуска утилиты klmover. Чтобы включить защиту паролем, в параметрах политики Агента администрирования выберите параметр **Использовать пароль деинсталляции**.

Утилита klmover требует прав локального администратора. Защиту паролем для запуска утилиты klmover можно не устанавливать для устройств, работающих без прав локального администратора.

При включении параметра **Использовать пароль деинсталляции** также включается защита паролем средствами Cleaner (cleaner.exe).

Использование Kaspersky Security Network

Во всех политиках управляемых приложений и в свойствах Сервера администрирования рекомендуется использовать Kaspersky Security Network (KSN) (см. раздел "Kaspersky Security Network и Kaspersky Private Security Network" на стр. [873](#)) и принять актуальное Положение о KSN. При обновлении Сервера администрирования вы также можете принять обновленное Положение о KSN. Когда использование облачных служб запрещено законодательством или иными нормативными актами, вы можете не включать KSN.

Регулярная проверка управляемых устройств

Для всех групп устройств вам нужно создать задачу (см. раздел "Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security" на стр. [412](#)), периодически запускающую полную проверку устройств.

Обнаружение новых устройств

Рекомендуется должным образом настроить параметры обнаружения устройств (см. раздел "Обнаружение устройств" на стр. [324](#)): настроить интеграцию с Active Directory и указать диапазоны IP-адресов для обнаружения новых устройств.

В целях безопасности вы можете использовать группу администрирования по умолчанию, в которую попадают все новые устройства, и политики по умолчанию, применяемые к этой группе.

Определение папки общего доступа

Если Сервер администрирования развернут на устройстве под управлением Windows, при выборе существующей папки общего доступа (см. раздел "Шаг 11. Определение папки общего доступа" на стр. [242](#)), (которая используется, например, для размещения инсталляционных пакетов и хранилища обновляемых баз) рекомендуем убедиться, что права на чтение предоставлены группе "Все" (Everyone), а права на запись – группе KLAAdmins.

Обслуживание Сервера администрирования

Резервное копирование данных Сервера администрирования

Резервное копирование данных (см. раздел "Создание задачи резервного копирования данных" на стр. [724](#)) позволяет восстановить данные Сервера администрирования без их потери. По умолчанию задача резервного копирования создается автоматически после установки Kaspersky Security Center и выполняется периодически с сохранением резервных копий в соответствующей директории.

Пользователь может изменить параметры задачи резервного копирования:

- увеличить частоту резервного копирования;
- определить особую директорию для сохранения копий;
- изменить пароль для резервной копии.

При хранении резервных копий в директории, отличной от директории по умолчанию, рекомендуется ограничить ACL этой директории. Учетные записи Сервера администрирования и сервера базы данных Сервера администрирования должны иметь доступ на запись в этой директории.

Обслуживание Сервера администрирования

Обслуживание Сервера администрирования (см. раздел "обслуживание Сервера администрирования;" на стр. [918](#)) позволяет сократить объем базы данных, повысить производительность и надежность работы приложения. Рекомендуется обслуживать Сервер администрирования не реже раза в неделю.

Обслуживание Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания Сервера администрирования приложение выполняет следующие действия:

- проверяет базу данных на наличие ошибок;
- перестраивает индексы базы данных;
- обновляет статистику базы данных;
- сжимает базу данных (при необходимости).

Обновление операционной системы и стороннего программного обеспечения на устройстве с Сервером администрирования

Настоятельно рекомендуется регулярно выполнять установку обновлений операционной системы и стороннего программного обеспечения (см. раздел "Установка обновлений приложений сторонних производителей" на стр. [498](#)) на устройстве с Сервером администрирования.

Клиентским устройствам не требуется постоянное подключение к Серверу администрирования, поэтому после установки обновлений можно безопасно перезагрузить устройство с Сервером администрирования. Все события, зарегистрированные на клиентских устройствах во время простоя Сервера администрирования, отправляются на него после восстановления соединения.

Передача событий в сторонние системы

Мониторинг и отчеты

Для своевременного реагирования на проблемы безопасности вы можете настроить функции мониторинга и параметры отчетов.

Экспорт событий в SIEM-системы

Для максимально быстрого выявления проблем безопасности до того, как будет нанесен существенный ущерб, рекомендуется использовать передачу событий в SIEM-систему (см. раздел "Экспорт событий в SIEM-системы" на стр. [879](#)).

Уведомление по электронной почте о событиях аудита

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Для своевременного реагирования на возникновение нештатных ситуаций рекомендуется настроить отправку Сервером администрирования уведомлений (см. раздел "Настройка параметров уведомлений о событиях" на стр. [311](#)) о публикуемых им событиях аудита (см. раздел "Информационные события Сервера администрирования" на стр. [666](#)), критических событиях (см. раздел "Критические события Сервера администрирования" на стр. [638](#)), событиях отказа функционирования (см. раздел "События отказа функционирования Сервера администрирования" на стр. [646](#)) и предупреждениях (см. раздел "События предупреждения Сервера администрирования" на стр. [652](#)).

Поскольку события аудита являются внутрисистемными, они регистрируются редко и количество уведомлений о подобных событиях вполне приемлемо для почтовой рассылки.

Статистическая информация о работе Сервера администрирования

Для своевременного реагирования на проблемы безопасности рекомендуется настроить отправку статистической информации работы Сервера администрирования приложениям сторонних производителей (см. раздел "Использование SNMP для отправки статистики приложениям сторонних производителей" см. стр. [900](#)) с помощью протокола Simple Network Management Protocol (SNMP).

Рекомендации по безопасности сторонних информационных систем

Рекомендации по безопасности CIS Benchmarks

При использовании версий операционных систем, платформ виртуализации или серверов баз данных, поддерживаемых Сервером администрирования (см. раздел "Требования к Серверу администрирования" см. стр. [16](#)) и Агентом (см. раздел "Требования к Агенту администрирования" см. стр. [19](#)) администрирования, для тонкой настройки этих информационных систем рекомендуется применять методы защиты информации Center for Internet Security (CIS), если они существуют.

Center for Internet Security (CIS) <https://www.cisecurity.org/> – некоммерческая организация, занимающаяся повышением безопасности в области информационных технологий. В частности, CIS разрабатывает и распространяет стандарты безопасности, такие как CIS Controls и CIS Benchmarks. Эти стандарты представляют собой набор рекомендаций и практик по обеспечению безопасности информационных систем.

На портале CIS есть рекомендации <https://downloads.cisecurity.org/> для версий следующих информационных систем, поддерживаемых Сервером администрирования и Агентом администрирования:

- Операционные системы следующих семейств:
 - Windows для рабочих станций
 - Windows для серверов
 - Debian
 - Ubuntu
 - CentOS

- Oracle Linux
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- macOS
- Платформы виртуализации VMware
- Серверы баз данных:
 - Microsoft SQL Server
 - MySQL
 - MariaDB
 - PostgreSQL

Рекомендации по безопасности для операционной системы Astra Linux

При использовании операционной системы Astra Linux следует соблюдать рекомендации по безопасности, описанные в Red Book для соответствующей версии Astra Linux <https://wiki.astralinux.ru/display/doc/Red+Books+Astra+Linux>.

Рекомендации по безопасности для операционной системы РЕД ОС

При использовании операционной системы РЕД ОС следует использовать рекомендации по безопасности, описанные в официальной документации РЕД ОС <https://redos.red-soft.ru/base/manual/safe-redos%20/>.

Рекомендации по использованию приложений безопасности "Лаборатории Касперского"

Использование пароля KAdmin в Kaspersky Endpoint Security для Windows

Компьютером с установленным приложением Kaspersky Endpoint Security для Windows могут пользоваться несколько пользователей с разным уровнем компьютерной грамотности. Если у пользователей есть неограниченный доступ к приложению Kaspersky Endpoint Security для Windows и его параметрам, общий уровень защиты компьютера может быть снижен. Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security для Windows в соответствии с предоставленными им правами (например, разрешение на завершение работы приложения).

Один из способов ограничить доступ к приложению Kaspersky Endpoint Security для Windows и его параметрам – это использовать учетную запись KAdmin <https://support.kaspersky.com/help/KESWin/12.6/en-US/41045.htm>. Учетная запись KAdmin – это учетная запись администратора с неограниченным доступом к приложению Kaspersky Endpoint Security для Windows. Учетная запись KAdmin имеет право выполнять любое действие, защищенное паролем, в Kaspersky Endpoint Security для Windows. Права для учетной записи KAdmin не могут быть отозваны. Вы можете установить пароль для учетной записи KAdmin в свойствах политики Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/help/KESWin/12.6/en-US/123303.htm>. Администратор Kaspersky Endpoint Security для Windows несет полную ответственность за безопасное использование пароля для учетной записи KAdmin. Если в вашей организации есть собственная политика использования паролей, следуйте указаниям этой политики.

Чтобы защитить организацию от кражи пароля KAdmin, выполните следующие действия:

- **Общие требования.**

Не используйте имя учетной записи или часть имени в качестве пароля.

- **Требования к минимальной длине пароля.**

Создайте пароль, который содержит не менее 10 символов.

- **Требования использования нескольких типов символов.**

Задайте комплексный пароль, который содержит символы из разных категорий: буквы нижнего и верхнего регистров, цифры и специальные символы.

- **Требования к сроку действия пароля.**

Установите минимальный срок действия пароля в 90 дней. Новый пароль не должен совпадать ни с одним из последних 24 паролей.

Подготовка к развертыванию

В этом разделе описаны шаги, которые вам нужно выполнить перед развертыванием Kaspersky Security Center.

В этом разделе

Планирование развертывания Kaspersky Security Center	133
Сведения о производительности Сервера администрирования.....	156
Сетевые параметры для взаимодействия с внешними сервисами	159

Планирование развертывания Kaspersky Security Center

Этот раздел содержит информацию об оптимальных вариантах развертывания компонентов Kaspersky Security Center в сети организации в зависимости от следующих критериев:

- общего количества устройств;
- наличия организационно или географически обособленных подразделений (офисов, филиалов);
- наличия обособленных сетей, связанных узкими каналами;
- необходимости доступа к Серверу администрирования из интернета.

См. также:

Основной сценарий установки.....	56

В этом разделе

Типовые способы развертывания системы защиты.....	134
О планировании развертывания Kaspersky Security Center в сети организации.....	135
Выбор структуры защиты организации.....	136
Типовые конфигурации Kaspersky Security Center	137
Выбор СУБД для Сервера администрирования	139
Настройка сервера MariaDB x64 для работы с Kaspersky Security Center	141
Настройка сервера MySQL x64 для работы с Kaspersky Security Center	142
Настройка сервера PostgreSQL или Postgres Pro для работы с Kaspersky Security Center	143
Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android.....	143
Предоставление доступа к Серверу администрирования из интернета	144
О точках распространения.....	147
Расчет количества и конфигурации точек распространения.....	149
Иерархия Серверов администрирования.....	150
Виртуальные Серверы администрирования	150
Информация об ограничениях Kaspersky Security Center	151
Нагрузка на сеть.....	152
Отказоустойчивые конфигурации.....	156

Типовые способы развертывания системы защиты

В этом разделе описаны типовые способы развертывания системы защиты в сети организации с помощью Kaspersky Security Center.

Необходимо обеспечить защиту системы от несанкционированного доступа всех видов. Перед установкой приложения на устройство рекомендуется установить все доступные обновления безопасности для операционной системы и обеспечить физическую защиту Серверов администрирования и точек распространения.

Вы можете развернуть систему защиты в сети организации с помощью Kaspersky Security Center, используя следующие схемы развертывания:

- Развертывание системы защиты средствами Kaspersky Security Center одним из следующих способов:
 - через Консоль администрирования;
 - через Kaspersky Security Center Web Console.

Установка приложений "Лаборатории Касперского" на клиентские устройства и подключение клиентских устройств к Серверу администрирования происходит автоматически с помощью Kaspersky Security Center.

Основной схемой развертывания является развертывание системы защиты через Консоль администрирования. Использование Kaspersky Security Center Web Console позволяет запускать установку приложений "Лаборатории Касперского" через браузер.

- Развертывание системы защиты вручную с помощью автономных инсталляционных пакетов, сформированных в Kaspersky Security Center.

Установка приложений "Лаборатории Касперского" на клиентские устройства и рабочее место администратора производится вручную, параметры подключения клиентских устройств к Серверу администрирования задаются при установке Агента администрирования.

Этот вариант развертывания рекомендуется применять в случаях, когда невозможно провести удаленную установку.

Kaspersky Security Center также позволяет разворачивать систему защиты с помощью групповых политик Active Directory.

О планировании развертывания Kaspersky Security Center в сети организации

Один Сервер администрирования может обслуживать не более чем 100 000 устройств. Если общее количество устройств в сети организации превышает 100 000, следует разместить в сети организации несколько Серверов администрирования, объединенных в иерархию для удобства централизованного управления.

Если в составе организации есть крупные географически удаленные офисы (филиалы) с собственными администраторами, целесообразно разместить в этих офисах Серверы администрирования. В противном случае такие офисы следует рассматривать как обособленные сети, связанные узкими каналами, см. раздел "Типовая конфигурация: несколько крупных офисов с собственными администраторами (на стр. [138](#))".

При наличии обособленных сетей, связанных узкими каналами, в целях экономии трафика в таких сетях следует назначить один или несколько Агентов администрирования точками распространения (см. таблицу для расчета количества точек распространения (см. раздел "Расчет количества и конфигурации точек распространения" на стр. [149](#))). В этом случае все устройства обособленной сети будут получать обновления с таких "локальных центров обновлений". Точки распространения могут загружать обновления как с Сервера администрирования (поведение по умолчанию), так и с размещенных в интернете серверов "Лаборатории Касперского", см. раздел "Типовая конфигурация: множество небольших изолированных офисов (см. раздел "Типовая конфигурация: множество небольших удаленных офисов" на стр. [138](#))".

В разделе "Типовые конфигурации Kaspersky Security Center (на стр. [137](#))" приведены подробные описания типовых конфигураций Kaspersky Security Center. При планировании развертывания следует, в зависимости от структуры организации, выбрать наиболее подходящую типовую конфигурацию.

На этапе планирования развертывания следует рассмотреть необходимость задания Серверу администрирования специального сертификата X.509. Задание сертификата X.509 для Сервера администрирования может быть целесообразно в следующих случаях (неполный список):

- для инспекции SSL трафика посредством SSL termination proxy или для использования Reverse Proxy;
- для интеграции с инфраструктурой открытых ключей (PKI) организации;

- для задания желательных значений полей сертификата;
- для обеспечения желаемой криптографической стойкости сертификата.

Выбор структуры защиты организации

Выбор структуры защиты организации определяют следующие факторы:

- Топология сети организации.
- Организационная структура.
- Число сотрудников, отвечающих за защиту сети, и распределение обязанностей между ними.
- Аппаратные ресурсы, которые могут быть выделены для установки компонентов управления защитой.
- Пропускная способность каналов связи, которые могут быть выделены для работы компонентов защиты в сети организации.
- Допустимое время выполнения важных административных операций в сети организации. К важным административным операциям относятся, например, распространение обновлений антивирусных баз и изменение политик для клиентских устройств.

При выборе структуры защиты рекомендуется сначала определить имеющиеся сетевые и аппаратные ресурсы, которые могут использоваться для работы централизованной системы защиты.

Для анализа сетевой и аппаратной инфраструктуры рекомендуется следующий порядок действий:

1. Определить следующие параметры сети, в которой будет развертываться защита:
 - число сегментов сети;
 - скорость каналов связи между отдельными сегментами сети;
 - число управляемых устройств в каждом из сегментов сети;
 - пропускную способность каждого канала связи, которая может быть выделена для функционирования защиты.
2. Определить допустимое время выполнения ключевых операций администрирования для всех управляемых устройств.
3. Проанализировать информацию из пунктов 1 и 2, а также данные нагрузочного тестирования системы администрирования (см. раздел "Нагрузка на сеть" на стр. [152](#)). На основании проведенного анализа ответить на следующие вопросы:
 - Возможно ли обслуживание всех клиентов одним Сервером администрирования или требуется иерархия Серверов администрирования?
 - Какая аппаратная конфигурация Серверов администрирования требуется для обслуживания всех клиентов за время, определенное в пункте 2?
 - Требуется ли использование точек распространения для снижения нагрузки на каналы связи?

После ответа на перечисленные вопросы вы можете составить набор допустимых структур защиты организации.

В сети организации можно использовать одну из следующих типовых структур защиты:

- Один Сервер администрирования. Все клиентские устройства подключены к одному Серверу администрирования. Роль точки распространения выполняет Сервер администрирования.

- Один Сервер администрирования с точками распространения. Все клиентские устройства подключены к одному Серверу администрирования. В сети выделены клиентские устройства, выполняющие роль точек распространения.
- Иерархия Серверов администрирования. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. Роль точки распространения выполняет главный Сервер администрирования.
- Иерархия Серверов администрирования с точками распространения. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. В сети выделены клиентские устройства, выполняющие роль точек распространения.

См. также:

Типовая конфигурация точек распространения: один офис.....	686
Типовая конфигурация: несколько крупных офисов с собственными администраторами	138
Типовая конфигурация: множество небольших удаленных офисов.....	138
Основной сценарий установки.....	56

Типовые конфигурации Kaspersky Security Center

В этом разделе описаны следующие типовые конфигурации размещения компонентов Kaspersky Security Center в сети организации:

- один офис;
- несколько крупных географически распределенных офисов с собственными администраторами;
- множество небольших географически распределенных офисов.

См. также:

Основной сценарий установки.....	56

В этом разделе

Типовая конфигурация: один офис	137
Типовая конфигурация: несколько крупных офисов с собственными администраторами	138
Типовая конфигурация: множество небольших удаленных офисов.....	138

Типовая конфигурация: один офис

В сети организации может быть размещен один или несколько Серверов администрирования. Количество Серверов может быть выбрано как исходя из наличия доступного аппаратного обеспечения, так и в зависимости от общего количества управляемых устройств.

Один Сервер администрирования может обслуживать до 100 000 устройств. Нужно учесть возможность увеличения количества управляемых устройств в ближайшем будущем: может оказаться желательным подключение несколько меньшего количества устройств к одному Серверу администрирования.

Серверы администрирования могут быть размещены как во внутренней сети, так и в демилитаризованной зоне, в зависимости от того, нужен ли доступ к Серверам администрирования из интернета.

Если Серверов несколько, рекомендуется объединить их в иерархию. Наличие иерархии Серверов администрирования позволяет избежать дублирования политик и задач, работать со всем множеством управляемых устройств, как если бы они все управлялись одним Сервером администрирования (то есть выполнять поиск устройств, создавать выборки устройств, создавать отчеты).

См. также:

О точках распространения	147
Порты, используемые Kaspersky Security Center	63
Основной сценарий установки	56

Типовая конфигурация: несколько крупных удаленных офисов с собственными администраторами

При наличии нескольких крупных удаленных офисов следует рассмотреть возможность размещения Серверов администрирования в каждом из офисов. По одному или по несколько Серверов администрирования в каждом офисе, в зависимости от количества клиентских устройств и доступного аппаратного обеспечения. В таком случае каждый из офисов может быть рассмотрен как "Типовая конфигурация: один офис (на стр. [137](#))". Для упрощения администрирования все Серверы администрирования следует объединить в иерархию, возможно, многоуровневую.

При наличии сотрудников, которые перемещаются между офисами вместе с устройствами (ноутбуками), в политике Агента администрирования следует создать профили подключения Агента администрирования. Профили подключения Агента администрирования поддерживают только устройства с операционными системами Windows и macOS.

См. также:

О профилях соединения для автономных пользователей	303
Типовая конфигурация: один офис	137
Порты, используемые Kaspersky Security Center	63

Типовая конфигурация: множество небольших удаленных офисов

Эта типовая конфигурация предусматривает один главный офис и множество небольших удаленных офисов, которые могут связываться с главным офисом через интернет. Каждый из удаленных офисов находится за Network Address Translation (далее также NAT), то есть подключение из одного удаленного офиса в другой невозможно, офисы изолированы друг от друга.

В главном офисе следует поместить Сервер администрирования, а в остальных офисах назначить по одной или по несколько точек распространения. Так как связь между офисами осуществляется через интернет, целесообразно создать для точек распространения задачу *Загрузка обновлений в хранилища точек распространения*, так, чтобы точки распространения загружали обновления не с Сервера

администрирования, а непосредственно с серверов "Лаборатории Касперского", локальной или сетевой папок.

Если в удаленном офисе часть устройств не имеет прямого доступа к Серверу администрирования (например, доступ к Серверу администрирования осуществляется через интернет, но доступ в интернет есть не у всех устройств), то точки распространения следует переключить в режим шлюза. В таком случае Агенты администрирования на устройствах в удаленном офисе будут подключаться (с целью синхронизации) к Серверу администрирования не напрямую, а через шлюз.

Поскольку Сервер администрирования, скорее всего, не сможет опрашивать сеть в удаленном офисе, целесообразно возложить выполнение этой функции на одну из точек распространения.

Сервер администрирования не сможет посылать уведомления на порт 15000 UDP управляемым устройствам, размещенным за NAT в удаленном офисе. Для решения этой проблемы вы можете включить в свойствах устройств, являющихся точками распространения, режим постоянного соединения с Сервером администрирования (флажок **Не разрывать соединение с Сервером администрирования**). Этот режим доступен, если общее количество точек распространения не превышает 300. Используйте push-серверы, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Дополнительную информацию см. в следующих разделах: Использование точки распространения в качестве извещающего сервера (на стр. [697](#)).

См. также:

О точках распространения	147
Предоставление доступа к Серверу администрирования из интернета	144
Порты, используемые Kaspersky Security Center	63

Выбор СУБД для Сервера администрирования

При выборе СУБД, используемой Сервером администрирования, следует руководствоваться количеством устройств, которые обслуживает Сервер администрирования.

В таблице ниже перечислены допустимые варианты СУБД и рекомендации и ограничения их использования.

Таблица 25. Рекомендации и ограничения СУБД

СУБД	Рекомендации и ограничения
SQL Server Express Edition 2012 и выше	Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 10 000 устройств и не собираетесь использовать компонент Контроль приложений для управляемых устройств. Недопустимо совместное использование СУБД SQL Server Express Edition Сервером администрирования и какого-либо другого приложения.
Локальный SQL Server Edition, отличный от Express, 2012 и выше	Нет ограничений.
Удаленный SQL Server Edition, отличный от Express, 2012 и выше	Допустимо только в случае, если оба устройства находятся в одном домене Windows; если домены разные, то между ними должно быть установлено двустороннее отношение доверия.
Локальный или удаленный MySQL 5.5, 5.6 или 5.7 (версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4 и 5.5.5 не поддерживаются)	Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 10 000 устройств и не собираетесь использовать компонент Контроль приложений для управляемых устройств.
Локальный или удаленный MySQL 8.0.20 или выше	Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 50 000 устройств и не собираетесь использовать компонент Контроль приложений для управляемых устройств.
Локальная или удаленная версия MariaDB (см. поддерживаемые версии (см. раздел "Аппаратные и программные требования" см. стр. 29))	Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 20 000 устройств и не собираетесь использовать компонент Контроль приложений для управляемых устройств.
PostgreSQL, Postgres Pro (см. поддерживаемые версии (см. раздел "Аппаратные и программные требования" см. стр. 29))	Используйте эту СУБД, если вы планируете использовать один Сервер администрирования, менее чем для 50 000 устройств, и не собираетесь использовать компонент Контроль приложений для управляемых устройств.

Если в качестве СУБД вы используете SQL Server 2019 и у вас нет накопительного исправления CU12 или выше, после установки Kaspersky Security Center необходимо выполнить следующие действия:

1. Подключитесь к SQL-серверу с помощью SQL Management Studio.
2. Выполните следующую команду (если вы выбрали другое имя для базы данных (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. 238), используйте это имя вместо KAV):

```
USE KAV
```

```
GO
```

```
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
```

```
GO
```

3. Перезапустите службу SQL Server 2019.

В противном случае использование SQL Server 2019 может завершиться с ошибкой, например, "Во 'внутреннем' пуле ресурсов недостаточно памяти для выполнения запроса".

Настройка сервера MariaDB x64 для работы с Kaspersky Security Center

Kaspersky Security Center поддерживает СУБД MariaDB. Дополнительные сведения о поддерживаемых версиях MariaDB см. в разделе Аппаратные и программные требования (см. стр. [29](#)).

Если вы используете СУБД MariaDB для Kaspersky Security Center, включите поддержку InnoDB и хранилища MEMORY, а также поддержку кодировок UTF-8 и UCS-2.

Рекомендуемые параметры для файла my.ini

► Чтобы настроить файл my.ini:

1. Откройте файл my.ini <https://mariadb.com/kb/en/configuring-mariadb-with-option-files/> с помощью текстового редактора.
2. Добавьте следующие строки в раздел [mysqld] файла my.ini:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=<value>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Значение `innodb_buffer_pool_size` должно быть не менее 80 процентов от ожидаемого размера базы данных KAV. Обратите внимание, что указанная память выделяется при запуске сервера. Если размер базы данных меньше указанного размера буфера, выделяется только необходимая память. Если вы используете MariaDB 10.4.3 или более раннюю версию, фактический размер выделенной памяти примерно на 10 процентов превышает указанный размер буфера.

Рекомендуется использовать значение параметра `innodb_flush_log_at_trx_commit=0`, поскольку значения "1" или "2" отрицательно влияют на скорость работы MariaDB. Убедитесь, что для параметра `innodb_file_per_table` установлено значение 1.

Для MariaDB 10.6 дополнительно введите в раздел [mysqld] следующие строки:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

По умолчанию надстройки оптимизатора `join_cache_incremental`, `join_cache_hashed` и `join_cache_bka` включены. Если эти надстройки не включены, их необходимо включить.

► Чтобы проверить, включены ли надстройки оптимизатора:

1. В клиентской консоли MariaDB выполните команду:

```
SELECT @@optimizer_switch;
```

2. Убедитесь, что вывод содержит следующие строки:

```
join_cache_incremental=on  
join_cache_hashed=on  
join_cache_bka=on
```

Если эти строки присутствуют и содержат значение `on`, то надстройки оптимизатора включены.

Если эти строки отсутствуют или имеют значение `off`, выполните следующее:

1. Откройте файл `my.ini` с помощью текстового редактора.
2. Добавьте следующие строки в раздел `[mysqld]` файла `my.ini`:

```
optimizer_switch='join_cache_incremental=on'  
optimizer_switch='join_cache_hashed=on'  
optimizer_switch='join_cache_bka=on'
```

Надстройки `join_cache_incremental`, `join_cache_hash` и `join_cache_bka` включены.

Настройка сервера MySQL x64 для работы с Kaspersky Security Center

Если вы используете СУБД MySQL для Kaspersky Security Center, включите поддержку InnoDB и хранилища MEMORY, а также поддержку кодировок UTF-8 и UCS-2.

Рекомендуемые параметры для файла `my.ini`

► Чтобы настроить файл `my.ini`:

1. Откройте файл `my.ini` с помощью текстового редактора.
2. Добавьте следующие строки в раздел `[mysqld]` файла `my.ini`:

```
sort_buffer_size=10M  
join_buffer_size=20M  
tmp_table_size=600M  
max_heap_table_size=600M  
key_buffer_size=200M  
innodb_buffer_pool_size=реальное значение должно быть не менее 80% от ожидаемого  
размера базы данных KAV  
innodb_thread_concurrency=20  
innodb_flush_log_at_trx_commit=0 (в большинстве случаев сервер использует  
небольшие транзакции)  
innodb_lock_wait_timeout=300  
max_allowed_packet=32M  
max_connections=151  
max_prepared_stmt_count=12800  
table_open_cache=60000  
table_open_cache_instances=4  
table_definition_cache=60000
```

Обратите внимание, что память, указанная в `innodb_buffer_pool_size`, выделяется при запуске сервера. Если размер базы данных меньше указанного размера буфера, выделяется только необходимая память. Фактический размер выделенной памяти примерно на 10 процентов превышает указанный размер буфера. Дополнительную информацию см. в документации MySQL https://dev.mysql.com/doc/refman/8.0/en/innodb-parameters.html#sysvar_innodb_buffer_pool_size.

Рекомендуется использовать значение параметра `innodb_flush_log_at_trx_commit = 0`, поскольку значения "1" или "2" отрицательно влияют на скорость работы MySQL. Убедитесь, что для параметра `innodb_file_per_table` установлено значение 1.

Настройка сервера PostgreSQL или Postgres Pro для работы с Kaspersky Security Center

Kaspersky Security Center поддерживает СУБД PostgreSQL и Postgres Pro. Если вы используете одну из этих СУБД, рассмотрите возможность настройки параметров сервера СУБД для оптимизации работы СУБД с Kaspersky Security Center.

Путь по умолчанию к конфигурационному файлу: `C:\Program Files\PostgreSQL\<ВЕРСИЯ>\data\postgresql.conf`

Рекомендуемые параметры для PostgreSQL и Postgres Pro:

- `shared_buffers` = 25 процентов от объема оперативной памяти устройства, на котором установлена СУБД

Если оперативной памяти меньше 1 ГБ, то оставьте значение по умолчанию.

- `max_stack_depth` = 2MB
- `temp_buffers` = 24MB
- `work_mem` = 16MB
- `max_connections` = 151
- `max_parallel_workers_per_gather` = 0
- `maintenance_work_mem` = 128 MB

Убедитесь, что для параметра `standard_conforming_strings` значение по умолчанию установлено `on`. Примените конфигурацию или перезапустите службу после обновления файла `postgresql.conf`.

Дополнительную информацию см. в документации PostgreSQL <https://www.postgresql.org/docs/current/config-setting.html>.

Подробнее о том, как создавать и настраивать учетные записи для PostgreSQL и Postgres Pro, см. в следующем разделе: Настройка учетных записей для работы с PostgreSQL и Postgres Pro (на стр. [222](#)).

Подробную информацию о параметрах сервера PostgreSQL и Postgres Pro, а также о том, как указать эти параметры, см. в соответствующей документации по СУБД.

Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android

Управление мобильными устройствами с установленным приложением Kaspersky Endpoint Security для Android™ (далее KES-устройства) осуществляется с помощью Сервера администрирования. Kaspersky Security Center поддерживает следующие возможности управления KES-устройствами:

- работа с мобильными устройствами как с клиентскими устройствами:

- членство в группах администрирования;
- мониторинг, например просмотр статусов, событий и отчетов;
- изменение локальных параметров и назначение политик для приложения Kaspersky Endpoint Security для Android;
- централизованная отправка команд;
- удаленная установка пакетов мобильных приложений.

Сервер администрирования управляет KES-устройствами по протоколу TLS, TCP-порт 13292.

См. также:

Предоставление доступа к Серверу администрирования из интернета[144](#)

Предоставление доступа к Серверу администрирования из интернета

В ряде случаев необходимо предоставить доступ к Серверу администрирования из интернета:

- Регулярное обновление баз, модулей приложений и приложений "Лаборатории Касперского".
- Обновление приложений сторонних производителей

По умолчанию Сервер администрирования не требует подключения к интернету для установки обновлений приложений Microsoft на управляемые устройства. Например, управляемые устройства могут загружать обновления приложений Microsoft непосредственно с серверов обновлений Microsoft или с Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации. Сервер администрирования должен быть подключен к интернету в следующих случаях:

- Когда вы используете Сервер администрирования в роли WSUS-сервера.
- Для установки обновлений приложений сторонних производителей, отличных от приложений Microsoft.
- Заккрытие уязвимостей в приложениях сторонних производителей

Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:

- Составление списка рекомендуемых исправлений уязвимостей в приложениях Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
- Заккрытие уязвимостей в приложениях сторонних производителей, отличных от приложений Microsoft.
- Для управления устройствами (ноутбуками) автономных пользователей.
- Для управления устройствами, находящимися в удаленных офисах.
- При взаимодействии с главным или подчиненными Серверами администрирования, находящимися в удаленных офисах.
- для управления мобильными устройствами.

В этом разделе рассмотрены типичные способы обеспечения доступа к Серверу администрирования из интернета. Во всех случаях предоставления доступа к Серверу администрирования из интернета может понадобиться задать Серверу администрирования специальный сертификат.

См. также:

Основной сценарий установки.....	56

В этом разделе

Доступ из интернета: Сервер администрирования в локальной сети	145
Доступ из интернета: Сервер администрирования в демилитаризованной зоне.....	145
Доступ из интернета: Использовать в качестве шлюза соединений в демилитаризованной зоне ..	146

Доступ из интернета: Сервер администрирования в локальной сети

Если Сервер администрирования располагается во внутренней сети организации, вы можете сделать порт Сервера администрирования 13000 TCP доступным извне с помощью механизма "Port Forwarding". Если требуется управление мобильными устройствами, вы можете сделать TCP-порт 13292 доступным.

См. также:

Порты, используемые Kaspersky Security Center	63
Основной сценарий установки.....	56
Схемы трафика данных и использования портов.....	87

Доступ из интернета: Сервер администрирования в демилитаризованной зоне

Если Сервер администрирования располагается в демилитаризованной зоне сети организации, у него отсутствует доступ во внутреннюю сеть организации. Как следствие, возникают следующие ограничения:

- Сервер администрирования не может самостоятельно обнаруживать новые устройства.
- Сервер администрирования не может выполнять первоначальное развертывание Агента администрирования посредством принудительной установки на устройства внутренней сети организации.

Речь идет только о первоначальной установке Агента администрирования. Последующие обновления версии Агента администрирования или установка приложения безопасности уже могут быть выполнены Сервером администрирования. Однако первоначальное развертывание Агентов администрирования может быть выполнено иными средствами, например, при помощи групповых политик Microsoft Active Directory.

- Сервер администрирования не может посылать управляемым устройствам уведомления на порт 15000 UDP, что не является критичным для работы Kaspersky Security Center.
- Сервер администрирования не может опрашивать Active Directory. Однако результаты опроса Active Directory не нужны в большинстве сценариев.

Если описанные выше ограничения критичны, они могут быть сняты при помощи точек распространения, размещенных в сети организации:

- Для выполнения первоначального развертывания на устройствах без Агента администрирования следует предварительно установить Агент администрирования на одно из устройств и назначить это устройство точкой распространения. В результате первоначальная установка Агента администрирования на прочие устройства будет выполняться Сервером администрирования через эту точку распространения.
- Для обнаружения новых устройств во внутренней сети организации и для опроса Active Directory следует на одной из точек распространения включить желаемые виды опроса сети.

Для успешной отправки уведомлений управляемым устройствам, размещенным во внутренней сети организации, на порт 15000 UDP, следует покрыть всю сеть предприятия точками распространения. В свойствах назначенных точек распространения установите флажок **Не разрывать соединение с Сервером администрирования**. В результате Сервер администрирования будет иметь постоянную связь с точками распространения, а точки распространения смогут посылать уведомления на порт 15000 UDP устройствам, размещенным во внутренней сети организации (см. раздел "О точках распространения" на стр. [147](#)) (это может быть IPv4-сеть или IPv6-сеть).

См. также:

Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете.....[101](#)

Доступ из интернета: Использовать в качестве шлюза соединений в демилитаризованной зоне

Сервер администрирования может располагаться во внутренней сети организации, а в демилитаризованной зоне сети может находиться устройство с Агентом администрирования, работающим в качестве шлюза соединения (см. раздел "Шлюз соединения" см. стр. [54](#)) с обратным направлением подключения (Сервер администрирования устанавливает соединение с Агентом администрирования). В этом случае для организации доступа из интернета нужно выполнить следующие условия:

- На устройство, находящееся в демилитаризованной зоне, следует установить (см. раздел "Локальная установка Агента администрирования" на стр. [193](#)) Агент администрирования. При установке Агента администрирования в окне **Шлюз соединения** мастера установки выберите **Использовать в качестве шлюза соединений в демилитаризованной зоне**.
- Устройство с установленным шлюзом соединения необходимо добавить в качестве точки распространения (см. раздел "Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения" см. стр. [693](#)). Когда вы добавляете шлюз соединения, в окне **Добавление точки распространения** выберите параметр **Выбрать → Добавить шлюз соединений, находящийся в демилитаризованной зоне, по адресу**.
- Чтобы использовать интернет для подключения внешних настольных компьютеров к Серверу администрирования, необходимо изменить инсталляционный пакет Агента администрирования. В свойствах созданного инсталляционного пакета (см. раздел "Подключение внешних настольных компьютеров к Серверу администрирования" см. стр. [302](#)) выберите параметр **Дополнительно → Подключаться к Серверу администрирования через шлюз соединения** и укажите вновь созданный шлюз соединения.

Для шлюза соединений, находящегося в демилитаризованной зоне, Сервер администрирования создает сертификат, подписанный сертификатом Сервера администрирования. Если администратор принял решение задать Серверу администрирования пользовательский сертификат, то это следует сделать до создания шлюза соединений в демилитаризованной зоне.

При наличии сотрудников с ноутбуками, которые могут подключаться к Серверу администрирования как из локальной сети, так и из интернета, может быть целесообразно создать в политике Агента администрирования правило переключения Агента администрирования.

О точках распространения

Устройства с установленным Агентом администрирования могут быть использованы в качестве точки распространения. В этом режиме Агент администрирования может выполнять следующие функции:

- Раздавать обновления, причем обновления могут быть получены как с Сервера администрирования, так и с серверов "Лаборатории Касперского". В последнем случае для устройства, являющегося точкой распространения, должна быть создана задача *Загрузка обновлений в хранилища точек распространения* (см. раздел "Создание задачи загрузки обновлений в хранилища точек распространения" на стр. [474](#)):
- Устанавливать программное обеспечение на другие устройства, в том числе выполнять первоначальное развертывание Агентов администрирования на устройствах.
- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.

Размещение точек распространения в сети организации преследует следующие цели:

- Уменьшение нагрузки на Сервер администрирования.
- Оптимизация трафика.
- Предоставление Серверу администрирования доступ к устройствам в труднодоступных частях сети организации. Наличие точки распространения в находящейся за NAT (по отношению к Серверу администрирования) сети позволяет Серверу администрирования выполнять следующие действия:
 - отправлять уведомления на устройства через UDP в IPv4-сети или IPv6-сети;
 - опрос IPv4-сети или IPv6-сети;
 - выполнять первоначальное развертывание;
 - использовать в качестве push-сервера (см. раздел "Использование точки распространения в качестве извещающего сервера" на стр. [697](#)).

Точка распространения назначается на группу администрирования. В этом случае областью действия точки распространения будут устройства, находящиеся в этой группе администрирования и всех ее подгруппах. При этом устройство, являющееся точкой распространения, не обязано находиться в группе администрирования, на которую она назначена.

Вы можете сделать точку распространения шлюзом соединений. В этом случае, устройства, находящиеся в области действия точки распространения, будут подключаться к Серверу администрирования не напрямую, а через шлюз. Данный режим полезен в сценариях, когда между Сервером администрирования и управляемыми устройствами невозможно прямое соединение.

Если вы используете устройство под управлением Linux в качестве точки распространения, настоятельно рекомендуется увеличить ограничения дескрипторов файлов для службы `klagent`, так как, если в область действия точки распространения входит много устройств, может не хватить максимального количества файлов, которые могут быть открыты по умолчанию.

См. также:

Настройка точек распространения и шлюзов соединений	685
Основной сценарий установки.....	56

Расчет количества и конфигурации точек распространения

Чем больше клиентских устройств содержит сеть, тем больше требуется точек распространения. Рекомендуется не отключать автоматическое назначение точек распространения. При включенном автоматическом назначении точек распространения Сервер администрирования назначает точки распространения, если число клиентских устройств достаточно велико, и определяет их конфигурацию.

Использование специально выделенных точек распространения

Если вы планируете использовать в качестве точек распространения какие-то определенные устройства (например, выделенные для этого серверы), то можно не использовать автоматическое назначение точек распространения. В этом случае убедитесь, что устройства, которые вы хотите назначить точками распространения, имеют достаточно свободного места на диске, их не отключают регулярно и на них выключен "спящий режим".

Таблица 26. Число уникально назначенных точек распространения в сети, содержащей один сегмент, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом из сегментов сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	Приемлемо: $(N/10\ 000 + 1)$, рекомендуется: $(N/5000 + 2)$, где N количество устройств в сети

Таблица 27. Число уникально назначенных точек распространения в сети, содержащей несколько сегментов, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10–100	1
Более 100	Приемлемо: $(N/10\ 000 + 1)$, рекомендуется: $(N/5000 + 2)$, где N количество устройств в сети

Использование клиентских устройств (рабочих станций) в качестве точек распространения

Если вы планируете использовать в качестве точек распространения обычное клиентское устройство (рабочую станцию), то рекомендуется назначать точку распространения, как показано в таблице ниже, чтобы избежать чрезмерной нагрузки на каналы связи и Сервер администрирования:

Таблица 28. Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит один сегмент сети, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом из сегментов сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	$(N/300 + 1)$, где N – число устройств в сети; не менее 3 точек распространения

Таблица 29. Число рабочих станций, выполняющих роль точек распространения в сети,

которая содержит несколько сегментов сети, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10–30	1
31–300	2
Более 300	(N/300 + 1), где N – число устройств в сети; не менее 3 точек распространения

Если точка распространения отключена или по другим причинам недоступна, то управляемые устройства из области действия этой точки распространения могут обращаться за обновлениями к Серверу администрирования.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....	455
Типовая конфигурация: множество небольших удаленных офисов.....	138

Иерархия Серверов администрирования.

У MSP может быть более одного Сервера администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики и задачи, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.

Главный Сервер администрирования получает данные только от неvirtуальных подчиненных Серверов администрирования в рамках перечисленных выше параметров. Это ограничение не распространяется на виртуальные Серверы администрирования, которые совместно используют базу данных со своим главным Сервером администрирования.

Виртуальные Серверы администрирования

В рамках физического Сервера администрирования можно создать несколько виртуальных Серверов администрирования, во многом подобных подчиненным Серверам. По сравнению с моделью разделения доступа, основанной на списках контроля доступа (ACL), модель виртуальных Серверов более функциональна и предоставляет большую степень изоляции. В дополнение к структуре групп администрирования, предназначенной для назначения устройствам политик и задач, каждый виртуальный Сервер администрирования имеет собственную группу нераспределенных устройств, собственные наборы отчетов, выборки устройств и события, инсталляционные пакеты, правила перемещения и т. д.

Функциональность виртуальных Серверов администрирования может быть использована как поставщиками услуг (xSP) для максимальной изоляции разных заказчиков друг от друга, так и крупными организациями со сложной структурой и большим количеством администраторов.

Виртуальные Серверы во многом подобны подчиненным Серверам администрирования, однако имеют следующие отличия:

- виртуальный Сервер не имеет большинства глобальных параметров и собственных TCP-портов;
- у виртуального Сервера не может быть подчиненных Серверов;
- у виртуального Сервера не может быть собственных виртуальных Серверов;
- на физическом Сервере администрирования видны устройства, группы, события и объекты с управляемых устройств (элементы карантина, реестра приложений и прочее) всех его виртуальных Серверов;
- виртуальный Сервер может сканировать сеть только посредством подключенных к нему точек распространения.

Информация об ограничениях Kaspersky Security Center

В таблице ниже приведены ограничения текущей версии Kaspersky Security Center.

Таблица 30. Ограничения Kaspersky Security Center

Тип ограничения	Значение
Максимальное количество управляемых устройств на один Сервер администрирования	100 000
Максимальное количество устройств, для которых выбран параметр Не разрывать соединение с Сервером администрирования	300
Максимальное количество групп администрирования	10 000
Максимальное количество хранимых событий	45 000 000
Максимальное количество политик	2000
Максимальное количество задач	2000
Максимальное суммарное количество объектов Active Directory (подразделений и учетных записей пользователей, устройств и групп безопасности)	1 000 000
Максимальное количество профилей в политике	100
Максимальное количество подчиненных Серверов у одного главного Сервера администрирования	500
Максимальное количество виртуальных Серверов администрирования	500
Максимальное количество устройств, которые может обслуживать одна точка распространения (точки распространения могут обслуживать только немобильные устройства)	10 000
Максимальное количество устройств, которые могут использовать один шлюз соединения	10 000, включая мобильные устройства
Максимальное количество мобильных устройств на один Сервер администрирования	100 000 минус количество стационарных управляемых устройств

Нагрузка на сеть

В этом разделе приводится информация об объеме сетевого трафика, которым обмениваются между собой клиентские устройства и Сервер администрирования в ходе выполнения ключевых административных сценариев.

Основная нагрузка на сеть связана с выполнением следующих административных сценариев:

- Первоначальное развертывание антивирусной защиты
- Первоначальное обновление антивирусных баз
- Синхронизация клиентского устройства с Сервером администрирования
- Регулярное обновление антивирусных баз
- Обработка событий на клиентских устройствах Сервером администрирования

В этом разделе

Первоначальное развертывание антивирусной защиты	152
Первоначальное обновление антивирусных баз	153
Синхронизация клиента с Сервером администрирования	153
Добавочное обновление антивирусных баз	154
Обработка событий клиентов Сервером администрирования	155
Расход трафика за сутки	155

Первоначальное развертывание антивирусной защиты

В этом разделе приведен расход трафика при установке на клиентском устройстве Агента администрирования версии и Kaspersky Endpoint Security для Windows (см. таблицу ниже).

Агент администрирования устанавливается путем принудительной установки, когда требуемые для установки файлы копируются Сервером администрирования в папку общего доступа на клиентском устройстве. После установки Агент администрирования получает дистрибутив Kaspersky Endpoint Security для Windows, используя соединение с Сервером администрирования.

Таблица 31. Расход трафика

Сценарий	Установка Агента администрирования для одного клиентского устройства	Установка Kaspersky Endpoint Security для Windows для одного клиентского устройства (с обновленными базами)	Совместная установка Агента администрирования и Kaspersky Endpoint Security для Windows
Трафик от клиентского устройства к Серверу администрирования, КБ	1638,4	7843,84	9707,52
Трафик от Сервера администрирования к клиентскому устройству, КБ	69 990,4	259 317,76	329 318,4
Общий трафик (для одного клиентского устройства), КБ	71 628,8	267 161,6	339 025,92

После установки Агентов администрирования на клиентские устройства можно назначить одно из устройств в группе администрирования точкой распространения. Он будет использоваться для распространения инсталляционных пакетов. В этом случае объем трафика, передаваемого при первоначальном развертывании антивирусной защиты, существенно отличается в зависимости от того, используется ли многоадресная IP-рассылка.

В случае использования многоадресной IP-рассылки инсталляционные пакеты рассылаются один раз по всем включенным устройствам в группе администрирования. Таким образом, общий трафик уменьшится примерно в N раз, где N – общее число включенных устройств в группе администрирования. Если многоадресная IP-рассылка не используется, общий трафик совпадает с трафиком загрузки дистрибутивов с Сервера администрирования. При этом источником инсталляционных пакетов является точка распространения, а не Сервер администрирования.

Первоначальное обновление антивирусных баз

Скорости трафика при первичном обновлении антивирусных баз (при первом запуске задачи обновления баз на клиентском устройстве) следующие:

- Трафик от клиентского устройства к Серверу администрирования:
- Трафик от Сервера администрирования к клиентскому устройству:
- Общий трафик (для одного клиентского устройства):

Данные могут несколько отличаться в зависимости от текущей версии антивирусных баз.

Синхронизация клиента с Сервером администрирования

Этот сценарий характеризует состояние системы администрирования в случае, когда происходит активная синхронизация данных между клиентским устройством и Сервером администрирования. Клиентские устройства подключаются к Серверу администрирования с периодом, заданным администратором. Сервер администрирования сравнивает состояние данных на клиентском устройстве с состоянием данных на Сервере, регистрирует данные о последнем подключении клиентского устройства в базе данных и проводит синхронизацию данных.

В разделе приведена информация о расходе трафика для основных административных сценариев при подключении клиента к Серверу администрирования с синхронизацией (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусных баз.

Таблица 32. Расход трафика

Сценарий	Трафик от клиентских устройств к Серверу администрирования, КБ	Трафик от Сервера администрирования к клиентским устройствам, КБ	Общий трафик (для одного клиентского устройства), КБ
Первоначальная синхронизация до обновления баз на клиентском устройстве	699,44	568,42	1267,86
Первоначальная синхронизация после обновления баз на клиентском устройстве	735,8	4474,88	5210,68
Синхронизация при отсутствии изменений на клиентском устройстве и на Сервере администрирования	11,99	6,73	18,72
Синхронизация при изменении одного параметра в политике группы	9,79	11,39	21,18
Синхронизация при изменении одного параметра в групповой задаче	11,27	11,72	22,99
Принудительная синхронизация при отсутствии изменений на клиентском устройстве	77,59	99,45	177,04

Объем общего трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Объем трафика при первоначальной синхронизации до и после обновления баз указан для следующих случаев:

- установка на клиентское устройство Агента администрирования и приложения безопасности;
- перенос клиентского устройства в группу администрирования;
- применение к клиентскому устройству политики и задач, созданных для группы по умолчанию.

В таблице указан объем трафика при изменении одного из параметров защиты, входящих в параметры политики Kaspersky Endpoint Security. Данные для других параметров политики могут отличаться от данных, представленных в таблице.

Добавочное обновление антивирусных баз

Расход трафика при инкрементальном обновлении антивирусных баз спустя 20 часов после предыдущего обновления следующий:

- Трафик от клиентского устройства к Серверу администрирования, КБ
- Трафик от Сервера администрирования к клиентскому устройству:
- Общий трафик (для одного клиентского устройства):

Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусных баз.

Объем трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Обработка событий клиентов Сервером администрирования

В этом разделе приведен расход трафика при возникновении на клиентском устройстве события "Найден вирус", информация о котором передается на Сервер администрирования и регистрируется в базе данных (см. таблицу ниже).

Таблица 33. Расход трафика

Сценарий	Передача на Сервер администрирования данных при наступлении события "Найден вирус"	Передача на Сервер администрирования данных при наступлении девяти событий "Найден вирус"
Трафик от клиентского устройства к Серверу администрирования, КБ	49,66	64,05
Трафик от Сервера администрирования к клиентскому устройству, КБ	28,64	31,97
Общий трафик (для одного клиентского устройства), КБ	78,3	96,02

Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусного приложения и в зависимости от того, какие именно события определены в политике как требующие регистрации в базе данных Сервера администрирования.

Расход трафика за сутки

В этом разделе приведена информация о расходе трафика за сутки работы системы администрирования в состоянии "покоя", когда не происходит изменений данных ни со стороны клиентских устройств, ни со стороны Сервера администрирования (см. таблицу ниже).

Данные, приведенные в таблице, характеризуют состояние сети после стандартной установки Kaspersky Security Center и завершения работы мастера первоначальной настройки. Период синхронизации клиентского устройства с Сервером администрирования составлял 20 минут, загрузка обновлений в хранилище Сервера администрирования происходила каждый час.

Таблица 34. Уровень трафика за сутки в состоянии простоя

Поток трафика	Значение
Трафик от клиентского устройства к Серверу администрирования, КБ	3235,84
Трафик от Сервера администрирования к клиентскому устройству, КБ	64 378,88
Общий трафик (для одного клиентского устройства), КБ	67 614,72

Отказоустойчивые конфигурации

Сведения о производительности Сервера администрирования

В разделе представлены результаты тестирования производительности Сервера администрирования для разных аппаратных конфигураций, а также ограничения на подключение управляемых устройств к Серверу администрирования.

Ограничения подключений к Серверу администрирования

Сервер администрирования поддерживает управление до 100 000 устройств без потери производительности.

Ограничения на подключения к Серверу администрирования без потери производительности:

- Один Сервер администрирования может поддерживать до 500 виртуальных Серверов администрирования.
- Главный Сервер администрирования поддерживает одновременно не более 1000 сессий.
- Виртуальные Серверы администрирования поддерживают одновременно не более 1000 сессий.

См. также:

Результаты тестов производительности Сервера администрирования[157](#)

Результаты тестов производительности Сервера администрирования

Результаты тестов производительности Сервера администрирования позволили определить максимальные количества клиентских устройств, с которыми Сервер администрирования может выполнить синхронизацию за указанные промежутки времени. Вы можете использовать эту информацию для выбора оптимальной схемы развертывания антивирусной защиты в компьютерных сетях.

Для тестирования использовались устройства со следующими аппаратными конфигурациями (см. таблицы ниже):

Таблица 35. Аппаратная конфигурация Сервера администрирования

Параметр	Значение
Процессор	Intel Xeon CPU E5630, тактовая частота 2,53 ГГц, 2 сокет, 8 ядер, 16 логических процессоров
ОЗУ	26 ГБ
Жесткий диск	IBM ServeRAID M5014 SCSI Disk Device, 487 ГБ
Операционная система	Microsoft Windows Server 2019 Standard, версия 10.0.17763, сборка 17763
Сеть	QLogic BCM5709C Gigabit Ethernet (NDIS VBD Client)

Таблица 36. Аппаратная конфигурация устройства с SQL Server

Параметр	Значение
Процессор	Intel Xeon CPU X5570, тактовая частота 2,93 ГГц, 2 сокет, 8 ядер, 16 логических процессоров
ОЗУ	32 ГБ
Жесткий диск	Adaptec Array SCSI Disk Device, 2047 ГБ
Операционная система	Microsoft Windows Server 2019 Standard, версия 10.0.17763, сборка 17763
Сеть	Intel 82576 Gigabit

Сервер администрирования поддерживал создание 500 виртуальных Серверов администрирования.

Период синхронизации составлял по 15 минут на каждые 10 000 управляемых устройств (см. таблицу ниже).

Таблица 37. Обобщенные результаты нагрузочного тестирования Сервера администрирования

Период синхронизации, мин	Количество управляемых устройств
15	10 000
30	20 000
45	30 000
60	40 000

Период синхронизации, мин	Количество управляемых устройств
75	50 000
90	60 000
105	70 000
120	80 000
135	90 000
150	100 000

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать приложение для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

Результаты тестирования производительности прокси-сервера KSN

Если ваша корпоративная сеть включает в себя большое количество клиентских устройств, и они используют Сервер администрирования в качестве прокси-сервера KSN, Сервер администрирования должен удовлетворять определенным аппаратным требованиям, чтобы обрабатывать запросы с клиентских устройств. Вы можете использовать результаты тестирования ниже для оценки загрузки Сервера администрирования в вашей сети и планирования аппаратных ресурсов, для обеспечения нормальной работы службы прокси-сервера KSN.

В таблице ниже приведена конфигурация аппаратного обеспечения Сервера администрирования и SQL Server. Эта конфигурация была использована для тестирования.

Таблица 38. Аппаратная конфигурация Сервера администрирования

Параметр	Значение
Процессор	Intel Xeon CPU E5450, тактовая частота 3,00 ГГц, 2 сокет, 8 ядер, 16 логических процессоров
ОЗУ	32 ГБ
Операционная система	Microsoft Windows Server 2016 Standard

Таблица 39. Аппаратная конфигурация SQL Server

Параметр	Значение
Процессор	Intel Xeon CPU E5450, тактовая частота 3,00 ГГц, 2 сокет, 8 ядер, 16 логических процессоров
ОЗУ	32 ГБ
Операционная система	Microsoft Windows Server 2019 Standard

В таблице ниже приведены результаты тестирования.

Таблица 40. Обобщенные результаты тестирования производительности прокси-сервера KSN

Параметр	Значение
Максимальное количество обработанных запросов в секунду	4914
Максимальное использование процессора	36%

Сетевые параметры для взаимодействия с внешними сервисами

Kaspersky Security Center использует следующие сетевые параметры для взаимодействия с внешними сервисами.

Таблица 41. Сетевые параметры

Сетевые параметры	Адрес	Описание
Порт: 443 Протокол: HTTPS	activation-v2.kaspersky.com/activation-service/activation-service.svc	Активация приложения.

Сетевые параметры	Адрес	Описание
Порт: 443 Протокол: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Обновление баз, модулей приложений и приложений "Лаборатории Касперского" (см. раздел "Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"" см. стр. 460).
Порт: 443 Протокол: HTTPS	https://downloads.upd.kaspersky.com	- Обновление баз, модулей приложений и приложений "Лаборатории Касперского" (см. раздел "Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"" см. стр. 460). - Проверка если серверы "Лаборатории Касперского" доступны. Kaspersky Security Center проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и модулей приложений "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы (см. раздел "Доступ к общедоступным DNS-серверам" на стр. 919).

Сетевые параметры	Адрес	Описание
Порт: 80 Протокол: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Обновление баз, модулей приложений и приложений "Лаборатории Касперского" (см. раздел "Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"" см. стр. 460).
Порт: 443 Протокол: HTTPS	ds.kaspersky.com	Использование Kaspersky Security Network (см. раздел "О KSN и KPSN" на стр. 873).
Порт: 443, 1443 Протокол: HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com	Использование Kaspersky Security Network (см. раздел "О KSN и KPSN" на стр. 873).

Сетевые параметры	Адрес	Описание
	ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	
Протокол: HTTPS	click.kaspersky.com redirect.kaspersky.com	Переход по ссылкам из интерфейса.
Порт: 80 Протокол: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Эти серверы являются частью инфраструктуры открытых ключей (PKI) и необходимы для проверки статуса действительности сертификатов цифровой подписи "Лаборатории Касперского". CRL является списком отозванных сертификатов. OCSP позволяет запрашивать статус конкретного сертификата в режиме реального времени. Эти службы помогают обеспечить безопасность взаимодействия с цифровыми сертификатами и защитить от возможных атак.
Порт: 443 Протокол: HTTPS	https://ipm-klca.kaspersky.com	Рекламные объявления.

Для корректного взаимодействия Kaspersky Security Center с внешними службами соблюдайте следующие рекомендации:

- Незашифрованный сетевой трафик должен быть разрешен на портах 443 и 1443 на сетевом оборудовании и прокси-сервере вашей организации.
- При взаимодействии Сервера администрирования с серверами обновлений "Лаборатории Касперского" и серверами Kaspersky Security Network необходимо избегать перехвата сетевого трафика с подменой сертификатов (MITM-атаки).

► Чтобы загрузить обновления по протоколу HTTP или HTTPS с помощью утилиты *klscflag*:

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой *klscflag*. Утилита *klscflag* расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Если вы хотите загружать обновления (см. раздел "Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского" см. стр. [460](#)) по протоколу HTTP, выполните одну из следующих команд:

- На устройстве, на котором установлен Сервер администрирования:

```
klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
```

- На точку распространения:

```
klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
```

Если вы хотите загружать обновления (см. раздел "Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"" см. стр. [460](#)) по протоколу HTTPS, выполните одну из следующих команд:

- На устройстве, на котором установлен Сервер администрирования:

```
klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
```

- На точку распространения:

```
klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
```

Развертывание Агента администрирования и приложения безопасности

Для управления устройствами организации требуется установить на устройства Агент администрирования. Развертывание распределенного приложения Kaspersky Security Center на устройствах организации обычно начинается с установки на них Агента администрирования.

В Microsoft Windows XP Агент администрирования может некорректно выполнять следующие операции: загрузка обновлений напрямую с серверов "Лаборатории Касперского" (если выполняет роль точки распространения); функционирование в качестве прокси-сервера KSN (если выполняет роль точки распространения); и обнаружение уязвимостей приложений сторонних производителей (при использовании Системного администрирования).

Первоначальное развертывание

Если на устройстве уже установлен Агент администрирования, удаленная установка приложений на такое устройство осуществляется с помощью самого Агента администрирования. При этом передача дистрибутива устанавливаемого приложения вместе с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентами администрирования и Сервером администрирования. Для передачи дистрибутива можно использовать промежуточные центры распространения в виде точек распространения, многоадресную рассылку и прочие средства. Подробные сведения об установке приложений на управляемые устройства, на которых уже установлен Агент администрирования, см. далее в этом разделе.

Первоначальную установку Агента администрирования на устройства на платформе Microsoft Windows можно осуществлять следующими способами:

- С помощью сторонних средств удаленной установки приложений.
- Путем клонирования образа жесткого диска с операционной системой и установленным Агентом администрирования: средствами, предоставляемыми Kaspersky Security Center для работы с образами дисков, или сторонними средствами.
- Через механизм групповых политик Microsoft Windows: с помощью штатных средств управления групповыми политиками Microsoft Windows или автоматизированно, с помощью соответствующего параметра в задаче удаленной установки приложений Kaspersky Security Center.

- Принудительно с помощью соответствующих параметров в задаче удаленной установки приложения Kaspersky Security Center.
- Путем рассылки пользователям устройств ссылок на автономные пакеты, сформированные Kaspersky Security Center. Автономные пакеты представляют собой исполняемые модули, содержащие в себе дистрибутивы выбранных приложений с настроенными параметрами.
- Вручную, запуская инсталляторы приложений на устройствах.

На управляемых устройствах, работающих под управлением платформ отличных от Microsoft Windows, вы можете выполнить удаленную установку (см. раздел "Установка приложений на клиентские устройства." на стр. [852](#)) Агента администрирования. Перед выполнением удаленной установки Агента администрирования на устройство с операционной системой Linux (см. раздел "Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux" на стр. [384](#)) или macOS (см. раздел "Подготовка устройства с операционной системой macOS к удаленной установке Агента администрирования" см. стр. [387](#)) необходимо подготовить устройство. Вы также можете установить Агент администрирования на устройство с операционной системой Linux в тихом режиме (см. раздел "Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)" см. стр. [195](#)) с помощью файла ответов. Обновлять Агент администрирования до новой версии, а также устанавливать другие приложения "Лаборатории Касперского" на этих платформах можно с помощью задач удаленной установки приложений, используя уже имеющиеся на устройствах Агенты администрирования. Установка в этом случае происходит аналогично установке на платформе Microsoft Windows.

Выбирая способ и стратегию развертывания приложений в управляемой сети, следует принимать во внимание ряд факторов (неполный список):

- конфигурацию сети организации (см. раздел "Типовые конфигурации Kaspersky Security Center" на стр. [137](#));
- общее количество устройств;
- наличие в сети организации устройств, не являющихся членами доменов Active Directory, и наличие унифицированных учетных записей с административными правами на таких устройствах;
- ширину канала между Сервером администрирования и устройствами;
- тип связи между Сервером администрирования и удаленными подсетями и ширину сетевых каналов внутри таких подсетей;
- используемые на момент начала развертывания параметры безопасности на удаленных устройствах (в частности использование UAC и режима Simple File Sharing).

Настройка параметров инсталляторов

Прежде чем приступить к развертыванию в сети приложений "Лаборатории Касперского", следует определить параметры инсталляции – те параметры, которые настраиваются в ходе установки приложения. При установке Агента администрирования требуется задать по крайней мере адрес для подключения к Серверу администрирования, а возможно, и некоторые дополнительные параметры. В зависимости от выбранного способа установки параметры можно задавать различными способами. В простейшем случае (при интерактивной установке вручную на выбранное устройство) необходимые параметры можно задать с помощью пользовательского интерфейса инсталлятора.

Этот способ настройки параметров не подходит для тихой установки приложений на группы устройств. В типичном случае администратор должен централизованно указать значения параметров, которые в дальнейшем могут быть использованы для тихой установки на выбранные устройства в сети.

Инсталляционные пакеты

Первый и основной способ настройки инсталляционных параметров приложений является универсальным и подходит для всех способов установки приложений: как средствами Kaspersky Security Center, так и с помощью большинства сторонних средств. Этот способ подразумевает создание в Kaspersky Security Center инсталляционных пакетов приложений.

Инсталляционные пакеты создаются следующими способами:

- автоматически из указанных дистрибутивов на основании входящих в их состав *описателей* (файлов с расширением *kud*, содержащих правила установки и анализа результата и другую информацию);
- из исполняемых файлов инсталляторов или инсталляторов в собственном формате (.msi, .deb, .rpm) – для стандартных или поддерживаемых приложений.

Созданные инсталляционные пакеты представляют собой папки с вложенными подпапками и файлами. Помимо исходного дистрибутива, в состав инсталляционного пакета входят редактируемые параметры (включая параметры самого инсталлятора и правила обработки таких ситуаций, как необходимость перезагрузки операционной системы для завершения инсталляции), а также небольшие вспомогательные модули.

Значения параметров инсталляции, специфичные для конкретного поддерживаемого приложения, можно задавать в пользовательском интерфейсе Консоли администрирования при создании инсталляционного пакета. В случае удаленной установки приложений средствами Kaspersky Security Center инсталляционные пакеты доставляются на устройства таким образом, что при запуске инсталлятора приложения ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки приложений "Лаборатории Касперского" достаточно обеспечить доступность на устройстве всего инсталляционного пакета, то есть дистрибутива и его параметров. Инсталляционные пакеты создаются и хранятся Kaspersky Security Center в соответствующей подпапке папки общего доступа (см. раздел "Задание папки общего доступа" на стр. [227](#)).

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

О том, как именно можно воспользоваться этим способом настройки параметров для приложений "Лаборатории Касперского" перед их развертыванием сторонними средствами, см. в разделе "Развертывание с помощью механизма групповых политик Microsoft Windows (на стр. [169](#))".

Сразу после установки Kaspersky Security Center автоматически создается несколько инсталляционных пакетов, готовых к установке, в том числе пакеты Агента администрирования и приложения безопасности для платформы Microsoft Windows.

Несмотря на то, что лицензионный ключ для лицензии на приложение можно задать в свойствах инсталляционного пакета, желательно не использовать этот способ распространения лицензий из-за широкой доступности инсталляционных пакетов на чтение. Следует использовать автоматически распространяемые лицензионные ключи или задачи установки лицензионных ключей.

Свойства MSI и файлы трансформации

Другим способом настроить параметры инсталляции на платформе Windows является задание свойств MSI

и файлов трансформации. Этот способ может быть использован в следующих случаях:

- при установке через групповые политики Windows при помощи штатных средств Microsoft или иных сторонних инструментов для работы с групповыми политиками Windows;
- при установке с помощью сторонних средств, ориентированных на работу с инсталляторами в формате Microsoft Installer (см. раздел "Настройка параметров инсталляторов" на стр. [178](#)).

Развертывание при помощи сторонних средств удаленной установки приложений

При наличии в организации каких-либо средств удаленной установки приложений (например, Microsoft System Center) целесообразно выполнять первоначальное развертывание при помощи этих средств.

Нужно выполнить следующие действия:

- Выбрать способ настройки параметров инсталляции, наиболее подходящий для используемого средства развертывания.
- Определить механизм синхронизации между изменением параметров инсталляционных пакетов через интерфейс Консоли администрирования и работой выбранных сторонних средств развертывания приложений из данных инсталляционных пакетов.
- В случае установки из папки общего доступа убедиться в достаточной производительности этого файлового ресурса.

См. также:

Задание папки общего доступа	227
Настройка параметров инсталляторов	178

О задачах удаленной установки приложений Kaspersky Security Center

Kaspersky Security Center предоставляет разнообразные механизмы удаленной установки приложений, реализованные в виде задач удаленной установки приложений (принудительная установка, установка с помощью копирования образа жесткого диска, установка с помощью групповых политик Microsoft Windows). Создать задачу удаленной установки можно как для указанной группы администрирования, так и для набора устройств или для выборки устройств (такие задачи отображаются в Консоли администрирования в папке **Задачи**). При создании задачи можно выбрать инсталляционные пакеты (Агента администрирования и/или другого приложения), подлежащие установке при помощи данной задачи, а также задать ряд параметров, определяющих способ удаленной установки. Кроме того, можно воспользоваться мастером удаленной установки приложений, в основе которого также лежит создание задачи удаленной установки приложений и мониторинг результатов.

Задачи для групп администрирования действуют не только на устройства, принадлежащие этой группе, но и на все устройства всех подгрупп выбранной группы. Если в параметрах задачи включен соответствующий параметр, задача распространяется на устройства подчиненных Серверов администрирования, расположенных в данной группе или ее подгруппах.

Задачи для наборов устройств актуализируют список клиентских устройств при каждом запуске в соответствии с составом выборки устройств на момент запуска задачи. Если в выборке устройств присутствуют устройства, подключенные к подчиненным Серверам администрирования, задача будет

запускаться и на этих устройствах. Подробнее об этих параметрах и способах установки будет рассказано далее в этом разделе.

Для успешной работы задачи удаленной установки на устройствах, подключенных к подчиненным Серверам администрирования, следует при помощи задачи ретрансляции предварительно ретранслировать используемые задачей инсталляционные пакеты на соответствующие подчиненные Серверы администрирования.

Развертывание захватом и копированием образа устройства

Если нужно инсталлировать Агент администрирования на устройства, на которые также предстоит установить (или переустановить) операционную систему и прочее программное обеспечение, можно воспользоваться механизмом захвата и копирования образа устройства.

► *Чтобы выполнить развертывание путем захвата и копирования жесткого диска:*

1. Создать эталонное устройство с установленной операционной системой и необходимым для работы набором программного обеспечения, включая Агент администрирования и приложение безопасности.
2. Захватить образ "эталонного" устройства и далее распространять этот образ на новые устройства посредством задачи Kaspersky Security Center.

Для захвата и установки образов диска можно воспользоваться как имеющимися в организации сторонними средствами, так и функциональностью, предоставляемой (при наличии лицензии на Системное администрирование) Kaspersky Security Center (см. раздел "Установка образов операционных систем" на стр. [846](#)).

Если для работы с образами диска используются сторонние инструменты, необходимо при развертывании на устройство из эталонного образа обеспечить удаление информации, с помощью которой Kaspersky Security Center идентифицирует управляемое устройство. В противном случае Сервер администрирования не сможет в дальнейшем корректно различать устройства, созданные путем копирования одного и того же образа (см. раздел "Подготовка эталонного устройства с установленным Агентом администрирования для создания образа операционной системы" на стр. [916](#)).

При захвате образа диска средствами Kaspersky Security Center эта проблема решается автоматически.

Копирование образа жесткого диска сторонними инструментами

При использовании сторонних инструментов для захвата образа устройства с установленным Агентом администрирования следует воспользоваться одним из следующих методов:

- Рекомендуемый метод. При установке Агента администрирования на эталонное устройство (см. раздел "Подготовка эталонного устройства с установленным Агентом администрирования для создания образа операционной системы" на стр. [916](#)) захватить образ устройства до первого запуска службы Агента администрирования (так как уникальная информация, идентифицирующая устройство, создается при первом подключении Агента администрирования к Серверу администрирования). В дальнейшем рекомендуется не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.

- На эталонном устройстве остановить службу Агента администрирования и запустить утилиту klmover с ключом -dupfix. Утилита klmover входит в состав инсталляционного пакета Агента администрирования. В дальнейшем не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.
- Обеспечить запуск утилиты klmover с ключом -dupfix до (это важно) первого запуска службы Агента администрирования на устройствах при первом старте операционной системы после развертывания образа. Утилита klmover входит в состав инсталляционного пакета Агента администрирования.
- Использовать режим клонирования диска Агента администрирования (см. раздел "Режим клонирования диска Агента администрирования" на стр. [914](#)).

Если образ жесткого диска был скопирован неправильно, вы можете решить эту проблему (см. раздел "Неверно выполнено копирование образа жесткого диска" на стр. [168](#)).

Также можно захватить образ устройства без установленного Агента администрирования. Для этого выполните развертывание образа на целевых устройствах, а затем установите Агент администрирования. При использовании этого метода предоставьте доступ к сетевой папке с автономными инсталляционными пакетами с устройства (см. раздел "Установка образов операционных систем" на стр. [846](#)).

См. также:

Режим клонирования диска Агента администрирования [914](#)

Неверно выполнено копирование образа жесткого диска

Если копирование образа жесткого диска с установленным Агентом администрирования было выполнено без учета правил развертывания (см. раздел "Развертывание захватом и копированием образа устройства" на стр. [167](#)), часть устройств в Консоли администрирования может отображаться как один значок устройства, постоянно меняющий имя.

Можно использовать следующие способы решения этой проблемы:

- Удаление Агента администрирования.
Этот способ является самым надежным. На устройствах, которые были скопированы из образа неправильно, нужно при помощи сторонних средств удалить Агент администрирования, а затем установить его заново. Удаление Агента администрирования не может быть выполнено средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).
- Запуск утилиты klmover с ключом "-dupfix".
На проблемных устройствах (на всех, которые были скопированы из образа неправильно) необходимо при помощи сторонних средств однократно запустить утилиту klmover с ключом "-dupfix" (klmover -dupfix), расположенную в папке установки Агента администрирования. Запуск утилиты не может быть выполнен средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

Затем следует удалить значок, на который отображались проблемные устройства до запуска утилиты.

- Ужесточение правила обнаружения неправильно скопированных устройств.

Этот способ можно использовать только в случае, если установлены Сервер администрирования и Агенты администрирования версии 10 Service Pack 1 или новее.

Следует ужесточить правило обнаружения неправильно скопированных Агентов администрирования таким образом, чтобы изменение NetBIOS-имени устройства приводило к автоматической "починке" таких Агентов администрирования (предполагается, что скопированные устройства имеют различные NetBIOS-имена).

На устройстве с Сервером администрирования нужно импортировать в Реестр представленный ниже reg-файл и перезапустить службу Сервера администрирования.

- Если на устройстве с Сервером администрирования установлена 32-разрядная операционная система:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

- Если на устройстве с Сервером администрирования установлена 64-разрядная операционная система:

```
REGEDIT4

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
"KLSRV_CheckClones"=dword:00000003
```

Развертывание с помощью механизма групповых политик Microsoft Windows

Первоначальное развертывание Агентов администрирования рекомендуется осуществлять с помощью групповых политик Microsoft Windows при выполнении следующих условий:

- устройства являются членами домена Active Directory;
- план развертывания позволяет дождаться штатной перезагрузки устройств до начала развертывания на них Агентов администрирования, или к устройствам можно принудительно применить групповую политику Windows.

Суть данного способа развертывания заключается в следующем:

- Дистрибутив приложения в формате Microsoft Installer (MSI-пакет) размещается в папке общего доступа (в папке, к которой имеют доступ на чтение учетные записи LocalSystem устройств).
- В групповой политике Active Directory создается объект установки данного дистрибутива.
- Область действия установки задается привязкой к организационному подразделению и / или к группе безопасности, в которую входят устройства.
- При очередном входе устройства в домен (до входа в систему пользователей устройства) выполняется проверка наличия требуемого приложения среди установленных приложений. Если приложение отсутствует, происходит загрузка дистрибутива с заданного в политике ресурса и его установка.

Одним из преимуществ этого способа развертывания является то, что назначенные приложения устанавливаются на устройства при загрузке операционной системы еще до входа пользователя в систему. Даже если пользователь, имеющий необходимые права, удалит приложение, при следующей загрузке операционной системы оно будет установлено снова. Недостатком этого способа развертывания является то, что произведенные администратором изменения в групповой политике не вступят в силу до перезагрузки устройств (без применения дополнительных средств).

С помощью групповых политик можно устанавливать как Агент администрирования, так и другие приложения, инсталляторы которых имеют формат Windows Installer.

При выборе этого способа развертывания, помимо прочего, необходимо оценить нагрузку на файловый ресурс, с которого будет осуществляться копирование файлов на устройства при применении групповой политики Windows.

Работа с политиками Microsoft Windows с помощью задачи удаленной установки приложений Kaspersky Security Center

Самым простым способом установки приложений с помощью групповых политик Microsoft Windows является выбор параметра **Назначить установку инсталляционного пакета в групповых политиках Active Directory** в свойствах задачи удаленной установки приложений Kaspersky Security Center. В этом случае при запуске задачи Сервер администрирования самостоятельно выполнит следующие действия:

- Создаст необходимые объекты в групповой политике Microsoft Windows.
- Создаст специальные группы безопасности, в которые включит устройства, и назначит установку выбранных приложений для этих групп безопасности. Состав групп безопасности будет обновляться при каждом запуске задачи в соответствии с набором устройств на момент запуска.

Для обеспечения работоспособности данной функции следует указать в параметрах задачи учетную запись, имеющую права на редактирование групповых политик Active Directory.

Если с помощью одной задачи предполагается установить и Агент администрирования, и другое приложение, выбор параметра **Назначить установку инсталляционного пакета в групповых политиках Active Directory** приведет к созданию в политике Active Directory объекта установки только для Агента администрирования. Второе выбранное в задаче приложение будет устанавливаться уже средствами Агента администрирования, как только он будет установлен на устройстве. Если по какой-то причине необходимо установить отличное от Агента администрирования приложение именно с помощью групповых политик Windows, то нужно создать задачу установки только для этого инсталляционного пакета (без пакета Агента администрирования). Не все приложения могут быть установлены с помощью групповых политик Microsoft Windows. О такой возможности вы можете узнать, обратившись к информации о способах установки приложения.

В случае, когда необходимые объекты создаются в групповой политике средствами Kaspersky Security Center, в качестве источника инсталляционного пакета будет использована папка общего доступа Kaspersky Security Center. При планировании развертывания следует соотнести скорость чтения из этой папки с количеством устройств и размером устанавливаемого дистрибутива. Возможно, будет целесообразно расположить папку общего доступа Kaspersky Security Center в мощном специализированном файловом хранилище (см. раздел "Задание папки общего доступа" на стр. [227](#)).

Помимо простоты, автоматическое создание групповых политик Windows средствами Kaspersky Security Center имеет еще одно преимущество: при планировании установки Агента администрирования легко указать группу администрирования Kaspersky Security Center, в которую будут автоматически перемещаться устройства по завершении установки. Группу можно указать в мастере создания задачи или в окне параметров задачи удаленной установки.

При работе с групповыми политиками Windows средствами Kaspersky Security Center задание устройств для объекта групповой политики осуществляется путем создания группы безопасности. Kaspersky Security Center синхронизирует состав группы безопасности с текущим набором устройств задачи. При использовании иных средств для работы с групповыми политиками можно привязывать объекты групповых политик непосредственно к выбранным подразделениям Active Directory.

Самостоятельная установка приложений с помощью политик Microsoft Windows

Администратор может самостоятельно создать в групповой политике Windows объекты, необходимые для установки. В этом случае можно сослаться на пакеты, лежащие в папке общего доступа Kaspersky Security Center, или выложить пакеты на отдельный файловый сервер и сослаться на них.

Возможны следующие сценарии установки:

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Объект групповой политики ссылается на MSI-файл этого сконфигурированного пакета, лежащего в папке общего доступа Kaspersky Security Center.
- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Затем администратор копирует целиком подпапку EXEC этого пакета из папки общего доступа Kaspersky Security Center в папку на специализированном файловом ресурсе организации. Объект групповой политики ссылается MSI-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации.
- Администратор загружает дистрибутив приложения (в том числе дистрибутив Агента администрирования) из интернета и выкладывает его на специализированный файловый ресурс организации. Объект групповой политики ссылается MSI-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации. Настройка параметров инсталляции осуществляется путем настройки свойств MSI или настройкой файлов трансформации MST.

См. также:

Установка приложения с помощью групповых политик Active Directory[361](#)

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center

Чтобы выполнить первоначальное развертывание Агента администрирования или других приложений, вы можете принудительно установить выбранные инсталляционные пакеты с помощью задачи удаленной установки Kaspersky Security Center при условии, что на каждом устройстве есть учетные записи пользователей с правами локального администратора.

Принудительная установка может быть использована и в случае, если устройства не доступны Серверу администрирования непосредственно: например, устройства расположены в изолированных сетях, или устройства расположены в локальной сети, а Сервер администрирования – в демилитаризованной зоне.

В случае первоначального развертывания Агент администрирования не устанавливается. Поэтому в параметрах задачи удаленной установки нельзя выбрать распространение файлов, необходимых для установки приложения с помощью Агента администрирования. Вы можете распространять файлы, только используя ресурсы операционной системы с помощью Сервера администрирования или точки распространения.

Служба Сервера администрирования должна запускаться под учетной записью, имеющей права администратора на целевых устройствах. Также вы можете указать учетную запись, имеющую доступ к административным ресурсам общего доступа admin\$, в параметрах задачи удаленной установки.

По умолчанию задача удаленной установки подключается к устройствам, используя учетные данные учетной записи, под которой запущен Сервер администрирования. Обратите внимание, что это учетная запись, используемая для доступа к административным ресурсам общего доступа admin\$, а не учетная запись, под которой выполняется задача удаленной установки. Установка выполняется под учетной записью LocalSystem.

Вы можете указать целевые устройства явно (списком), выбрав группу администрирования Kaspersky Security Center, которой они принадлежат, либо созданием выборки устройств по определенному условию. Время запуска установки определяется расписанием задачи. Если в свойствах задачи включен параметр **Запускать пропущенные задачи**, задача может запускаться сразу при включении устройств или при переносе их в целевую группу администрирования.

Принудительная установка осуществляется путем доставки инсталляционных пакетов на целевые устройства, последующего копирования файлов на административный ресурс admin\$ каждого из устройств и удаленной регистрации на них вспомогательных служб. Доставка инсталляционных пакетов на целевые устройства выполняется с помощью функции Kaspersky Security Center, отвечающей за сетевое взаимодействие. При этом должны выполняться следующие условия:

- Целевые устройства доступны со стороны Сервера администрирования или со стороны точки распространения.
- В сети корректно работает разрешение имен для устройств.
- На целевых устройствах включены административные ресурсы общего доступа admin\$.
- На целевых устройствах запущены следующие системные службы:
 - Сервер (LanmanServer).
По умолчанию эта служба запущена.
 - DCOM Server Process Launcher (DcomLaunch).
 - RPC Endpoint Mapper (RpcEptMapper).
 - Вызов удаленной процедуры (Remote Procedure Call, RpcSs).
- TCP-порт 445 открыт на целевых устройствах для обеспечения удаленного доступа с помощью инструментов Windows.

TCP 139, UDP 137 и UDP 138 используются старыми протоколами и больше не нужны для текущих приложений.

На сетевом экране должны быть разрешены динамические исходящие порты доступа для соединения Сервера администрирования и точек распространения с целевыми устройствами.

- В параметрах безопасности политики домена Active Directory разрешено обеспечивать работу NTDM-протокола при развертывании Агента администрирования.
- На целевых устройствах под управлением Microsoft Windows XP режим Simple File Sharing выключен.

- На целевых устройствах настроена модель совместного доступа и безопасности *Классическая* – *локальные пользователи выполняют аутентификацию самих себя*. Такая модель не может быть *Только гостевой* – *локальные пользователи выполняют аутентификацию как Гость*.
- Устройства являются членами домена, либо на устройствах заблаговременно созданы унифицированные учетные записи с административными правами.

Чтобы успешно развернуть Агент администрирования или другие приложения на устройстве, не подключенном к домену Active Directory с версией операционной системы Windows Server 2003 и выше, необходимо выключить удаленный UAC на этом устройстве. Удаленный UAC – это одна из причин, по которой учетные записи локальных администраторов не могут получить доступ к admin\$, который требуется для принудительного развертывания Агента администрирования и других приложений. Выключение удаленного UAC не влияет на локальный UAC.

При установке на новые устройства, еще не размещенные в группах администрирования Kaspersky Security Center, в свойствах задачи удаленной установки можно задать группу администрирования, в которую устройства будут перемещаться по завершении установки на них Агента администрирования.

При создании групповой задачи необходимо помнить, что групповая задача действует на устройства всех вложенных подгрупп выбранной группы. Поэтому не следует дублировать задачи установки в подгруппах.

Упрощенным способом создания задач для принудительной установки приложений является автоматическая установка. Для этого в свойствах группы администрирования вам нужно открыть список инсталляционных пакетов и выбрать те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Чтобы снизить нагрузку на Сервер администрирования при распространении инсталляционных пакетов на целевые устройства, вы можете выбрать установку с помощью точек распространения в задаче установки. Следует учитывать, что данный способ установки создает значительную нагрузку на устройства, назначенные точками распространения. Рекомендуется выбирать устройства, соответствующие требованиям для точек распространения. Если вы используете точки распространения, вам нужно убедиться, что они присутствуют в каждой из изолированных подсетей, на которых размещены целевые устройства.

Использование точек распространения в качестве локальных центров установки может быть удобно и для установки на устройства в подсетях, соединенных с Сервером администрирования узким каналом связи при наличии широкого канала связи между устройствами внутри подсети.

Объем свободного места в разделе с папкой %ALLUSERSPROFILE%\Application Data\KasperskyLab\admindkit должен многократно превосходить суммарный объем дистрибутивов устанавливаемых приложений.

Запуск автономных пакетов, сформированных Kaspersky Security Center

Описанные выше способы первоначального развертывания Агента администрирования и приложений могут быть реализованы не всегда из-за невозможности выполнить все необходимые условия. В таких случаях из

подготовленных администратором инсталляционных пакетов с необходимыми параметрами установки средствами Kaspersky Security Center можно создать единый исполняемый файл, который называется *автономным пакетом установки*. Автономный инсталляционный пакет размещается в папке общего доступа Kaspersky Security Center.

При помощи Kaspersky Security Center можно разослать по электронной почте выбранным пользователям ссылку на этот файл в папке общего доступа с просьбой запустить файл (интерактивно или с ключом тихой установки "-s"). Автономный инсталляционный пакет можно прикрепить к сообщению электронной почты для пользователей устройств, не имеющих доступа к папке общего доступа Kaspersky Security Center. Администратор может скопировать автономный пакет на съемный диск и доставить пакет на нужное устройство с целью его последующего запуска.

Автономный пакет можно создать из пакета Агента администрирования, пакета другого приложения (например, приложения безопасности) или сразу из обоих пакетов. Если автономный пакет создан из Агента администрирования и другого приложения, установка начнется с Агента администрирования.

При создании автономного пакета с Агентом администрирования можно указать группу администрирования, в которую будут автоматически перемещаться новые устройства (ранее не размещенные в группах администрирования) по завершении установки на них Агента администрирования.

Автономные пакеты могут работать интерактивно (по умолчанию), с отображением результата установки входящих в них приложений, или в тихом режиме (при запуске с ключом "-s"). Тихий режим может быть использован для установки из каких-либо скриптов (например, из скриптов, настраиваемых для запуска по завершении развертывания образа операционной системы, и тому подобное). Результат установки в тихом режиме определяется кодом возврата процесса.

Возможности ручной установки приложений

Администраторы или опытные пользователи могут устанавливать приложения вручную в интерактивном режиме. При этом можно использовать как исходные дистрибутивы, так и сформированные из них инсталляционные пакеты, расположенные в папке общего доступа Kaspersky Security Center. Инсталляторы по умолчанию работают в интерактивном режиме, запрашивая у пользователя все необходимые значения параметров. Но при запуске процесса setup.exe из корня инсталляционного пакета с ключом "-s" инсталлятор будет работать в тихом режиме с параметрами, заданными при настройке инсталляционного пакета.

При запуске setup.exe из корня инсталляционного пакета расположенного в папке общего доступа Kaspersky Security Center, сначала произойдет копирование пакета во временную локальную папку, затем из локальной папки будет запущен инсталлятор приложения.

Удаленная установка приложений на устройства с установленным Агентом администрирования

Если на устройстве установлен работоспособный Агент администрирования, подключенный к главному Серверу администрирования или к одному из его подчиненных Серверов, то на этом устройстве можно обновлять версию Агента администрирования, а также устанавливать, обновлять или удалять с помощью Агента администрирования любые поддерживаемые приложения.

Эта функция включается параметром **С помощью Агента администрирования** в свойствах задачи удаленной установки приложений (см. раздел "О задачах удаленной установки приложений Kaspersky Security Center" на стр. [166](#)).

Если параметр выбран, то передача на устройства инсталляционных пакетов с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентом администрирования и Сервером администрирования.

Для оптимизации нагрузки на Сервер администрирования и минимизации трафика между Сервером администрирования и устройствами целесообразно назначать в каждой удаленной сети или в каждом широковебательном домене точки распространения (см. разделы "О точках распространения (на стр. [147](#))" и "Построение структуры групп администрирования и назначение точек распространения (см. раздел "Настройка точек распространения и шлюзов соединений" на стр. [685](#))"). В этом случае распространение инсталляционных пакетов и параметров инсталлятора осуществляется с Сервера администрирования на устройства через точки распространения.

Также с использованием точек распространения можно выполнять широковебательную (многоадресную) рассылку инсталляционных пакетов, что позволяет многократно снизить сетевой трафик в ходе развертывания приложений.

При передаче инсталляционных пакетов на устройства по каналам связи между Агентами администрирования и Сервером администрирования подготовленные к передаче инсталляционные пакеты дополнительно кешируются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\working\FTServer. При использовании большого числа различных инсталляционных пакетов большого размера и при большом количестве точек распространения размер этой папки может существенно увеличиваться.

Удалять файлы из папки FTServer вручную невозможно. При удалении исходных инсталляционных пакетов соответствующие данные будут автоматически удаляться и из папки FTServer.

Данные, принимаемые точками распространения, сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\FTCITmp.

Удалять файлы из папки \$FTCITmp вручную невозможно. По мере завершения задач, использующих данные из папки, содержимое этой папки будет удаляться автоматически.

Поскольку инсталляционные пакеты распространяются по каналам связи между Сервером администрирования и Агентами администрирования из промежуточного хранилища в оптимизированном для передачи по сети формате, невозможно вносить изменения в инсталляционные пакеты в исходной папке инсталляционного пакета. Такие изменения не будут автоматически учтены Сервером администрирования. Если необходимо изменить вручную файлы инсталляционных пакетов (хотя делать это не рекомендуется), нужно обязательно изменить какие-либо параметры инсталляционного пакета в Консоли администрирования. Изменение параметров инсталляционного пакета в Консоли администрирования заставит Сервер администрирования обновить образ пакета в кеше, подготовленном для передачи на устройства.

Управление перезагрузкой устройств в задаче удаленной установки

Часто для завершения удаленной установки приложений (особенно на платформе Windows) требуется перезагрузка устройства.

Если используется задача удаленной установки приложений Kaspersky Security Center, в мастере создания задачи или в окне свойств созданной задачи (раздел **Перезагрузка операционной системы**) можно

выбрать вариант действия при необходимости перезагрузки устройства с операционной системой Windows:

- **Не перезагружать устройство.** В этом случае автоматическая перезагрузка не будет выполнена. Для завершения установки потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки будет сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач установки на серверы и другие устройства, для которых критически важна бесперебойная работа.
- **Перезагрузить устройство.** В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения установки. Этот вариант подходит для задач установки на устройства, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).
- **Запрашивать у пользователя.** На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Вариант **Запрашивать у пользователя** наиболее подходит для рабочих станций, пользователи которых должны иметь возможность выбрать наиболее подходящий момент для перезагрузки.

Целесообразность обновления баз в инсталляционном пакете приложения безопасности

Перед началом развертывания защиты необходимо учитывать возможность обновления антивирусных баз (включая модули автопатчей), распространяемых вместе с дистрибутивом приложения безопасности. Целесообразно перед началом развертывания принудительно обновить базы в составе инсталляционного пакета приложения (например, с помощью соответствующей команды в контекстном меню выбранного инсталляционного пакета). Это уменьшит количество перезагрузок, требующихся для завершения развертывания защиты на устройствах.

Использование средств удаленной установки приложений Kaspersky Security Center для запуска на управляемых устройствах произвольных исполняемых файлов

С помощью мастера создания инсталляционного пакета можно выбрать произвольный исполняемый файл и задать для него параметры командной строки. При этом в инсталляционный пакет можно поместить как сам выбранный файл, так и всю папку, в которой этот файл содержится. Затем следует создать задачу удаленной установки и выбрать созданный инсталляционный пакет.

В ходе работы задачи на устройствах будет запущен указанный при создании исполняемый файл с заданными параметрами командной строки.

Если используются инсталляторы в формате Microsoft Windows Installer (MSI), Kaspersky Security Center использует штатные возможности по анализу результата установки.

Если есть лицензия на Системное администрирование, при создании инсталляционного пакета для одного из поддерживаемых приложений, распространенных в корпоративной среде, Kaspersky Security Center также использует правила установки и анализа результатов установки, имеющиеся в его обновляемой базе.

В иных случаях для исполняемых файлов задача по умолчанию дожидается завершения запущенного процесса и всех порожденных им дочерних процессов. По завершении запущенных процессов задача будет завершена успешно независимо от кода возврата исходного процесса. Чтобы изменить такое поведение задачи, перед созданием задачи следует изменить вручную файлы с расширением kpd, сформированные Kaspersky Security Center в папке созданного инсталляционного пакета и в его подпапках.

Для того чтобы задача не ожидала завершения запущенного процесса, в секции [SetupProcessResult] нужно задать значение 0 для параметра Wait:

Пример:

```
[SetupProcessResult]
```

```
Wait=0
```

Для того чтобы на платформе Windows задача ожидала только завершения исходного процесса, но не порожденных им дочерних процессов, нужно в секции [SetupProcessResult] задать значение 0 для параметра WaitJob, например:

Пример:

```
[SetupProcessResult]
```

```
WaitJob=0
```

Для того чтобы задача завершалась успешно или с ошибкой в зависимости от кода возврата запущенного процесса, нужно перечислить успешные коды возврата в секции [SetupProcessResult_SuccessCodes], например:

Пример:

```
[SetupProcessResult_SuccessCodes]
```

```
0=
```

```
3010=
```

В этом случае любой код, отличный от перечисленных, будет означать ошибку.

Для того чтобы в результатах задачи отображалась строка с комментарием об успешном завершении задачи или сообщения об ошибках, нужно задать краткие описания ошибок, соответствующих кодам возврата процесса, в секциях [SetupProcessResult_SuccessCodes] и [SetupProcessResult_ErrorCodes], например:

Пример:

```
[SetupProcessResult_SuccessCodes]
```

```
0 = установка завершена успешно
```

```
3010=A reboot is required to complete the installation
```

```
[SetupProcessResult_ErrorCodes]
```

```
1602=Installation cancelled by the user
```

```
1603 = критическая ошибка при установке
```

Для того чтобы задействовать средства Kaspersky Security Center по управлению перезагрузкой устройства (если перезагрузка необходима для завершения операции), нужно дополнительно перечислить коды возврата процесса, означающие необходимость перезагрузки, в секции [SetupProcessResult_NeedReboot]:

Пример:

[SetupProcessResult_NeedReboot]

3010=

Мониторинг развертывания

Для контроля развертывания Kaspersky Security Center, а также для контроля наличия на управляемых устройствах приложения безопасности и Агента администрирования, следует обращать внимание на цветовой индикатор в блоке **Развертывание**. Индикатор расположен в рабочей области узла Сервер администрирования в главном окне Консоли администрирования (см. раздел "Мониторинг цветowych индикаторов и зарегистрированных событий в Консоли администрирования" на стр. [595](#)). Индикатор отображает текущее состояние развертывания. Рядом с индикатором отображается количество устройств с установленными Агентами администрирования и приложениями безопасности. При наличии активных задач установки отображается прогресс выполнения задач. При наличии ошибок установки, здесь отображается количество ошибок. Просмотреть детальную информацию об ошибке можно по ссылке.

Также можно воспользоваться диаграммой развертывания в рабочей области папки **Управляемые устройства** на вкладке **Группы**. Диаграмма отражает процесс развертывания: количество устройств без Агента администрирования, с Агентом администрирования, с Агентом администрирования и приложением безопасности.

Более детальное описание хода развертывания (или работы конкретной задачи установки) можно увидеть в окне результатов выполнения соответствующей задачи удаленной установки: В контекстном меню задачи выберите **Результаты**. В окне отображаются два списка: в верхнем списке содержится список состояний задачи на устройствах, а в нижнем – список событий задачи на устройстве, которое в данный момент выбрано в верхнем списке.

Информация об ошибках при развертывании записывается в журнал событий Kaspersky Event Log Сервера администрирования. Информация об ошибках также доступна в соответствующей выборке событий в узле Сервера администрирования на вкладке **События**.

Настройка параметров инсталляторов

В разделе содержится информация о файлах инсталляторов Kaspersky Security Center и параметрах установки, а также рекомендации по установке Сервера администрирования и Агента администрирования в тихом режиме.

Общая информация

Инсталляторы компонентов Kaspersky Security Center – Сервера администрирования, Агента администрирования, Консоли администрирования – построены на технологии Windows Installer. Ядром инсталлятора является MSI-пакет. Этот формат упаковки дистрибутива позволяет использовать все преимущества технологии Windows Installer: масштабируемость, возможность использовать систему патчевания, систему трансформации, возможность установки централизованно сторонними решениями, прозрачность регистрации в операционной системе.

См. также:

Установка в тихом режиме (с файлом ответов).....	179
Установка Агента администрирования в тихом режиме (без файла ответов).....	180
Частичная настройка параметров установки через setup.exe	181
Параметры установки Сервера администрирования	181
Параметры установки Агента администрирования	185

Установка в тихом режиме (с файлом ответов)

В инсталляторах Сервера администрирования и Агента администрирования реализована возможность работы с файлом ответов (ss_install.xml), в котором записаны параметры для установки в тихом режиме без участия пользователя. Файл ss_install.xml расположен в той же папке, что и MSI-пакет, и используется автоматически при установке в тихом режиме. Вы можете включить режим автоматической установки с помощью ключа командной строки "/s".

Пример запуска:

```
setup.exe /s
```

Прежде чем запускать приложение установки в тихом режиме, прочтите Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center Linux не входит TXT файл с текстом Лицензионного соглашения, вы можете загрузить этот файл с сайта "Лаборатории Касперского" <https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint>.

Файл ss_install.xml представляет собой внутренний формат параметров инсталлятора Kaspersky Security Center. В составе дистрибутивов поставляется файл ss_install.xml с параметрами по умолчанию.

Не следует изменять файл ss_install.xml вручную. Этот файл изменяется средствами Kaspersky Security Center при изменении параметров инсталляционных пакетов в Консоли администрирования.

► Чтобы изменить файл ответов для установки Сервера администрирования:

1. Откройте дистрибутив Kaspersky Security Center. Если вы используете полный пакет EXE-файла, распакуйте его.
2. Сформируйте папку Сервер, откройте командную строку и выполните следующую команду:

```
setup.exe /r ss_install.xml
```

Запустится приложение установки Kaspersky Security Center.

3. Следуйте инструкциям мастера, чтобы настроить установку Kaspersky Security Center.

По завершении работы мастера файл ответов автоматически изменится в соответствии с новыми параметрами, указанными вами.

См. также:

Общая информация.....	178
Установка Агента администрирования в тихом режиме (без файла ответов).....	180
Частичная настройка параметров установки через setup.exe.....	181
Параметры установки Сервера администрирования.....	181
Параметры установки Агента администрирования.....	185
Основной сценарий установки.....	56

Установка Агента администрирования в тихом режиме (без файла ответов)

Агент администрирования можно установить при помощи одного только msi-пакета, задавая при этом значения свойств MSI стандартным образом. Такой сценарий позволяет устанавливать Агент администрирования, используя групповые политики.

Не переименовывайте инсталляционный пакет Kaspersky Network Agent.msi. Переименование пакета может привести к ошибкам установки при обновлении Агента администрирования.

Для того чтобы не возникал конфликт между параметрами, заданными с помощью свойств MSI, и параметрами, заданными в файле ответов, предусмотрена возможность отключения файла ответов путем задания свойства `DONT_USE_ANSWER_FILE=1`. MSI-файл расположен в дистрибутиве приложения Kaspersky Security Center в папке `Packages\NetAgent\exec`. Ниже приведен пример запуска инсталлятора Агента администрирования с помощью msi-пакета.

Установка Агента администрирования в неинтерактивном режиме требует принятия Лицензионного соглашения (см. раздел "О Лицензионном соглашении" см. стр. [342](#)). Используйте параметр `EULA=1`, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения.

Пример:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1  
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Также параметры инсталляции msi-пакета можно задать, подготовив предварительно файл трансформации (файл с расширением mst). Команда будет выглядеть следующим образом:

Пример:

```
msiexec /i "Kaspersky Network Agent.msi" /qn  
TRANSFORMS=test.mst;test2.mst
```

В одной команде можно указать более одного файла трансформации.

См. также:

Установка Агента администрирования в тихом режиме	193
Параметры установки Агента администрирования	185
Порты, используемые Kaspersky Security Center	63
Общая информация.....	178
Установка в тихом режиме (с файлом ответов).....	179
Частичная настройка параметров установки через setup.exe	181
Параметры установки Сервера администрирования	181
Основной сценарий установки.....	56

Частичная настройка параметров установки через setup.exe

Запуская установку приложений через setup.exe, можно передавать в MSI-пакет значения любых свойств MSI.

Команда будет выглядеть следующим образом:

Пример:

```
/v "PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2 "
```

См. также:

Общая информация.....	178
Установка в тихом режиме (с файлом ответов).....	179
Установка Агента администрирования в тихом режиме (без файла ответов).....	180
Параметры установки Сервера администрирования	181
Параметры установки Агента администрирования	185

Параметры установки Сервера администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Сервера администрирования. Все параметры являются необязательными, кроме EULA и PRIVACYPOLICY.

Таблица 42. Параметры установки Сервера администрирования в тихом режиме

Свойство MSI	Описание	Доступные значения
EULA	Согласие с условиями Лицензионного соглашения (обязательный параметр).	1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения (см. раздел "О Лицензионном соглашении" см. стр. 342). - Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
PRIVACYPOLICY	Согласие с условиями Политики конфиденциальности (обязательный параметр).	1 – Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности (см. раздел "Просмотр Политики конфиденциальности" см. стр. 205). Я подтверждаю, что полностью прочитал(а) и понимаю Политику конфиденциальности. - Другое значение или не задано – Я не принимаю условия Политики конфиденциальности (установка не выполняется).
INSTALLATIONMODETYPE	Тип установки Сервера администрирования.	- Стандартная. - Выборочная.
INSTALLDIR	Папка установки приложения.	Строковое значение.
ADDLOCAL	Список компонентов для установки (через запятую).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Минимальный достаточный для корректной установки Сервера администрирования список компонентов: ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86

Свойство MSI	Описание	Доступные значения
NETRANGETYPE	Размер сети.	- NRT_1_100 – от 1 до 100 устройств. - NRT_100_1000 – от 101 до 1000 устройств. - NRT_GREATER_1000 – более 1000 устройств.
SRV_ACCOUNT_TYPE	Способ задания пользователя для работы службы Сервера администрирования.	- SrvAccountDefault – учетная запись пользователя будет создана автоматически. - SrvAccountUser – учетная запись пользователя задана вручную.
SERVERACCOUNTNAME	Имя пользователя для службы.	Строковое значение.
SERVERACCOUNTPWD	Пароль пользователя для службы.	Строковое значение.
DBTYPE	Тип базы данных.	- MySQL – будет использоваться база данных MySQL или MariaDB. - MSSQL – будет использоваться база данных Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	Полное имя сервера MySQL или MariaDB.	Строковое значение.
MYSQLSERVERPORT	Номер порта для подключения к серверу MySQL или MariaDB.	Числовое значение.
MYSQLDBNAME	Имя базы данных сервера MySQL или MariaDB.	Строковое значение.
MYSQLACCOUNTNAME	Имя пользователя для подключения к базе сервера MySQL или MariaDB.	Строковое значение.
MYSQLACCOUNTPWD	Пароль пользователя для подключения к базе сервера MySQL или MariaDB.	Строковое значение.
MSSQLCONNECTIONTYPE	Тип использования базы данных MSSQL.	- InstallMSSEE – установить из пакета. - ChooseExisting – использовать установленный сервер.
MSSQLSERVERNAME	Полное имя экземпляра SQL Server.	Строковое значение.
MSSQLDBNAME	Имя базы данных SQL Server.	Строковое значение.
MSSQLAUTHTYPE	Способ аутентификации при подключении к SQL Server.	- Windows. - SQLServer.

Свойство MSI	Описание	Доступные значения
MSSQLACCOUNTNAME	Имя пользователя для подключения к SQL Server в режиме SQLServer.	Строковое значение.
MSSQLACCOUNTPWD	Пароль пользователя для подключения к SQL Server в режиме SQLServer.	Строковое значение.
CREATE_SHARE_TYPE	Способ задания папки общего доступа.	• Create – создать новую папку общего доступа. В этом случае должны быть заданы следующие свойства: • SHARELOCALPATH – путь к локальной папке. • SHAREFOLDERNAME – сетевое имя папки. • Пусто – должно быть задано свойство EXISTSHAREFOLDERNAME.
EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа.	Строковое значение.
SERVERPORT	Номер порта для подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для установки SSL-соединения с Сервером администрирования.	Числовое значение.
SERVERADDRESS	Адрес Сервера администрирования.	Строковое значение.
SERVERCERT2048BITS	Длина ключа для сертификата Сервера администрирования (в битах).	• 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит. • 0 – длина ключа для сертификата Сервера администрирования составляет 1024 бит. • Если параметр не задан, длина ключа для сертификата Сервера администрирования составляет 1024 бит.
MOBILESERVERADDRESS	Адрес Сервера администрирования для подключения мобильных устройств; игнорируется, если не выбран компонент MobileSupport.	Строковое значение.

См. также:

Общая информация.....	178
Установка в тихом режиме (с файлом ответов).....	179
Установка Агента администрирования в тихом режиме (без файла ответов).....	180
Параметры установки Агента администрирования	185
Установка Агента администрирования в тихом режиме	193
Частичная настройка параметров установки через setup.exe	181

Параметры установки Агента администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Агента администрирования. Все параметры являются необязательными, кроме EULA и SERVERADDRESS.

Таблица 43. Параметры установки Агента администрирования в тихом режиме

Свойство MSI	Описание	Доступные значения
EULA	Согласие с условиями Лицензионного соглашения	1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения (см. раздел "О Лицензионном соглашении" см. стр. 342). 0 – Я не принимаю условия Лицензионного соглашения (установка не выполняется). - Значение не задано – Я не принимаю условия Лицензионного соглашения (установка не выполняется).
DONT_USE_ANSWER_FILE	Читать параметры установки из файла ответов.	1 – Не использовать. - другое значение или не задано – читать.
INSTALLDIR	Путь к папке установки Агента администрирования.	Строковое значение.
SERVERADDRESS	Адрес Сервера администрирования (обязательный параметр).	Строковое значение.
SERVERPORT	Номер порта подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL.	Числовое значение.

Свойство MSI	Описание	Доступные значения
USESSL	Использовать ли SSL-соединение.	1 – использовать; - другое значение или не задано – не использовать.
OPENUDPPORT	Открыть ли UDP-порт.	1 – открывать; - другое значение или не задано – не открывать.
UDPPORT	Номер UDP-порта.	Числовое значение.
USEPROXY	Использовать ли прокси-сервер. В целях совместимости не рекомендуется указывать параметры подключения к прокси-серверу в параметрах инсталляционного пакета Агента администрирования.	1 – использовать; - другое значение или не задано – не использовать.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Адрес прокси-сервера и номер порта для подключения к прокси-серверу.	Строковое значение.
PROXYLOGIN	Учетная запись для подключения к прокси-серверу.	Строковое значение.
PROXYPASSWORD	Пароль учетной записи для подключения к прокси-серверу (Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.)	Строковое значение.
GATEWAYMODE	Режим использования шлюза соединения.	0 – не использовать шлюз соединений; 1 – использовать данный Агент администрирования в качестве шлюза соединений; 2 – подключаться к Серверу администрирования через шлюз соединений.
GATEWAYADDRESS	Адрес шлюза соединений.	Строковое значение.
CERTSELECTION	Способ получения сертификата.	- GetOnFirstConnection – получить сертификат от Сервера администрирования; - GetExistent – задать существующий сертификат. Если выбран этот вариант, должно быть задано свойство CERTFILE.
CERTFILE	Путь к файлу сертификата.	Строковое значение.

Свойство MSI	Описание	Доступные значения
VMVDI	Включить динамический режим для VDI.	1 – включать; 0 – не включать; - Значение не задано – не включать.
VMOPTIMIZE	Являются ли параметры Агента администрирования оптимальными для гипервизора.	1 – включать; 0 – не включать; - Значение не задано – не включать.
LAUNCHPROGRAM	Запускать ли службу Агента администрирования после установки. Параметр игнорируется, если VMVDI=1.	1 – запускать; - другое значение или не задано – не запускать.
NAGENTTAGS	Тег для Агента администрирования (имеет приоритет над тегом, указанным в файле ответов).	Строковое значение.

См. также:

Общая информация.....	178
Установка в тихом режиме (с файлом ответов).....	179
Установка Агента администрирования в тихом режиме	193
Установка Агента администрирования в тихом режиме (без файла ответов).....	180
Порты, используемые Kaspersky Security Center	63
Частичная настройка параметров установки через setup.exe	181
Параметры установки Сервера администрирования	181

Виртуальная инфраструктура

Kaspersky Security Center поддерживает работу с виртуальными машинами. Вы можете установить Агент администрирования и приложения безопасности на каждую виртуальную машину, а также вы можете защищать виртуальные машины на уровне гипервизора. В первом случае для защиты виртуальных машин можно использовать как обычную программу безопасности, так и Kaspersky Security для виртуальных сред Легкий агент. Во втором случае вы можете использовать Kaspersky Security для виртуальных сред Защита без агента.

Kaspersky Security Center поддерживает откат виртуальных машин к предыдущему состоянию (см. раздел "Поддержка отката файловой системы для устройств с Агентом администрирования" на стр. [190](#)).

См. также:

Основной сценарий установки.....	56

В этом разделе

Рекомендации по снижению нагрузки на виртуальные машины.....	188
Поддержка динамических виртуальных машин	189
Поддержка копирования виртуальных машин	189

Рекомендации по снижению нагрузки на виртуальные машины

В случае инсталляции Агента администрирования на виртуальную машину следует рассмотреть возможность отключения той части функциональности Kaspersky Security Center, которая не очень полезна для виртуальных машин.

При установке Агента администрирования на виртуальную машину или на шаблон, из которого в дальнейшем будут получены виртуальные машины, рекомендуется выполнить следующие действия:

- если выполняется удаленная установка, в окне свойств инсталляционного пакета Агента администрирования (в разделе **Дополнительно**) выбрать параметр **Оптимизировать параметры для VDI**;
- если выполняется интерактивная установка с помощью мастера, в окне мастера выбрать параметр **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**.

Выбор параметров изменит параметры Агента администрирования таким образом, чтобы по умолчанию (до применения политики) были выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

Как правило, перечисленные функции не нужны на виртуальных машинах в силу того, что программное обеспечение и виртуальное аппаратное обеспечение на них единообразны.

Выключение функций обратимо. Если любая из выключенных функций все же нужна, ее можно включить при помощи политики Агента администрирования, или в локальных параметрах Агента администрирования. Локальные параметры Агента администрирования доступны из контекстного меню соответствующего устройства в Консоли администрирования.

См. также:

Основной сценарий установки.....	56

Поддержка динамических виртуальных машин

Kaspersky Security Center поддерживает динамические виртуальные машины. Если в сети организации развернута виртуальная инфраструктура, то в некоторых случаях могут использоваться динамические (временные) виртуальные машины. Такие машины создаются с уникальными именами из заранее подготовленного администратором шаблона. Пользователь работает с созданной машиной некоторое время, а после выключения виртуальная машина удаляется из виртуальной инфраструктуры. Если в сети организации развернут Kaspersky Security Center, то виртуальная машина с установленным на ней Агентом администрирования добавляется в базу данных Сервера администрирования. После выключения виртуальной машины запись о ней должна быть также удалена и из базы данных Сервера администрирования.

Чтобы функциональность автоматического удаления записей о виртуальных машинах работала, при установке Агента администрирования на шаблон, из которого будут созданы динамические виртуальные машины, нужно выбрать параметр **Включить динамический режим для VDI**:

- в случае удаленной установки – в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**) (см. раздел "Параметры инсталляционного пакета Агента администрирования" на стр. [201](#));
- в случае интерактивной установки – в мастере установки Агента администрирования (см. раздел "Локальная установка Агента администрирования" на стр. [193](#)).

Параметр **Включить динамический режим для VDI** не следует выбирать при установке Агента администрирования на физические устройства.

Если нужно, чтобы события с динамических виртуальных машин сохранялись на Сервере администрирования некоторое время после удаления машин, то следует в окне свойств Сервера администрирования в разделе **Хранилище событий** выбрать параметр **Хранить события после удаления устройств** и указать максимальное время хранения событий в днях.

См. также:

Основной сценарий установки.....[56](#)

Поддержка копирования виртуальных машин

Копирование виртуальной машины с установленным на нее Агентом администрирования или ее создание из шаблона с установленным Агентом администрирования эквивалентно развертыванию Агентов администрирования захватом и копированием образа жесткого диска. Поэтому в общем случае при копировании виртуальных машин нужно выполнять те же действия, что и при развертывании копированием образа диска (см. раздел "Развертывание захватом и копированием образа устройства" на стр. [167](#)).

Однако в описанных ниже двух случаях Агент администрирования обнаруживает факт копирования автоматически. Поэтому выполнять сложные действия, описанные в разделе «Развертывание захватом и копированием жесткого диска устройства», необязательно:

- При установке Агента администрирования был выбран параметр **Включить динамический режим для VDI**: после каждой перезагрузки операционной системы такая виртуальная машина будет считаться новым устройством, независимо от факта ее копирования.

- Используется один из следующих гипервизоров: VMware™, HyperV® или Xen®: Агент администрирования определит факт копирования виртуальной машины по изменившимся идентификаторам виртуального аппаратного обеспечения.

Анализ изменений виртуального аппаратного обеспечения не абсолютно надежен. Прежде чем широко использовать данный метод, следует предварительно проверить его работоспособность на небольшом количестве виртуальных машин для используемой в организации версии гипервизора.

См. также:

Основной сценарий установки.....56

Поддержка отката файловой системы для устройств с Агентом администрирования

Kaspersky Security Center является распределенным приложением. Откат файловой системы в предыдущее состояние на одном из устройств с установленным Агентом администрирования приведет к рассинхронизации данных и неправильной работе Kaspersky Security Center.

Откат файловой системы (или ее части) в предыдущее состояние может происходить в следующих случаях:

- при копировании образа жесткого диска;
- при восстановлении состояния виртуальной машины средствами виртуальной инфраструктуры;
- при восстановлении данных из резервной копии или точки восстановления.

Для Kaspersky Security Center критичны только те сценарии, при которых стороннее программное обеспечение на устройствах с установленным Агентом администрирования затрагивает папку %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\l. Поэтому следует всегда исключать эту папку из процедуры восстановления, если это возможно.

Поскольку в ряде организаций регламент работы предполагает выполнение отката состояния файловой системы устройств, в Kaspersky Security Center, начиная с версии 10 Maintenance Release 1 (Сервер администрирования и Агенты администрирования должны быть версии 10 Maintenance Release 1 или выше), была добавлена поддержка обнаружения отката файловой системы на устройствах с установленным Агентом администрирования. В случае обнаружения такие устройства автоматически переподключаются к Серверу администрирования с полной очисткой и полной синхронизацией данных.

В Kaspersky Security Center поддержка обнаружения отката файловой системы включена по умолчанию.

Следует при любой возможности избегать отката папки %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\l на устройствах с установленным Агентом администрирования, так как полная повторная синхронизация данных требует большого количества ресурсов.

Для устройства с установленным Сервером администрирования откат состояния системы недопустим. Недопустимым также является откат в предыдущее состояние базы данных, используемой Сервером администрирования.

Восстановить состояние Сервера администрирования из резервной копии можно только при помощи штатной утилиты klbackup (см. раздел "Резервное копирование и восстановление параметров Сервера администрирования" на стр. [721](#)).

Локальная установка приложений

В этом разделе описана процедура установки приложений, которые могут быть установлены на устройства только локально.

Для проведения локальной установки приложений на выбранном клиентском устройстве вам необходимо обладать правами администратора на этом устройстве.

► Чтобы установить приложения локально на выбранное клиентское устройство:

1. Установите на клиентское устройство Агент администрирования и настройте связь клиентского устройства с Сервером администрирования.
2. Установите на устройство необходимые приложения согласно описаниям, изложенным в Руководствах к этим приложениям.
3. Установите на рабочее место администратора плагин управления для каждого из установленных приложений.

Kaspersky Security Center также поддерживает возможность локальной установки приложений с помощью автономного инсталляционного пакета. Kaspersky Security Center не поддерживает установку всех приложений «Лаборатории Касперского» (см. раздел «Совместимые приложения и решения “Лаборатории Касперского”» на стр. [29](#)).

В этом разделе

Локальная установка Агента администрирования	193
Установка Агента администрирования в тихом режиме	193
Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)	195
Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования	196
Установка Агента администрирования для Linux в интерактивном режиме	197
Локальная установка плагина управления приложением	199
Установка приложений в тихом режиме	199
Установка приложений с помощью автономных пакетов	200
Параметры инсталляционного пакета Агента администрирования	201
Просмотр Политики конфиденциальности	205

См. также:

Совместимые приложения и решения "Лаборатории Касперского"	29
Основной сценарий установки	56

Локальная установка Агента администрирования

► Чтобы установить Агент администрирования на устройство локально:

1. На устройстве запустите файл `setup.exe` из дистрибутива, полученного через интернет. Дополнительную информацию см. в следующих разделах: Получение инсталляционного пакета Агента администрирования из комплекта поставки Kaspersky Security Center (на стр. [378](#)).
Откроется окно с выбором приложений "Лаборатории Касперского" для установки.
2. В окне с выбором приложений по ссылке **Установить только Агент администрирования Kaspersky Security Center** запустите мастер установки Агента администрирования. Следуйте далее указаниям мастера.
 - a. **Сервер администрирования**
 - b. **Конфигурация прокси-сервера**
 - c. **Шлюз соединения**
 - d. **Сертификат Сервера администрирования**
 - e. **Теги агента**
 - f. **Дополнительные параметры**
 - g. **Запуск приложения**

По окончании работы мастера установки Агент администрирования будет установлен на устройстве.

Вы можете просмотреть свойства службы Агента администрирования Kaspersky Security Center, а также запускать, останавливать и контролировать активность Агента администрирования с помощью стандартных инструментов Microsoft Windows: Управление компьютером\Службы.

См. также:

Поддержка динамических виртуальных машин	189
Просмотр Политики конфиденциальности	205

Установка Агента администрирования в тихом режиме

Агент администрирования может быть установлен в тихом режиме, то есть без интерактивного ввода параметров установки. Для тихой установки используется инсталляционный пакет (MSI) Агента администрирования. MSI-файл расположен в дистрибутиве приложения Kaspersky Security Center в папке `Packages\NetAgent\exes`.

Не переименовывайте инсталляционный пакет `Kaspersky Network Agent.msi`. Переименование пакета может привести к ошибкам установки при обновлении Агента администрирования.

Установка Агента администрирования из пакета MSI возможна только в тихом режиме. Интерактивная установка Агента из пакета MSI не поддерживается.

► Чтобы установить Агент администрирования на локальном устройстве в тихом режиме:

1. Прочитайте Лицензионное соглашение (см. раздел "О Лицензионном соглашении" см. стр. [342](#)). Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.

2. Выполните команду

```
msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (PROP1=PROP1VAL PROP2=PROP2VAL).

В список параметров вам нужно включить параметр `EULA=1`. В противном случае Агент администрирования не будет установлен.

Если вы используете стандартные параметры подключения для Kaspersky Security Center и Агента администрирования на удаленных устройствах, выполните команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx  
c:\windows\temp\nag_inst.log SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` – ключ для записи в журнал событий. Журнал событий создается при установке Агента администрирования и сохраняется в папке `C:\windows\temp\nag_inst.log`.

Помимо `nag_inst.log`, приложение создает файл `$klssinstlib.log`, который содержит журнал событий установки. Этот файл хранится в папке `%windir%\temp or %temp%`. Для устранения неполадок вам или специалисту Службы технической поддержки "Лаборатории Касперского" могут потребоваться оба файла журнала – `nag_inst.log` и `$klssinstlib.log`.

Если вам необходимо дополнительно указать порт для подключения к Серверу администрирования, введите команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx  
c:\windows\temp\nag_inst.log SERVERADDRESS=kscserver.mycompany.com EULA=1  
SERVERPORT=14000
```

Параметр `SERVERPORT` соответствует номеру порта подключения к Серверу администрирования.

Имена и возможные значения параметров, которые можно использовать при установке Агента администрирования в тихом режиме, приведены в разделе Параметры установки Агента администрирования (на стр. [185](#)).

См. также:

Параметры установки Агента администрирования	185
Параметры установки Сервера администрирования	181
Установка Агента администрирования в тихом режиме (без файла ответов).....	180
Просмотр Политики конфиденциальности	205

Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)

Вы можете установить Агент администрирования на устройства с операционной системой Linux с помощью файла ответов – текстового файла, который содержит пользовательский набор параметров установки: переменные и их соответствующие значения. Использование файла ответов позволяет запустить установку в тихом режиме, то есть без участия пользователя.

► Чтобы выполнить установку Агента администрирования для Linux в тихом режиме:

1. Подготовьте требуемое устройство с операционной системой Linux для удаленной установки (см. раздел "Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux" см. стр. [384](#)). Загрузите и создайте пакет удаленной установки, используя пакет Агента администрирования .deb или .rpm, с помощью любой подходящей системы управления пакетами.
2. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat (см. раздел "Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования" см. стр. [386](#)), чтобы настроить Агент администрирования.

Если вы хотите установить Агент администрирования на устройства с операционной системой РЕД ОС 7.3.4 или выше, установите пакет libxscrypt-compat для корректной работы Агента администрирования.

3. Прочитайте Лицензионное соглашение (см. раздел "О Лицензионном соглашении" см. стр. [342](#)). Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.
4. Задайте значение переменной среды KLAUTOANSWERS, введя полное имя файла ответов (включая путь), например, следующим образом:

```
export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
```

5. Создайте файл ответов (в формате TXT) в каталоге, который вы указали в переменной среды. Добавьте в файл ответов список переменных в формате VARIABLE_NAME = variable_value, каждая переменная находится на отдельной строке.

Для правильного использования файла ответов вам нужно включить в него минимальный набор из трех обязательных переменных:

- KLNAGENT_SERVER
- KLNAGENT_AUTOINSTALL
- EULA_ACCEPTED

Вы также можете добавить любые дополнительные переменные, чтобы использовать более конкретные параметры вашей удаленной установки. В следующей таблице перечислены все переменные, которые можно включать в файл ответов:

Переменные файла ответов, используемые в качестве параметров установки Агента администрирования для Linux в тихом режиме

6. Установка Агента администрирования:

- Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
`# rpm -i klnagent-<номер сборки>.i386.rpm`
- Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
`# rpm -i klnagent64-<номер сборки>.x86_64.rpm`
- Чтобы установить Агент администрирования из RPM-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
`# rpm -i klnagent64-<номер сборки>.aarch64.rpm`
- Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
`# apt-get install ./klnagent_<номер сборки>_i386.deb`
- Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
`# apt-get install ./klnagent64_<номер сборки>_amd64.deb`
- Чтобы установить Агент администрирования из DEB-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
`# apt-get install ./klnagent64_<номер сборки>_arm64.deb`

Установка Агента администрирования для Linux начинается в тихом режиме; пользователю не предлагается выполнять никаких действий во время процесса.

Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования

Перед установкой Агента администрирования на устройство под управлением Astra Linux в режиме замкнутой программной среды вам нужно выполнить две подготовительные процедуры: одну, которая описана в приведенных ниже инструкциях, и общие подготовительные шаги для любого устройства с операционной системой Linux (см. раздел "Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux" см. стр. [384](#)).

Предварительные условия:

- Убедитесь, что на устройстве, на которое вы хотите установить Агент администрирования Linux, работает один из поддерживаемых дистрибутивов Linux (см. раздел "Аппаратные и программные требования" см. стр. [29](#)).

- Загрузите установочный файл Агента администрирования с сайта "Лаборатории Касперского" <https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint>.

Выполните команды, представленные в этой инструкции, под учетной записью root.

► Чтобы подготовить устройство под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования:

1. Откройте файл `/etc/digsig/digsig_initramfs.conf` и укажите следующие параметры:
`DIGSIG_ELF_MODE=1`
2. В командной строке введите следующую команду, чтобы установить пакет совместимости:
`apt install astra-digsig-oldkeys`
3. Создайте директорию для ключа приложения:
`mkdir -p /etc/digsig/keys/legacy/kaspersky/`
4. Поместите ключ приложения `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` в директорию, созданную на предыдущем шаге:
`cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/`

Если в комплект поставки Kaspersky Security Center не входит ключ `kaspersky_astra_pub_key.gpg`, вы можете загрузить этот ключ по ссылке https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Обновите оперативную память дисков:
`update-initramfs -u -k all`
Перезагрузите систему.
6. Выполните шаги подготовки, общие для любого устройства с операционной системой Linux (см. раздел "Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux" см. стр. [384](#)).

Устройство подготовлено. Теперь вы можете приступить к установке Агента администрирования (см. раздел "Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux" см. стр. [384](#)).

Установка Агента администрирования для Linux в интерактивном режиме

В этой статье описывается, как установить Агент администрирования на устройства с операционной системой Linux в интерактивном режиме, указав параметры установки шаг за шагом. Вы также можете использовать файл ответов – текстовый файл, который содержит пользовательский набор параметров установки: переменные и их соответствующие значения. Использование файла ответов позволяет запустить установку в тихом режиме (см. раздел "Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)" см. стр. [195](#)), то есть без участия пользователя.

Если вы хотите установить Агент администрирования на устройства с операционной системой РЕД ОС 7.3.4 или выше, установите пакет `libxscrypt-compat` для корректной работы Агента администрирования.

► Чтобы установить Агент администрирования в интерактивном режиме:

1. Запустите инсталляционный пакет Агент администрирования. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:

- Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-битной операционной системой:

```
# yum -i klnagent-<номер сборки>.i386.rpm
```

- Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-битной операционной системой:

```
# yum -i klnagent64-<номер сборки>.x86_64.rpm
```

- Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-битной операционной системой для Arm-архитектуры:

```
# yum -i klnagent64-<номер сборки>.aarch64.rpm
```

- Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-битной операционной системой:

```
# apt install ./klnagent_<номер сборки>_i386.deb
```

- Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-битной операционной системой:

```
# apt install ./klnagent64_<номер сборки>_amd64.deb
```

- Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-битной операционной системой для Arm-архитектуры:

```
# apt install ./klnagent64_<номер сборки>_arm64.deb
```

2. Запустите настройку Агента администрирования:

```
# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl
```

3. Прочитайте Лицензионное соглашение (см. раздел "О Лицензионном соглашении" см. стр. [342](#)). Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите одно из следующих значений:

- Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения.
- Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать Агент администрирования, вам нужно принять условия Лицензионного соглашения.
- Введите `r`, чтобы снова отобразить Лицензионное соглашение.

4. Введите DNS-имя Сервера администрирования или IP-адрес.

5. Введите номер порта Сервера администрирования. По умолчанию номер порта – 14000.

6. Введите номер SSL-порта Сервера администрирования. По умолчанию номер порта – 13000.

7. Введите `y`, если вы хотите использовать SSL-шифрование для трафика между Агентом администрирования и Сервером администрирования. Иначе введите `n`.

8. Выберите один из следующих способов настройки Агента администрирования:

- [1] – не настраивать шлюз соединения.

Ваше устройство не будет выступать в роли шлюза соединения и не будет подключаться к Серверу администрирования через шлюз соединения.

- [2] – не использовать шлюз соединения.

Ваше устройство не будет подключаться к Серверу администрирования через шлюз соединения.

- [3] – подключитесь к Серверу с помощью шлюза соединения.

Ваше устройство будет подключаться к Серверу администрирования через шлюз соединения.

- [4] – использовать в качестве шлюза соединения.

Ваше устройство будет выступать в роли шлюза соединения.

Агент администрирования установлен на устройстве с операционной системой Linux.

См. также:

Поддержка динамических виртуальных машин	189
Просмотр Политики конфиденциальности	205

Локальная установка плагина управления приложением

► Чтобы установить плагин управления приложением,

на устройстве, где установлена Консоль администрирования, запустите исполняемый файл `klcfginst.exe`, входящий в дистрибутив этого приложения.

Файл `klcfginst.exe` входит в состав всех приложений, которыми может управлять Kaspersky Security Center. Установка сопровождается мастером и не требует настройки параметров.

Установка приложений в тихом режиме

► Чтобы установить приложение в тихом режиме:

1. Откройте главное окно приложения Kaspersky Security Center.
2. В папке дерева консоли **Удаленная установка** во вложенной папке **Инсталляционные пакеты** выберите инсталляционный пакет нужного приложения или сформируйте для этого приложения новый инсталляционный пакет.

Инсталляционный пакет будет сохранен на Сервере администрирования в папке общего доступа в служебной папке `Packages`. При этом каждому инсталляционному пакету соответствует отдельная вложенная папка.

3. Откройте папку нужного инсталляционного пакета одним из следующих способов:

- Скопируйте папку, соответствующую нужному инсталляционному пакету, с Сервера администрирования на клиентское устройство. Затем откройте скопированную папку на клиентском устройстве.
- С клиентского устройства откройте на Сервере администрирования папку общего доступа, соответствующую нужному инсталляционному пакету.

Если папка общего доступа расположена на устройстве с установленной операционной системой Microsoft Windows Vista, необходимо установить значение **Выключено** для параметра **Управление учетными записями пользователей: все администраторы работают в режиме одобрения администратором** (Пуск → Панель управления → Администрирование → Локальная политика безопасности → Параметры безопасности).

4. В зависимости от выбранного приложения выполните следующие действия:
 - Для Антивируса Касперского для Windows Workstations, Антивируса Касперского для Windows Servers и Kaspersky Security Center перейдите во вложенную папку ехес и запустите исполняемый файл (файл с расширением ехе) с ключом /s.
 - Для остальных приложений "Лаборатории Касперского" запустите из открытой папки исполняемый файл (файл с расширением ехе) с ключом /s.

Запуск исполняемого файла с ключами EULA=1 и PRIVACYPOLICY=1 означает, что вы полностью прочитали, поняли и принимаете положения Лицензионного соглашения (см. раздел "О Лицензионном соглашении" см. стр. 342) и Политики конфиденциальности (см. раздел "Просмотр Политики конфиденциальности" см. стр. 205) соответственно. Вам также известно, что ваши данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности. Текст Лицензионного соглашения и текст Политики конфиденциальности входят в комплект поставки Kaspersky Security Center. Согласие с положениями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки приложения или обновления предыдущей версии приложения.

Установка приложений с помощью автономных пакетов

Kaspersky Security Center позволяет формировать автономные инсталляционные пакеты приложений. Автономный инсталляционный пакет представляет собой исполняемый файл, который можно разместить на Веб-сервере, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки приложения без участия Kaspersky Security Center.

► Чтобы установить приложение с помощью автономного инсталляционного пакета:

1. Подключитесь к нужному Серверу администрирования.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В рабочей области выберите инсталляционный пакет нужного приложения.
4. Запустите процесс создания автономного инсталляционного пакета одним из следующих способов:
 - В контекстном меню инсталляционного пакета выберите пункт **Создать автономный инсталляционный пакет**.

- Перейдите по ссылке **Создать автономный инсталляционный пакет** в рабочей области инсталляционного пакета.

В результате запускается мастер создания автономного инсталляционного пакета. Следуйте далее указаниям мастера.

На завершающем шаге мастера выберите способ передачи автономного инсталляционного пакета на клиентское устройство.

5. Передайте автономный инсталляционный пакет приложения на клиентское устройство.
6. Запустите автономный инсталляционный пакет на клиентском устройстве.

В результате приложение будет установлено на клиентском устройстве с параметрами, указанными в автономном пакете.

При создании автономный инсталляционный пакет автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных инсталляционных пакетов. При необходимости вы можете отменить публикацию выбранного автономного пакета и снова опубликовать его на Веб-сервере. По умолчанию для загрузки автономных инсталляционных пакетов используется порт 8060.

Параметры инсталляционного пакета Агента администрирования

► Чтобы настроить параметры инсталляционного пакета Агента администрирования:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

Откроется окно свойств инсталляционного пакета Агента администрирования.

Общие

Раздел **Общие** содержит общую информацию об инсталляционном пакете:

- название инсталляционного пакета;
- имя и версию приложения, для которого сформирован инсталляционный пакет;
- размер инсталляционного пакета;
- дату создания инсталляционного пакета;
- путь к папке размещения инсталляционного пакета.

Параметры

В этом разделе можно настроить параметры, необходимые для обеспечения работоспособности Агента администрирования сразу после его установки.

В блоке параметров **Папка установки** можно выбрать папку на клиентском устройстве, в которую будет установлен Агент администрирования:

- **Устанавливать в папку по умолчанию**

Если выбран этот вариант, Агент администрирования будет установлен в папку <Диск>:\Program Files\Kaspersky Lab\NetworkAgent. Если такой папки нет, она будет

создана автоматически.

Этот вариант выбран по умолчанию.

- **Устанавливать в заданную папку**

Если выбран этот вариант, Агент администрирования будет установлен в папку, указанную в поле ввода.

В блоке параметров ниже можно задать пароль для задачи удаленной деинсталляции Агента администрирования:

- **Использовать пароль деинсталляции**

Если флажок установлен, при нажатии на кнопку **Изменить** можно ввести пароль для удаления приложения (доступно только для Агента администрирования на устройствах под управлением операционных систем семейства Windows).

По умолчанию флажок снят.

- **Статус**

Статус пароля: **Пароль установлен** или **Пароль не установлен**.

По умолчанию пароль не установлен.

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

Если этот параметр включен, после того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

По умолчанию параметр выключен.

- **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**

Если флажок установлен, то загруженные обновления и патчи для Сервера администрирования, Агента администрирования, Консоли администрирования и Сервера iOS MDM будут устанавливаться автоматически (автоматическая установка доступна для Агента администрирования начиная с версии Kaspersky Security Center 10 Service Pack 2).

Если флажок снят, то загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобен*. Обновления и патчи со статусом *Не определено* не будут установлены.

По умолчанию флажок установлен.

Подключение

В этом разделе можно настроить параметры подключения Агента администрирования к Серверу администрирования. Для установления соединения можно использовать SSL-протокол или UDP-протокол. Для настройки соединения укажите следующие параметры:

- **Сервер администрирования**

Адрес устройства, на котором установлен Сервер администрирования.

- **Порт**

Номер порта, по которому будет выполняться подключение.

- **SSL-порт**

Номер порта, по которому будет выполняться подключение с использованием протокола SSL.

- **Использовать сертификат Сервера**

Если флажок установлен, для аутентификации доступа Агента администрирования к Серверу администрирования будет использоваться файл сертификата, который можно указать при нажатии на кнопку **Обзор**.

Если флажок не установлен, файл сертификата будет получен с Сервера администрирования при первом подключении Агента администрирования по адресу, указанному в поле **Адрес сервера**.

Не рекомендуется снимать флажок, так как автоматическое получение сертификата Сервера администрирования Агентом администрирования при подключении к Серверу является небезопасным.

По умолчанию флажок установлен.

- **Использовать SSL**

Если флажок установлен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

По умолчанию флажок снят.

- **Использовать UDP-порт**

Если флажок установлен, подключение Агента администрирования к Серверу администрирования будет выполняться через UDP-порт.

По умолчанию флажок установлен.

- **Номер UDP-порта**

В поле можно указать номер порта подключения Агента администрирования к Серверу администрирования по протоколу UDP.

По умолчанию номер UDP-порта – 15000.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

Если флажок установлен, после установки Агента администрирования на клиентском устройстве в список исключений брандмауэра Microsoft Windows будет добавлен UDP-порт, необходимый для работы Агента администрирования.

По умолчанию флажок установлен.

- **Использовать прокси-сервер**

В целях совместимости не рекомендуется указывать параметры подключения к прокси-серверу в параметрах инсталляционного пакета Агента администрирования.

Дополнительно

В разделе **Дополнительно**, вы можете настроить, как использовать шлюз соединения. Для этого можно выполнить следующие действия:

- Используйте Агент администрирования в качестве шлюза соединения в демилитаризованной зоне (DMZ) для подключения к Серверу администрирования, связи с ним и сохранения данных в безопасности на Агента администрирования (см. раздел "Шлюз соединения" см. стр. [54](#)), во время передачи данных.
- Подключайтесь к Серверу администрирования с помощью шлюза соединения, чтобы уменьшить количество подключений к Серверу администрирования. В этом случае введите адрес устройства, которое будет выступать в качестве шлюза соединения в поле **Адрес шлюза соединения**.
- Настройте подключение для Virtual Desktop Infrastructure (VDI), если в вашей сети есть виртуальные машины. Для этого выполните следующее:

- **Включить динамический режим для VDI**

Если флажок установлен, для Агента администрирования, установленного на виртуальной машине, будет включен динамический режим для Virtual Desktop Infrastructure (VDI).

По умолчанию флажок снят.

- **Оптимизировать параметры для VDI**

Если флажок установлен, в параметрах Агента администрирования выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

По умолчанию флажок снят.

Дополнительные компоненты

В этом разделе можно выбрать дополнительные компоненты для совместной установки с Агентом администрирования.

Теги

В разделе **Теги** отображается список ключевых слов (тегов), которые можно добавлять клиентским устройствам после установки на них Агента администрирования. Вы можете добавлять и удалять теги из списка, а также переименовывать теги.

Если рядом с тегом установлен флажок, тег будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования.

Если флажок рядом с тегом снят, тег не будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования. Этот тег можно добавить устройствам вручную.

При удалении тега из списка тег автоматически снимается со всех устройств, которым он добавлен.

История ревизий

В этом разделе можно посмотреть историю ревизий инсталляционного пакета (см. раздел "Работа с ревизиями объектов" на стр. [852](#)). Вы можете сравнивать ревизии, просматривать ревизии, сохранять ревизии в файл, добавлять и изменять описания ревизий.

Параметры инсталляционного пакета Агента администрирования доступны для конкретной операционной системы, которые приведены в таблице ниже.

Таблица 44. Параметры инсталляционного пакета Агента администрирования

Раздел свойств	Windows	Mac	Linux
Общие	✓	✓	✓
Параметры	✓	—	—
Подключение	✓	✓ (кроме параметров Открывать порты Агента администрирования в брандмауэре Microsoft Windows и Использовать только автоматическое определение прокси- сервера))	✓ (кроме параметров Открывать порты Агента администрирования в брандмауэре Microsoft Windows и Использовать только автоматическое определение прокси- сервера))
Дополнительно	✓	✓	✓
Дополнительные компоненты	✓	✓	✓
Теги	✓	✓ (кроме правил автоматического назначения тегов)	✓ (кроме правил автоматического назначения тегов)
История ревизий	✓	✓	✓

Просмотр Политики конфиденциальности

Политика конфиденциальности доступна в интернете на странице <https://www.kaspersky.ru/products-and-services-privacy-policy>; также она доступна в офлайн-режиме. Вы можете ознакомиться с Политикой конфиденциальности, например, перед установкой Агента администрирования.

► Чтобы прочитать Политику конфиденциальности в офлайн-режиме:

1. Запустите установщик Kaspersky Security Center.
2. В окне установщика перейдите по ссылке **Извлечь инсталляционные пакеты**.
3. В открывшемся списке выберите Агент администрирования Kaspersky Security Center и нажмите на кнопку **Далее**.

Файл privacy_policy.txt появится на вашем устройстве в указанной вами папке в подпапке NetAgent.

Установка Kaspersky Security Center

В этом разделе описывается установка компонентов Kaspersky Security Center. Если вы хотите установить приложение локально только на одно устройство, доступны два варианта установки:

- **Стандартная.** Этот параметр рекомендуется, если вы хотите ознакомиться с программой Kaspersky Security Center, например, протестировать ее работу на небольшом участке вашей сети. При стандартной установке вы настраиваете только параметры базы данных. Также вы можете установить только набор плагинов управления, заданный по умолчанию, для приложений "Лаборатории Касперского". Вы также можете воспользоваться стандартной установкой, если вы уже имеете опыт работы с Kaspersky Security Center и знаете, как после стандартной установки настроить все необходимые вам параметры.
- **Выборочная.** Этот параметр рекомендуется, если вы планируете настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления приложениями "Лаборатории Касперского" будут установлены. При необходимости вы можете запустить выборочную установку в тихом режиме (см. раздел "Установка Сервера администрирования в тихом режиме" на стр. [264](#)).

Если в сети установлен хотя бы один Сервер администрирования, Серверы на других устройствах сети могут быть установлены с помощью задачи удаленной установки методом принудительной установки (см. раздел "Установка приложений с помощью задачи удаленной установки" на стр. [359](#)). При создании задачи удаленной установки приложения необходимо использовать инсталляционный пакет Сервера администрирования: `ksc_<номер_версии>.<номер сборки>_full_<язык локализации>.exe`.

Используйте этот пакет, если вы хотите установить все компоненты, необходимые для работы всех функций Kaspersky Security Center, или обновить существующие версии этих компонентов.

Если хотите развернуть отказоустойчивый кластер Kaspersky Security Center (см. раздел "Развертывание отказоустойчивого кластера Kaspersky Security Center" на стр. [244](#)), вам необходимо установить Kaspersky Security Center на все узлы кластера.

См. также:

Основной сценарий установки.....[56](#)

Подготовка к установке

Выполните следующие действия перед запуском установки.

- Проверка требований к оборудованию и программному обеспечению
Убедитесь, что аппаратное и программное обеспечение устройства соответствует требованиям, предъявляемым к Серверу администрирования и Консоли администрирования (см. раздел "Аппаратные и программные требования" на стр. [29](#)).
- Выбор и установка системы управления базами данных (СУБД)

Kaspersky Security Center хранит свою информацию в базе данных, управляемой СУБД. Установите СУБД в сети до установки Kaspersky Security Center (узнайте больше о том, как выбрать СУБД). Если вы решили установить СУБД PostgreSQL или Postgres Pro, укажите пароль для суперпользователя. Если пароль не указан, Сервер администрирования может не подключиться к базе данных.

Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

- Подготовка папок для Сервера администрирования, Агента администрирования и Консоли администрирования

Сервер администрирования, Агент администрирования и Консоль администрирования должны быть установлены в папках, в которых выключен учет регистра. Также необходимо выключить учет регистра для общей папки Сервера администрирования и скрытой папки Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\admindkit).

- Удалите старую версию Агента администрирования

Вместе с компонентом Сервер администрирования на устройство будет установлена серверная версия Агента администрирования. Его совместная установка с обычной версией Агента администрирования невозможна. Если серверная версия Агента администрирования уже установлена на вашем устройстве, требуется удалить ее и запустить установку Сервера администрирования повторно. Подробнее о серверной версии Агента администрирования см. раздел Изменения в системе после установки Kaspersky Security Center (на стр. [271](#)).

- Проверка учетных записей

Для установки Kaspersky Security Center необходимо наличие прав локального администратора на устройстве, где осуществляется установка.

Kaspersky Security Center поддерживает управляемые учетные записи службы и групповые управляемые учетные записи службы. Если эти типы учетных записей используются в вашем домене и вы хотите указать одну из них в качестве учетной записи для службы Сервера администрирования, то сначала установите учетную запись на том же устройстве, на котором вы хотите установить Сервер администрирования. Подробнее об установке управляемых учетных записей служб на локальном устройстве см. в официальной документации Microsoft.

Учетные записи для работы с СУБД

Для установки Сервера администрирования и работы с ним вам потребуется учетная запись Windows, под которой вы будете запускать приложение установки Сервера администрирования (далее также "инсталлятор"), учетная запись Windows, под которой вы будете запускать службу Сервера администрирования, и внутренняя учетная запись СУБД для доступа к СУБД. Можно создать учетные записи или использовать существующие. Все эти учетные записи требуют определенных прав. Набор необходимых учетных записей и их права зависят от следующих критериев:

- Тип СУБД (см. раздел "Выбор СУБД для Сервера администрирования" на стр. [139](#)):
 - Microsoft SQL Server (с аутентификацией Windows или с аутентификацией SQL Server).
 - MySQL или MariaDB.
 - PostgreSQL или Postgres Pro.

- Расположение СУБД:
 - **Локальная СУБД.** *Локальной СУБД* называется СУБД, установленная на том же устройстве, что и Сервер администрирования.
 - **Удаленная СУБД.** *Удаленной СУБД* называется СУБД, установленная на другом устройстве.
- Способ создания базы данных Сервера администрирования:
 - **Автоматически.** При установке Сервера администрирования вы можете автоматически создать базу данных Сервера администрирования (далее также база данных Сервера) с помощью инсталлятора.
 - **Вручную.** Можно использовать приложение стороннего производителя (например, SQL Server Management Studio) или скрипт для создания пустой базы данных. После этого вы можете указать эту базу данных в качестве базы данных Сервера при установке Сервера администрирования.

При предоставлении прав и разрешений учетным записям соблюдайте принцип наименьших привилегий. Это означает, что предоставленных прав достаточно только для выполнения требуемых действий.

В приведенных ниже таблицах содержится информация о системных правах и правах на СУБД, которые требуется предоставить учетным записям перед установкой и запуском Сервера администрирования.

Microsoft SQL Server с аутентификацией Windows

Если вы выбираете SQL Server в качестве СУБД, можно использовать аутентификацию Windows для доступа к SQL Server. Настройте системные права для учетной записи Windows, используемой для запуска приложения установки, и для учетной записи Windows, используемой для запуска службы Сервера администрирования. В SQL Server создайте учетные записи для этих учетных записей Windows. В зависимости от метода создания базы данных Сервера предоставьте необходимые права SQL Server этим учетным записям, как описано в таблице ниже. Подробнее о настройке прав учетных записей см. раздел Настройка учетных записей для работы с SQL Server (аутентификация Windows) (на стр. [215](#)).

Таблица 45. Microsoft SQL Server (в том числе и Express Edition) с аутентификацией Windows

	Автоматическое создание базы данных (приложением установки)	Создание базы данных вручную (администратором)
Учетная запись, от имени которой работает инсталлятор	- Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. - Локальная СУБД: учетная запись локального администратора или учетная запись домена.	- Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. - Локальная СУБД: учетная запись локального администратора или учетная запись домена.
Права учетной записи, от имени которой работает инсталлятор	- Системные права: права локального администратора. - Права SQL Server: Роль уровня сервера: sysadmin.	- Системные права: права локального администратора. - Права SQL Server: Роль уровня сервера: public. Роль членства базы данных для базы данных Сервера: db_owner, public. Схема по умолчанию для базы данных Сервера: dbo.
Учетная запись службы Сервера администрирования	- Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. - Локальная СУБД: Учетная запись Windows, выбранная администратором. Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.	- Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. - Локальная СУБД: Учетная запись Windows, выбранная администратором. Учетная запись в формате KL-AK-*, которую создает приложение установки автоматически (в этом случае не рекомендуется создавать учетную запись KL-AK-* (см. раздел "Настройка учетных записей для работы с SQL Server (аутентификация Windows)" на стр. 215)).
Права учетной записи службы Сервера администрирования	- Системные права: необходимые права, присвоенные инсталлятором. - Права SQL Server: необходимые права, присвоенные инсталлятором.	- Системные права: необходимые права, присвоенные инсталлятором. - Права SQL Server: Роль уровня сервера: public. Роль членства базы данных для базы данных Сервера: db_owner, public. Схема по умолчанию для базы данных Сервера: dbo.

Microsoft SQL Server с аутентификацией SQL Server

Если вы выбираете SQL Server в качестве СУБД, вы можете использовать аутентификацию SQL Server для подключения к SQL Server. Настройте системные права для учетной записи Windows, используемой для запуска приложения установки, и для учетной записи Windows, используемой для работы с Сервером администрирования. В SQL Server создайте учетную запись с паролем, чтобы использовать это для аутентификации. Затем предоставьте этой учетной записи SQL Server необходимые права, перечисленные в таблице ниже. Подробнее о настройке прав учетных записей см. раздел Настройка учетных записей для работы с SQL Server (аутентификация SQL Server) (на стр. 217).

Таблица 46. Microsoft SQL Server (в том числе и Express Edition) с

	Автоматическое создание базы данных (приложением установки)	Создание базы данных вручную (администратором)
Учетная запись, от имени которой работает инсталлятор	- Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. - Локальная СУБД: учетная запись локального администратора или учетная запись домена.	- Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. - Локальная СУБД: учетная запись локального администратора или учетная запись домена.
Права учетной записи, от имени которой работает инсталлятор	Системные права: права локального администратора.	Системные права: права локального администратора.
Учетная запись службы Сервера администрирования	- Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. - Локальная СУБД: - Учетная запись Windows, выбранная администратором. - Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.	- Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. - Локальная СУБД: - Учетная запись пользователя Windows, выбранная администратором. - Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.
Права учетной записи службы Сервера администрирования	Системные права: необходимые права, присвоенные инсталлятором.	Системные права: необходимые права, присвоенные инсталлятором.

	Автоматическое создание базы данных (приложением установки)	Создание базы данных вручную (администратором)
Права учетной записи, используемой для аутентификации SQL Server	Права SQL Server, необходимые для создания базы данных и установки Сервера администрирования: - Роль уровня сервера: public. - Роль членства базы данных для базы данных <i>master</i>: db_owner. - Схема по умолчанию для базы данных <i>master</i>: dbo. - Разрешения: CONNECT ANY DATABASE CONNECT SQL CREATE ANY DATABASE VIEW ANY DATABASE VIEW SERVER STATE (если включен параметр Always On) Права SQL Server, необходимые для работы с Сервером администрирования: - Роль уровня сервера: public. - Роль членства базы данных для базы данных Сервера: db_owner. - Схема по умолчанию для базы данных Сервера: dbo. - Разрешения: CONNECT SQL VIEW ANY DATABASE VIEW SERVER STATE (если включен параметр Always On) VIEW ANY DEFINITION	Права SQL Server: - Роль уровня сервера: public. - Роль членства базы данных для базы данных Сервера: db_owner. - Схема по умолчанию для базы данных Сервера: dbo. - Разрешения: CONNECT SQL VIEW ANY DATABASE VIEW ANY DEFINITION

Настройка прав SQL Server для восстановления данных Сервера администрирования

Чтобы восстановить данные Сервера администрирования из резервной копии, запустите утилиту kbackup под учетной записью Windows, под которой был установлен Сервер администрирования. Перед запуском утилиты kbackup на SQL Server предоставьте права для входа в SQL Server, связанного с этой учетной записью Windows. Права SQL Server различаются в зависимости от версии Сервера администрирования. Для Сервера администрирования версии 14.2 и выше можно назначить серверную роль sysadmin или серверную роль dbcreator.

Таблица 47. Права SQL Server для восстановления базы данных Сервера администрирования

Сервер администрирования версии 14.2 и выше	Другие версии Сервера администрирования
Права SQL Server: Роль уровня сервера: sysadmin.	Права SQL Server: Роль уровня сервера: sysadmin.
- Права SQL Server: Роль уровня сервера: dbcreator. - Разрешения: VIEW ANY DEFINITION Перед запуском утилиты klbackup укажите флаг сервера KLSRV_SKIP_ADJUSTING_DBMS_ACCESS. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Далее выполните следующую команду в командной строке: <pre>klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1</pre>	

MySQL и MariaDB

Если вы выбираете MySQL или MariaDB в качестве СУБД, создайте внутреннюю учетную запись СУБД и предоставьте этой учетной записи необходимые права, перечисленные в таблице ниже. Приложение установки и служба Сервера администрирования используют эту внутреннюю учетную запись СУБД для доступа к СУБД. Обратите внимание, что способ создания базы данных не влияет на набор необходимых прав. Подробнее о настройке прав учетной записи см. раздел Настройка учетных записей для работы с MySQL и MariaDB (на стр. [220](#)).

Таблица 48. MySQL и MariaDB

	Автоматическое или ручное создание базы данных
Учетная запись, от имени которой работает инсталлятор	- Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД. - Локальная СУБД: учетная запись локального администратора или учетная запись домена.
Права учетной записи, от имени которой работает инсталлятор	Системные права: права локального администратора.
Учетная запись службы Сервера администрирования	- Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД. - Локальная СУБД: Учетная запись Windows, выбранная администратором. Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.
Права учетной записи службы Сервера администрирования	Системные права: необходимые права, присвоенные инсталлятором.
Права внутренней учетной записи СУБД	Схема привилегий: - База данных Сервера администрирования: ALL (кроме GRANT OPTION). - Схемы системы (mysql и sys): SELECT, SHOW VIEW. - Хранимая процедура sys.table_exists: EXECUTE (если вы используете MariaDB 10.5 или более раннюю версию в качестве СУБД, вам не нужно предоставлять право EXECUTE). Глобальные привилегии для всех схем: PROCESS, SUPER.

Настройка прав на восстановление данных Сервера администрирования

Прав, которые вы предоставили для внутренней учетной записи СУБД, достаточно для восстановления данных Сервера администрирования из резервной копии. Чтобы начать восстановление, запустите утилиту klbackup под учетной записью Windows, под которой был установлен Сервер администрирования.

PostgreSQL или Postgres Pro.

Если вы выбираете PostgreSQL или Postgres Pro в качестве СУБД, вы можете использовать пользователя *Postgres* (роль *Postgres* по умолчанию) или создать роль *Postgres* (далее также роль) для доступа к СУБД. В зависимости от способа создания базы данных Сервера предоставьте необходимые права роли, как описано в таблице ниже. Подробнее о настройке прав роли см. раздел Настройка учетных записей для работы с PostgreSQL или Postgres Pro (см. раздел "Настройка учетных записей для работы с PostgreSQL и Postgres Pro" на стр. [222](#)).

Таблица 49. СУБД: PostgreSQL или Postgres Pro

	Автоматическое создание базы данных	Создание базы данных вручную
Учетная запись, от имени которой работает инсталлятор	- Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД. - Локальная СУБД: учетная запись локального администратора или учетная запись домена.	- Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД. - Локальная СУБД: учетная запись локального администратора или учетная запись домена.
Права учетной записи, от имени которой работает инсталлятор	Системные права: права локального администратора.	Системные права: права локального администратора.
Учетная запись службы Сервера администрирования	- Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД. - Локальная СУБД: Учетная запись Windows, выбранная администратором. Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.	- Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД. - Локальная СУБД: Учетная запись Windows, выбранная администратором. Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.
Права учетной записи службы Сервера администрирования	Системные права: необходимые права, присвоенные инсталлятором.	Системные права: необходимые права, присвоенные инсталлятором.
Права роли Postgres	Пользователю <i>Postgres</i> не требуются дополнительные права. Права для новой роли: <code>CREATEDB</code>.	Для новой роли: - Права доступа к базе данных Сервера администрирования: <code>ALL</code>. - Права доступа ко всем таблицам в общедоступной схеме: <code>ALL</code>. - Права доступа ко всем последовательностям в общедоступной схеме: <code>ALL</code>.

Настройка прав на восстановление данных Сервера администрирования

Чтобы восстановить данные Сервера администрирования из резервной копии, запустите утилиту `klbackup` под учетной записью Windows, под которой был установлен Сервер администрирования. Обратите внимание, что роль *Postgres*, используемая для доступа к СУБД, должна иметь права владельца на базу данных Сервера администрирования.

См. также:

Основной сценарий установки.....[56](#)

Настройка учетных записей для работы с SQL Server (аутентификация Windows)

Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с SQL Server.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.
5. В SQL Server создайте учетную запись для учетной записи Windows, используемой для запуска приложения установки Сервера администрирования (далее также "инсталлятор"). Также создайте учетную запись Windows, используемую для запуска службы Сервера администрирования.

Если вы используете SQL Server Management Studio, на странице **Общие** окна свойств входа выберите параметр **Аутентификация Windows**.

Если вы хотите установить Сервер администрирования и SQL Server на устройства, расположенные в разных доменах Windows, обратите внимание, что эти домены должны иметь двусторонние отношения доверия, чтобы обеспечить корректную работу Сервера администрирования, включая выполнение задач и применение политик. Информацию о необходимых учетных записях для работы с различными СУБД и правах учетных записей см. в разделе [Учетные записи для работы с СУБД](#) (на стр. [207](#)).

Настройка учетных записей для установки Сервера администрирования (автоматическое создание базы данных Сервера администрирования)

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. В SQL Server назначьте роль sysadmin на уровне сервера для учетной записи Windows, которая используется для запуска приложения установки.
2. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.
3. Запустите приложение установки Сервера администрирования.
Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
4. Выберите выборочную установку Сервера администрирования (см. раздел "Выборочная установка" на стр. [234](#)).
5. Выберите Microsoft SQL Server как СУБД (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)), в которой хранится база данных Сервера администрирования.

6. Выберите Режим аутентификации Microsoft Windows (см. раздел "Шаг 8. Выбор режима аутентификации" на стр. [239](#)), чтобы установить соединение между Сервером администрирования и SQL Server с помощью учетной записи Windows.
7. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. раздел "Шаг 9. Выбор учетной записи для запуска Сервера администрирования" на стр. [240](#)).

Можно выбрать учетную запись пользователя Windows, для которой вы ранее создали учетную запись SQL Server. Кроме того, вы можете автоматически создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. В этом случае приложение установки автоматически создает для этой учетной записи учетную запись для SQL Server. Независимо от выбора учетной записи приложение установки назначает необходимые системные права и права SQL Server учетной записи службы Сервера администрирования.

После завершения установки создается база данных Сервера и все необходимые системные права и права SQL Server назначаются учетной записи службы Сервера администрирования. Сервер администрирования готов к работе.

Настройка учетных записей для установки Сервера администрирования (создание базы данных Сервера администрирования вручную)

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. На SQL Server создайте пустую базу данных. Эта база данных будет использоваться в качестве базы данных Сервера администрирования (далее также база данных Сервера).
2. Для обеих учетных записей SQL Server, созданных для учетных записей Windows, укажите общедоступную роль уровня сервера и настройте сопоставление с созданной базой данных:
 - Роль уровня сервера: public.
 - Роль членства базы данных: db_owner, public.
 - Схема по умолчанию: dbo.
3. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.
4. Запустите приложение установки Сервера администрирования.
Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
5. Выберите выборочную установку Сервера администрирования (см. раздел "Выборочная установка" на стр. [234](#)).
6. Выберите Microsoft SQL Server как СУБД (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)), в которой хранится база данных Сервера администрирования.
7. Укажите имя созданной базы данных в качестве имени базы данных Сервера администрирования (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. [238](#)).
8. Выберите Режим аутентификации Microsoft Windows (см. раздел "Шаг 8. Выбор режима аутентификации" на стр. [239](#)), чтобы установить соединение между Сервером администрирования и SQL Server с помощью учетной записи Windows.
9. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. раздел "Шаг 9. Выбор учетной записи для запуска Сервера администрирования" на стр. [240](#)).

Вы можете выбрать учетную запись пользователя Windows, для которой вы ранее создали учетную запись входа в SQL Server и настроили права входа.

Не рекомендуется автоматически создавать учетную запись Windows в формате KL-AK-*. В этом случае приложение установки создает учетную запись Windows, для которой вы не создали и не настроили учетную запись SQL Server. Сервер администрирования не может использовать эту учетную запись для запуска службы Сервера администрирования. Если необходимо создать учетную запись KL-AK-* Windows, не запускайте Консоль администрирования после установки. Вместо этого сделайте следующее:

1. Остановите службу kladminserver.
2. В SQL Server создайте учетную запись SQL Server для созданной учетной записи KL-AK-* Windows.
3. Предоставьте права этой учетной записи SQL Server и настройте сопоставление с созданной базой данных:
 - Роль уровня сервера: public.
 - Роль членства базы данных: db_owner, public.
 - Схема по умолчанию: dbo.
4. Перезапустите службу kladminserver, а затем запустите Консоль администрирования.

После завершения установки Сервер администрирования будет использовать созданную базу данных для хранения данных Сервера. Сервер администрирования готов к работе.

Настройка учетных записей для работы с SQL Server (аутентификация SQL Server)

Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с SQL Server.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.
5. В SQL Server включите режим аутентификации SQL Server.

Если вы используете SQL Server Management Studio, в окне свойств SQL Server на странице **Безопасность** выберите параметр **SQL Server и режим аутентификации Windows**.

6. В SQL Server создайте учетную запись с паролем. Приложение установки Сервера администрирования (приложение установки) и служба Сервера администрирования используют эту учетную запись SQL Server для доступа к SQL Server.

Если вы используете SQL Server Management Studio, на странице **Общие** окна свойств входа выберите параметр **Аутентификация SQL-сервера**.

Если вы хотите установить Сервер администрирования и SQL Server на устройства, расположенные в разных доменах Windows, обратите внимание, что эти домены должны иметь двусторонние отношения доверия, чтобы обеспечить корректную работу Сервера администрирования, включая выполнение задач и применение политик. Информацию о необходимых учетных записях для работы с различными СУБД и правах учетных записей см. в разделе Учетные записи для работы с СУБД (на стр. [207](#)).

Настройка учетных записей для установки Сервера администрирования (автоматическое создание базы данных Сервера администрирования)

► Чтобы настроить учетные записи для установки Сервера администрирования:

1. В SQL Server сопоставьте учетную запись SQL Server с учетной записью по умолчанию в базе данных *master*. База данных *master* является шаблоном для базы данных Сервера администрирования (далее также база данных Сервера). База данных *master* используется для сопоставления до тех пор, пока приложение установки не создаст базу данных Сервера. Предоставьте следующие права и разрешения учетной записи SQL Server:
 - Роль уровня сервера: *public*.
 - Роль членства базы данных для *мастер* базы данных: *db_owner*.
 - Схема по умолчанию для базы данных *master*: *dbo*.
 - Разрешения:
 - CONNECT ANY DATABASE
 - CONNECT SQL
 - CREATE ANY DATABASE
 - VIEW ANY DATABASE
2. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.
3. Запустите приложение установки.

Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
4. Выберите выборочную установку Сервера администрирования (см. раздел "Выборочная установка" на стр. [234](#)).
5. Выберите Microsoft SQL Server как СУБД (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)), в которой хранится база данных Сервера администрирования.
6. Укажите имя базы данных Сервера администрирования (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. [238](#)).
7. Выберите режим аутентификации SQL Server (см. раздел "Шаг 8. Выбор режима аутентификации" на стр. [239](#)), чтобы установить соединение между Сервером администрирования и SQL Server с помощью созданной учетной записью SQL Server. Затем укажите данные учетной записи SQL Server.
8. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. раздел "Шаг 9. Выбор учетной записи для запуска Сервера администрирования" на стр. [240](#)).

Вы можете выбрать существующую учетную запись пользователя Windows или создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. Независимо от выбранной учетной записи приложение установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки создается база данных Сервера и все необходимые системные права назначаются учетной записи службы Сервера администрирования. Сервер администрирования готов к работе.

Вы можете отменить привязку к базе данных *master*, так как приложение установки создала базу данных Сервера и настроила сопоставление с этой базой данных при установке Сервера администрирования.

Так как для автоматического создания базы данных требуется больше разрешений, чем для ежедневной работы с Сервером администрирования, вы можете отозвать некоторые разрешения. На SQL Server выберите учетную запись SQL Server и предоставьте следующие права для работы с Сервером администрирования:

- Роль уровня сервера: public.
- Роль членства базы данных для базы данных Сервера: db_owner.
- Схема по умолчанию для базы данных Сервера: dbo.
- Разрешения:
 - CONNECT SQL
 - VIEW ANY DATABASE

Настройка учетных записей для установки Сервера администрирования (создание базы данных Сервера администрирования вручную)

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. На SQL Server создайте пустую базу данных. Эта база данных будет использоваться в качестве базы данных Сервера администрирования.
2. В SQL Server предоставьте следующие права и разрешения учетной записи SQL Server:
 - Роль уровня сервера: public.
 - Роль членства базы данных для создания базы данных: db_owner.
 - Схема по умолчанию для создания базы данных: dbo.
 - Разрешения:
 - CONNECT SQL
 - VIEW ANY DATABASE
3. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.
4. Запустите приложение установки.
Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
5. Выберите выборочную установку Сервера администрирования (см. раздел "Выборочная установка" на стр. [234](#)).
6. Выберите Microsoft SQL Server как СУБД (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)), в которой хранится база данных Сервера администрирования.
7. Укажите имя созданной базы данных в качестве имени базы данных Сервера администрирования (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. [238](#)).
8. Выберите режим аутентификации SQL Server (см. раздел "Шаг 8. Выбор режима аутентификации" на стр. [239](#)), чтобы установить соединение между Сервером администрирования и SQL Server с помощью созданной учетной записью SQL Server. Затем укажите данные учетной записи SQL Server.
9. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. раздел "Шаг 9. Выбор учетной записи для запуска Сервера администрирования" на стр. [240](#)).

Вы можете выбрать существующую учетную запись пользователя Windows или создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. Независимо от выбранной учетной записи приложение установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки Сервер администрирования будет использовать созданную базу данных для хранения данных Сервера администрирования. Все необходимые системные права назначены учетной записи службы Сервера администрирования. Сервер администрирования готов к работе.

Настройка учетных записей для работы с MySQL и MariaDB

Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с MySQL или MariaDB.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.

Настройка учетных записей для установки Сервера администрирования

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. Запустите среду для работы с MySQL или MariaDB под учетной записью root, которую вы создали при установке СУБД.
2. Создайте внутреннюю учетную запись СУБД с паролем. Приложение установки Сервера администрирования (далее также приложение установки) и служба Сервера администрирования используют эту внутреннюю учетную запись СУБД для доступа к СУБД. Предоставьте этой учетной записи следующие права:
 - Схема привилегий:
 - База данных Сервера администрирования: ALL (кроме GRANT OPTION).
 - Схемы системы (mysql и sys): SELECT, SHOW VIEW.
 - Хранимая процедура sys.table_exists: EXECUTE.
 - Глобальные привилегии для всех схем: PROCESS, SUPER.

Чтобы создать внутреннюю учетную запись СУБД и предоставить этой учетной записи необходимые права, запустите приведенный ниже скрипт (в этом скрипте учетная запись СУБД – KSCAdmin, а имя базы данных Сервера администрирования – kav):

```
/* Создать пользователя с именем KSCAdmin */
CREATE USER 'KSCAdmin'

/* Указать пароль для KSCAdmin */
IDENTIFIED BY '<пароль>';

/* Предоставить привилегии KSCAdmin */
GRANT USAGE ON *.* TO 'KSCAdmin';
```



```
GRANT ALL ON kav.* TO 'KSCAdmin';  
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';  
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';  
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';  
GRANT PROCESS ON *.* TO 'KSCAdmin';  
GRANT SUPER ON *.* TO 'KSCAdmin';
```

Если вы используете MariaDB 10.5 или более раннюю версию в качестве СУБД, вам не нужно предоставлять право EXECUTE. В этом случае исключите из скрипта следующую команду:
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'.

3. Чтобы просмотреть список привилегий, предоставленных учетной записи СУБД, запустите следующий скрипт:

```
SHOW grants for 'KSCAdmin';
```

4. Чтобы вручную создать базу данных Сервера администрирования, запустите следующий скрипт (в этом скрипте имя базы данных Сервера администрирования – kav):

```
CREATE DATABASE kav  
DEFAULT CHARACTER SET ascii  
DEFAULT COLLATE ascii_general_ci;
```

Используйте то же имя базы данных, которое вы указали в сценарии, создающем учетную запись СУБД.

5. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.
6. Запустите приложение установки.
Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
7. Выберите выборочную установку Сервера администрирования (см. раздел "Выборочная установка" на стр. [234](#)).
8. Выберите MySQL или MariaDB как СУБД (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)), в которой хранится база данных Сервера администрирования.
9. Укажите имя базы данных Сервера администрирования (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. [238](#)). Используйте то же имя базы данных, которое вы указали в скрипте.
10. Укажите учетные данные учетной записи СУБД (см. раздел "Шаг 8. Выбор режима аутентификации" на стр. [239](#)), которую вы создали с помощью скрипта.
11. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. раздел "Шаг 9. Выбор учетной записи для запуска Сервера администрирования" на стр. [240](#)).

Вы можете выбрать существующую учетную запись пользователя Windows или автоматически создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. Независимо от выбранной учетной записи приложение установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки создается база данных Сервера администрирования и Сервер администрирования готов к работе.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Настройка учетных записей для работы с PostgreSQL и Postgres Pro

Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с PostgreSQL и Postgres Pro.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.

Настройка учетных записей для установки Сервера администрирования (автоматическое создание базы данных Сервера администрирования)

► Чтобы настроить учетные записи для установки Сервера администрирования:

1. Запустите среду для работы с PostgreSQL и Postgres Pro.
2. Выберите роль Postgres для доступа к СУБД. Вы можете использовать одну из следующих ролей:
 - Пользователь *Postgres* (роль *Postgres* по умолчанию).
Если вы используете пользователя *Postgres*, предоставлять ему дополнительные права не требуется.
 - Новая роль *Postgres*.
Если вы хотите использовать новую роль *Postgres*, создайте эту роль и предоставьте ей право **CREATEDB**. Для этого запустите следующий скрипт (в этом скрипте роль имеет значение *KSCAdmin*):

```
CREATE USER "KSCAdmin" WITH PASSWORD '<пароль>' CREATEDB;
```

Созданная роль будет использоваться в качестве владельца базы данных Сервера администрирования (далее также база данных Сервера).
3. Войдите в систему под учетной записью Windows, под которой было запущено приложение установки Сервера администрирования (далее также инсталлятор).
4. Запустите приложение установки.
Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
5. Выберите выборочную установку Сервера администрирования (см. раздел "Выборочная установка" на стр. [234](#)).
6. Выберите PostgreSQL или Postgres Pro как СУБД (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)), в которой хранится база данных Сервера администрирования.
7. Укажите имя базы данных Сервера (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. [238](#)). Приложение установки автоматически создаст базу данных Сервера.

8. Укажите учетные данные роли Postgres (см. раздел "Шаг 8. Выбор режима аутентификации" на стр. [239](#)).
9. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. раздел "Шаг 9. Выбор учетной записи для запуска Сервера администрирования" на стр. [240](#)).

Вы можете выбрать существующую учетную запись пользователя Windows или автоматически создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. Независимо от выбранной учетной записи приложение установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки автоматически создается база данных Сервера, и Сервер администрирования готов к работе.

Настройка учетных записей для установки Сервера администрирования (создание базы данных Сервера администрирования вручную)

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. Запустите среду для работы с Postgres.
2. Создайте роль Postgres и базу данных Сервера администрирования. Затем предоставьте роли все права в базе данных Сервера администрирования. Для этого выполните вход под пользователем *Postgres* в базу данных *Postgres* и запустите следующий скрипт (в этом скрипте роль имеет значение *KSCAdmin*, а имя базы данных Сервера администрирования – *KAV*):

```
CREATE USER "KSCAdmin" WITH PASSWORD '<пароль>';  
CREATE DATABASE "KAV" ENCODING 'UTF8';  
GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
```

3. Предоставьте следующие права созданной роли Postgres:
 - Права доступа ко всем таблицам в общедоступной схеме: ALL.
 - Права доступа ко всем последовательностям в общедоступной схеме: ALL.

Для этого выполните вход под пользователем *Postgres* в базу данных Сервера и запустите следующий скрипт (в этом скрипте роль имеет значение *KSCAdmin*):

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";  
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
```

4. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.
5. Запустите приложение установки Сервера администрирования.
Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
6. Выберите выборочную установку Сервера администрирования (см. раздел "Выборочная установка" на стр. [234](#)).
7. Выберите PostgreSQL или Postgres Pro как СУБД (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)), в которой хранится база данных Сервера администрирования.
8. Укажите имя базы данных Сервера (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. [238](#)). Используйте то же имя базы данных, которое вы указали в скрипте. Учитывайте регистр при вводе имени базы данных.

9. Укажите учетные данные роли Postgres (см. раздел "Шаг 8. Выбор режима аутентификации" на стр. [239](#)).
10. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. раздел "Шаг 9. Выбор учетной записи для запуска Сервера администрирования" на стр. [240](#)).

Вы можете выбрать существующую учетную запись пользователя Windows или автоматически создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. Независимо от выбранной учетной записи приложение установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки Сервер администрирования будет использовать созданную базу данных для хранения данных Сервера администрирования. Сервер администрирования готов к работе.

Сценарий: аутентификация Microsoft SQL Server

Информация в этом разделе применима только к конфигурациям, в которых Kaspersky Security Center использует Microsoft SQL Server в качестве системы управления базами данных.

Чтобы защитить данные Kaspersky Security Center, передаваемые в базу данных или из нее, а также данные, хранящиеся в базе данных, от несанкционированного доступа, вам нужно защитить связь между Kaspersky Security Center и SQL Server. Самый надежный способ обеспечить безопасную связь – это установить Kaspersky Security Center и SQL Server на одном устройстве и использовать механизм совместной памяти для обоих приложений. Во всех других случаях мы рекомендуем использовать сертификат SSL или TLS для аутентификации экземпляра SQL Server. Вы можете использовать сертификат доверенного центра сертификации (CA) или самоподписанный сертификат. Рекомендуется использовать сертификат аккредитованного центра сертификации, так как самоподписанный сертификат обеспечивает лишь ограниченную защиту.

Аутентификация SQL Server состоит из следующих этапов:

- а. **Создание самоподписанного сертификата SSL или TLS для SQL Server в соответствии с требованиями сертификата <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017#certificate-requirements>**

Если у вас уже есть сертификат для SQL Server, пропустите этот шаг.

SSL-сертификат можно применять только к версиям SQL Server ранее 2016 года (13.x). В версиях SQL Server 2016 (13.x) и выше используйте TLS-сертификат.

Например, чтобы создать TLS-сертификат, введите следующую команду в PowerShell:

```
New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation
cert:\LocalMachine -KeySpec KeyExchange
```

В командной строке в качестве SQL_HOST_NAME вам нужно ввести имя экземпляра SQL Server, если экземпляр включен в домен, или ввести *полное доменное имя* (FQDN) экземпляра, если экземпляр не включен в домен. В мастере установки Сервера администрирования (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. 238) в качестве имени экземпляра SQL Server должно быть указано то же имя – имя экземпляра или полное доменное имя.

b. Добавление сертификата на экземпляр SQL Server

Инструкции этого этапа зависят от платформы, на которой работает SQL Server. Дополнительную информацию см. в официальной документации:

- Windows <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017>
- Linux <https://docs.microsoft.com/en-us/sql/linux/sql-server-linux-encrypted-connections?view=sql-server-2017>
- Служба реляционных баз данных Amazon https://docs.aws.amazon.com/en_us/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html
- Windows Azure <https://azure.microsoft.com/en-us/blog/windows-azure-root-certificate-migration/>

Чтобы использовать сертификат в отказоустойчивом кластере, необходимо установить сертификат на каждом узле отказоустойчивого кластера. Подробнее см. документацию Microsoft <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/manage-certificates?view=sql-server-2017>.

c. Назначение разрешений для учетной записи службы

Убедитесь, что учетная запись службы, под которой запускается служба SQL Server, имеет разрешения "Полный доступ" для доступа к закрытым ключам. Подробнее см. документацию Microsoft <https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/startup-shutdown/event-id-33565-start-sql-server>.

d. Добавление сертификата в список доверенных сертификатов для Kaspersky Security Center

На устройство Сервера администрирования добавьте сертификат в список доверенных сертификатов. Подробнее см. документацию Microsoft <https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate>.

e. Включение зашифрованных подключений между экземпляром SQL Server и Kaspersky Security Center

На устройстве Сервера администрирования установите значение 1 для переменной среды `KLDBADO_UseEncryption`. Например, в Windows Server 2012 R2 вы можете изменить переменные среды, нажав на **Переменные среды**, на вкладке **Дополнительно** окна **Свойства системы**. Добавьте переменную с именем `KLDBADO_UseEncryption` и установите значение 1.

f. Дополнительная настройка для использования TLS-протокола 1.2

Если вы используете TLS-протокол 1.2, дополнительно выполните следующие действия:

- Убедитесь, что установленная версия SQL Server является 64-разрядным приложением.
- Установите драйвер Microsoft OLE DB на устройство Сервера администрирования. Подробнее см. документацию Microsoft <https://docs.microsoft.com/en-us/sql/connect/oledb/oledb-driver-for-sql-server?view=sql-server-2017>.
- На устройстве Сервера администрирования установите значение 1 для переменной среды `KLDBADO_UseMSOLEDBSQL`. Например, в Windows Server 2012 R2 вы можете изменить

переменные среды, нажав на **Переменные среды**, на вкладке **Дополнительно** окна **Свойства системы**. Добавьте новую переменную с именем `KLDBADO_UseMSOLEDBSQL` и установите значение `1`.

Если версия драйвера OLE DB – 19 или выше, также установите значение `MSOLEDBSQL19` в переменную окружения `KLDBADO_ProviderName`.

г. Включение использования протокола TCP/IP на именованном экземпляре SQL Server

Если вы используете именованный экземпляр SQL Server, дополнительно включите использование протокола TCP/IP <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-or-disable-a-server-network-protocol?view=sql-server-ver15> и назначьте номер порта TCP/IP <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-server-to-listen-on-a-specific-tcp-port?view=sql-server-ver15> для компонента SQL Server Database Engine. При настройке подключения к SQL Server в мастере установки Сервера администрирования (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. [238](#)) укажите имя экземпляра SQL Server и номер порта в поле **Имя экземпляра SQL Server**.

Рекомендации по установке Сервера администрирования

В этом разделе содержатся рекомендации, касающиеся установки Сервера администрирования. В разделе также содержатся сценарии использования папки общего доступа на устройстве с Сервером администрирования для развертывания Агента администрирования на клиентских устройствах.

См. также:

Сценарий: задание пользовательского сертификата Сервера администрирования [78](#)

В этом разделе

Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере	226
Задание папки общего доступа	227
Удаленная установка средствами Сервера администрирования с помощью групповых политик Active Directory	227
Удаленная установка рассылкой UNC-пути на автономный пакет	228
Обновление из общей папки Сервера администрирования	228
Установка образов операционных систем	228
Указание адреса Сервера администрирования	228

Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере

По умолчанию инсталлятор самостоятельно создает непривилегированные учетные записи для служб Сервера администрирования. Такое поведение наилучшим образом подходит для установки Сервера администрирования на обычное устройство.

Однако при установке Сервера администрирования на отказоустойчивый кластер следует поступить иначе:

1. Создать непривилегированные доменные учетные записи для служб Сервера администрирования и сделать их членами глобальной доменной группы безопасности KLAAdmins.
2. Задать в инсталляторе Сервера администрирования созданные доменные учетные (см. раздел "Шаг 10. Выбор учетной записи для запуска служб Kaspersky Security Center" на стр. [241](#)) записи для служб.

См. также:

Основной сценарий установки.....	56

Задание папки общего доступа

Во время установки Сервера администрирования можно задать месторасположение папки общего доступа. Также месторасположение папки общего доступа можно задать после установки, в свойствах Сервера администрирования. По умолчанию папка общего доступа создается на устройстве с Сервером администрирования (с доступом на чтение для встроенной группы **Everyone**). Однако в некоторых случаях (таких как высокая нагрузка или необходимость доступа из изолированной сети) целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Папка общего доступа используется в нескольких сценариях развертывания Агента администрирования.

Учет регистра для общей папки должен быть выключен.

См. также:

Удаленная установка средствами Сервера администрирования с помощью групповых политик Active Directory.....	227
Удаленная установка рассылкой UNC-пути на автономный пакет	228
Обновление из общей папки Сервера администрирования	228
Установка образов операционных систем.....	846

Удаленная установка средствами Сервера администрирования с помощью групповых политик Active Directory

В случае если устройства находятся в домене Windows (нет рабочих групп), первоначальное развертывание (установку Агента администрирования и программы безопасности на пока еще не управляемые устройства) целесообразно выполнять при помощи групповых политик Active Directory. Развертывание выполняется с помощью штатной задачи удаленной инсталляции Kaspersky Security Center. Если размер сети велик, с целью уменьшения нагрузки на дисковую подсистему устройства с Сервером администрирования целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Удаленная установка рассылкой UNC-пути на автономный пакет

В случае если пользователи устройств сети организации имеют права локального администратора, еще одним способом первоначального развертывания является создание автономного пакета Агента администрирования (или даже "спаренного" пакета Агента администрирования совместно с приложением безопасности). После создания автономного пакета нужно отправить пользователям устройств сети ссылку на пакет, находящийся в папке общего доступа. Инсталляция запускается по ссылке.

Обновление из общей папки Сервера администрирования

В задаче обновления антивируса можно настроить обновление из папки общего доступа Сервера администрирования. Если задача назначена для большого количества устройств, целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Установка образов операционных систем

Установка образов операционных систем всегда выполняется с использованием папки общего доступа: устройства читают из папки образы операционных систем. Если планируется развертывание образов на большом количестве устройств организации, то целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

См. также:

Развертывание Агента администрирования и приложения безопасности[163](#)

Указание адреса Сервера администрирования

При установке Сервера администрирования можно задать адрес Сервера администрирования. Этот адрес по умолчанию используется при создании инсталляционных пакетов Агента администрирования.

В качестве адреса Сервера администрирования вы можете указать:

- NetBIOS-имя Сервера администрирования, указанное по умолчанию.
- Полное доменное имя (FQDN) Сервера администрирования, если система доменных имен (DNS) в сети организации настроена и работает должным образом.
- Внешний адрес, если Сервер администрирования установлен в демилитаризованной зоне (DMZ).

В дальнейшем адрес Сервера администрирования можно будет изменить средствами Консоли администрирования, однако при этом он не изменится автоматически в уже созданных инсталляционных пакетах Агента администрирования.

См. также:

Доступ из интернета: Сервер администрирования в демилитаризованной зоне[145](#)

Стандартная установка

Стандартная установка – это установка Сервера администрирования, при которой используются заданные по умолчанию пути для файлов приложения, устанавливается набор плагинов по умолчанию и не включается Управление мобильными устройствами.

- Чтобы установить Сервер администрирования Kaspersky Security Center на локальное устройство,

запустите исполняемый файл `ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe`.

Откроется окно с выбором приложений "Лаборатории Касперского" для установки. В окне с выбором приложений по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

См. также:

Основной сценарий установки.....[56](#)

В этом разделе

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности	229
Шаг 2. Выбор типа установки.....	230
Шаг 3. Установка Kaspersky Security Center Web Console	230
Шаг 4. Выбор размера сети	230
Шаг 5. Выбор базы данных	231
Шаг 6. Настройка параметров SQL-сервера	232
Шаг 7. Выбор режима аутентификации	233
Шаг 8. Распаковка и установка файлов на жесткий диск	234

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины для управления приложениями.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, подтвердите это, установив соответствующие флажки.

Установка приложения будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку приложения, нажав на кнопку **Отмена**.

Шаг 2. Выбор типа установки

В окне выбора типа установки укажите тип **Стандартная**.

Стандартная установка рекомендуется, если вы хотите ознакомиться с приложением Kaspersky Security Center, например, протестировать ее работу на небольшом участке вашей сети. При стандартной установке вы настраиваете только параметры базы данных. Параметры Сервера администрирования не настраиваются, для них используются заданные по умолчанию значения. Стандартная установка не позволяет выбрать устанавливаемые плагины управления, устанавливается заданный по умолчанию набор плагинов. Во время стандартной установки инсталляционные пакеты для мобильных устройств не создаются. Вы можете создать их позже в Консоли администрирования.

Шаг 3. Установка Kaspersky Security Center Web Console

Этот шаг отображается, только если вы используете 64-разрядную операционную систему. В противном случае этот шаг не отображается, поскольку Kaspersky Security Center Web Console не работает с 32-разрядными операционными системами.

По умолчанию будут установлены и Kaspersky Security Center Web Console, и Консоль администрирования на основе консоли Microsoft Management Console (MMC).

► Если вы хотите установить только Kaspersky Security Center Web Console:

1. Выберите **Установить только одну из консолей**.
2. В раскрывающемся списке выберите **Консоль на основе веб-интерфейса**.

Установка Kaspersky Security Center Web Console запускается автоматически после завершения установки Сервера администрирования.

► Если вы хотите установить только Консоль администрирования на основе консоли Microsoft Management Console (MMC):

1. Выберите **Установить только одну из консолей**.
2. В раскрывающемся списке выберите **Консоль на основе MMC**.

Шаг 4. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса приложения.

В таблице ниже перечислены параметры установки приложения и отображения интерфейса при выборе разных размеров сети.

Таблица 50. Зависимость параметров установки от выбора размеров сети

Параметры	1–100 устройств	101–1000 устройств	1001–5000 устройств	Более 5000 устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами	Отсутствует	Отсутствует	Присутствует	Присутствует
Отображение разделов Безопасность в окнах свойств Сервера и групп администрирования	Отсутствует	Отсутствует	Присутствует	Присутствует
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	Отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL 5.7 и SQL Express не рекомендуется использовать приложение для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

Шаг 5. Выбор базы данных

На этом шаге мастера выберите одну из следующих систем управления базами данных (СУБД), которая будет использоваться для хранения базы данных Сервера администрирования:

- Microsoft SQL Server или SQL Server Express
- MySQL или MariaDB
- PostgreSQL или Postgres Pro

Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

Структура базы данных Сервера администрирования представлена в файле klakdb.chm, который находится в папке установки Kaspersky Security Center. Этот файл также доступен в архиве на портале "Лаборатории Касперского": klakdb.zip (<https://support.kaspersky.com/help/KSC/common/klakdb.zip>).

Шаг 6. Настройка параметров SQL-сервера

На этом шаге мастера укажите следующие параметры подключения в зависимости от выбранной вами системы управления базами данных (СУБД):

- Если вы выбрали **Microsoft SQL Server или SQL Server Express** на предыдущем шаге:
 - В поле **Имя экземпляра SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

Если вы подключаетесь к SQL Server через пользовательский порт, то вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

```
SQL_Server_host_name,1433
```

Если вы защищаете соединение между Сервером администрирования и SQL Server с помощью сертификата (см. раздел "Сценарий: аутентификация Microsoft SQL Server" см. стр. 224), укажите в поле **Имя экземпляра SQL-сервера** то же имя экземпляра, которое использовалось при создании сертификата. Если вы используете именованный экземпляр SQL Server, вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

```
SQL_Server_name,1433
```

Если вы используете несколько экземпляров SQL Server на одном устройстве, дополнительно укажите через обратную косую черту имя экземпляра, например:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

Если для SQL Server в корпоративной сети включена функция Always On, укажите имя прослушивателя группы доступности в поле **Имя экземпляра SQL-сервера**. Обратите внимание, что Сервер администрирования поддерживает только режим доступности с синхронной фиксацией <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/availability-modes-always-on-availability-groups?view=sql-server-2016#SyncCommitAvMode>, когда включена функция Always On.

- В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение KAV.

Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL Server и вернитесь к установке Kaspersky Security Center.

- Если вы выбрали **MySQL** или **MariaDB** на предыдущем шаге:
 - В поле **Имя экземпляра SQL-сервера** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
 - В поле **Порт** укажите порт для подключения Сервера администрирования к базе данных DBMS-сервера. По умолчанию установлен порт 3306.
 - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.
- Если вы выбрали **PostgreSQL** или **Postgres Pro** на предыдущем шаге:
 - В поле **PostgreSQL** или **Postgres Pro Server** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
 - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 5432.
 - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Шаг 7. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к системе управления базами данных (СУБД).

В зависимости от выбранной СУБД вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
 - **Режим аутентификации Microsoft Windows.** В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
 - **Режим аутентификации SQL-сервера.** В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Приложение проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вам нужно указать правильные учетные данные.

Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

- Для MySQL, MariaDB, PostgreSQL или Postgres Pro укажите учетную запись и пароль.

Шаг 8. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные приложения, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые приложения будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую консоль требуется запустить для работы с Kaspersky Security Center:

- **Запустить Консоль на основе MMC**
- **Запустить как Kaspersky Security Center Web Console**

Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Завершить**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования или Kaspersky Security Center Web Console вы можете выполнить первоначальную настройку приложения (см. стр. [281](#)).

По окончании работы мастера установки следующие компоненты приложения будут установлены на жесткий диск, на котором установлена операционная система:

- Сервер администрирования (совместно с серверной версией Агента администрирования);
- Консоль администрирования на основе консоли управления Microsoft Management Console (MMC);
- Kaspersky Security Center Web Console (если выбрана ее установка);
- доступные в дистрибутиве плагины управления приложениями.

Кроме того, будет установлено приложение Microsoft Windows Installer версии 4.5, если это приложение не было установлено ранее.

Выборочная установка

Выборочная установка – это установка Сервера администрирования, при которой вам предлагается выбрать компоненты для установки и указать папку, в которую будет установлено приложение.

С помощью этого типа установки вы можете настроить параметры базы данных, параметры Сервера администрирования, установить компоненты, которые не включены в стандартную установку и плагины управления приложениями безопасности "Лаборатории Касперского". Вы можете также включить Управление мобильными устройствами.

- *Чтобы установить Сервер администрирования Kaspersky Security Center на локальное устройство,*

запустите исполняемый файл `ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe`.

Откроется окно с выбором приложений "Лаборатории Касперского" для установки. В окне с выбором приложений по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

См. также:

Основной сценарий установки.....56

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины для управления приложениями.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, подтвердите это, установив соответствующие флажки.

Установка приложения будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку приложения, нажав на кнопку **Отмена**.

Шаг 2. Выбор типа установки

В окне выбора типа установки укажите тип **Выборочная**.

Выборочная установка позволяет настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления приложениями "Лаборатории Касперского" будут установлены. При выборочной установке вы можете создать инсталляционные пакеты для мобильных устройств, указав соответствующий параметр.

Шаг 3. Выбор компонентов для установки

Выберите компоненты Сервера администрирования Kaspersky Security Center, которые вы хотите установить:

- **Управление мобильными устройствами.** Установите этот флажок, если требуется создать инсталляционные пакеты для мобильных устройств во время работы мастера установки Kaspersky Security Center. Вы можете также создать инсталляционные пакеты для мобильных устройств вручную, после установки Сервера администрирования средствами Консоли администрирования (см. раздел "Создание инсталляционных пакетов приложений" на стр. [850](#)).
- **Агент SNMP.** Получает статистическую информацию для Сервера администрирования по протоколу SNMP. Компонент доступен при установке приложения на устройство с установленным компонентом SNMP.

После установки Kaspersky Security Center необходимые для получения статистической информации mib-файлы будут расположены в папке установки приложения во вложенной папке SNMP.

Компоненты Агент администрирования и Консоль администрирования не отображаются в списке компонентов. Эти компоненты устанавливаются автоматически, их установку отменить невозможно.

На этом шаге мастера также следует указать папку для установки компонентов Сервера администрирования. По умолчанию компоненты устанавливаются в папку <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Если папки с таким названием нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

Шаг 3. Установка Kaspersky Security Center Web Console

Этот шаг отображается, только если вы используете 64-разрядную операционную систему. В противном случае этот шаг не отображается, поскольку Kaspersky Security Center Web Console не работает с 32-разрядными операционными системами.

Если требуется установить Kaspersky Security Center Web Console, установите флажок **Установить Kaspersky Security Center Web Console**. Если этот флажок не установлен, приложение Kaspersky Security Center Web Console не будет установлено. Будет установлена только Консоль администрирования на основе консоли управления Microsoft Management Console (MMC). Если вы используете 64-разрядную операционную систему, вы можете установить Kaspersky Security Center Web Console позже, после начала работы с Kaspersky Security Center.

Шаг 5. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса приложения.

В таблице ниже перечислены параметры установки приложения и отображения интерфейса при выборе разных размеров сети.

Таблица 51. Зависимость параметров установки от выбора размеров сети

Параметры	1–100 устройств	101–1000 устройств	1001–5000 устройств	Более 5000 устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами	Отсутствует	Отсутствует	Присутствует	Присутствует
Отображение разделов Безопасность в окнах свойств Сервера и групп администрирования	Отсутствует	Отсутствует	Присутствует	Присутствует
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	Отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL 5.7 и SQL Express не рекомендуется использовать приложение для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

Шаг 6. Выбор базы данных

На этом шаге мастера выберите одну из следующих систем управления базами данных (СУБД), которая будет использоваться для хранения базы данных Сервера администрирования:

- Microsoft SQL Server или SQL Server Express
- MySQL или MariaDB
- PostgreSQL или Postgres Pro

Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

Структура базы данных Сервера администрирования представлена в файле klakdb.chm, который находится в папке установки Kaspersky Security Center. Этот файл также доступен в архиве на портале "Лаборатории Касперского": klakdb.zip (<https://support.kaspersky.com/help/KSC/common/klakdb.zip>).

Шаг 7. Настройка параметров SQL-сервера

На этом шаге мастера укажите следующие параметры подключения в зависимости от выбранной вами системы управления базами данных (СУБД):

- Если вы выбрали **Microsoft SQL Server или SQL Server Express** на предыдущем шаге:
 - В поле **Имя экземпляра SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

Если вы подключаетесь к SQL Server через пользовательский порт, то вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

```
SQL_Server_host_name,1433
```

Если вы защищаете соединение между Сервером администрирования и SQL Server с помощью сертификата (см. раздел "Сценарий: аутентификация Microsoft SQL Server" см. стр. [224](#)), укажите в поле **Имя экземпляра SQL-сервера** то же имя экземпляра, которое использовалось при создании сертификата. Если вы используете именованный экземпляр SQL Server, вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

```
SQL_Server_name,1433
```

Если вы используете несколько экземпляров SQL Server на одном устройстве, дополнительно укажите через обратную косую черту имя экземпляра, например:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

Если для SQL Server в корпоративной сети включена функция Always On, укажите имя прослушивателя группы доступности в поле **Имя экземпляра SQL-сервера**. Обратите внимание, что Сервер администрирования поддерживает только режим доступности с синхронной фиксацией <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/availability-modes-always-on-availability-groups?view=sql-server-2016#SyncCommitAvMode>, когда включена функция Always On.

- В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение KAV.

Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL Server и вернитесь к установке Kaspersky Security Center.

- Если вы выбрали **MySQL или MariaDB** на предыдущем шаге:
 - В поле **Имя экземпляра SQL-сервера** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
 - В поле **Порт** укажите порт для подключения Сервера администрирования к базе данных DBMS-сервера. По умолчанию установлен порт 3306.
 - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.
- Если вы выбрали **PostgreSQL или Postgres Pro** на предыдущем шаге:
 - В поле **PostgreSQL или Postgres Pro Server** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
 - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 5432.
 - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

См. также:

Основной сценарий установки.....[56](#)

Шаг 8. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к системе управления базами данных (СУБД).

В зависимости от выбранной СУБД вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
 - **Режим аутентификации Microsoft Windows.** В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
 - **Режим аутентификации SQL-сервера.** В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Приложение проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вам нужно указать правильные учетные данные.

Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

- Для MySQL, MariaDB, PostgreSQL или Postgres Pro укажите учетную запись и пароль.

Шаг 9. Выбор учетной записи для запуска Сервера администрирования

Выберите учетную запись, под которой Сервер администрирования будет запускаться как служба.

- **Создать учетную запись автоматически.** Приложение создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования kladminserver.

Вы можете выбрать этот вариант, если вы планируете разместить папку общего доступа (см. раздел "Шаг 11. Определение папки общего доступа" на стр. [242](#)) и СУБД (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)) на том же устройстве, что и Сервер администрирования.

- **Выбрать учетную запись.** Служба Сервера администрирования (kladminserver) будет запускаться под выбранной вами учетной записью.

Вам потребуется выбрать доменную учетную запись, например, если вы планируете использовать в качестве СУБД SQL-сервер любого выпуска, в том числе SQL-express (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)), расположенный на другом устройстве, и/или если вы планируете разместить папку общего доступа (см. раздел "Шаг 11. Определение папки общего доступа" на стр. [242](#)) на другом устройстве.

Kaspersky Security Center поддерживает управляемые учетные записи службы (MSA) и групповые управляемые учетные записи службы (gMSA). Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования.

Прежде чем выбрать MSA или gMSA, необходимо установить учетную запись на том же устройстве, на котором вы хотите установить Сервер администрирования. Если учетная запись еще не установлена, отмените установку Сервера администрирования, установите учетную запись и перезапустите установку Сервера администрирования. Подробнее об установке управляемых учетных записей служб на локальном устройстве см. в официальной документации Microsoft.

Чтобы указать MSA или gMSA:

1. Нажмите на кнопку **Обзор**.
2. В появившемся окне нажмите на кнопку **Тип объекта**.
3. Выберите тип **Учетная запись для служб** и нажмите на кнопку **ОК**.
4. Выберите нужную учетную запись и нажмите на кнопку **ОК**.

Выбранная вами учетная запись должна обладать различными правами в зависимости от того, какую СУБД вы планируете использовать (см. раздел "Учетные записи для работы с СУБД" на стр. [207](#)).

Из соображений безопасности не делайте учетную запись, под которой запускается Сервер администрирования, привилегированной.

Если в дальнейшем вы захотите изменить учетную запись Сервера администрирования, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования (klsrvswch) (см. раздел "Смена учетной записи службы Сервера администрирования. Утилита klsrvswch" на стр. [712](#)). Обратите внимание, что вам нужно запустить утилиту klsrvswch на устройстве Сервера администрирования под учетной записью с правами администратора, которая использовалась для установки Сервера администрирования.

См. также:

Учетные записи для работы с СУБД	207
Изменения в системе после установки Kaspersky Security Center	271
Основной сценарий установки.....	56

Шаг 10. Выбор учетной записи для запуска служб Kaspersky Security Center

Выберите учетную запись, под которой будут запускаться службы Kaspersky Security Center на этом устройстве:

- **Создать учетную запись автоматически.** Kaspersky Security Center создает локальную учетную запись KIScSvc на этом устройстве в группе kladmins. Службы Kaspersky Security Center будут запускаться под созданной учетной записью.
- **Выбрать учетную запись.** Службы Kaspersky Security Center будут запускаться под выбранной вами учетной записью.

Вам потребуется выбрать доменную учетную запись, например, если вы планируете сохранять отчеты в папке, расположенной на другом устройстве, или же если этого требует политика безопасности в вашей организации. Также вам может потребоваться выбрать доменную учетную запись при установке Сервера администрирования на отказоустойчивый кластер (см. раздел "Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере" на стр. [226](#)).

Из соображений безопасности не делайте учетную запись, под которой запускаются службы, привилегированной.

Под выбранной учетной записью будут запускаться службы прокси-сервера KSN (ksnproxy), прокси-сервера активации "Лаборатории Касперского" (klactprx) и портала авторизации "Лаборатории Касперского" (klwebsrv).

См. также:

Изменения в системе после установки Kaspersky Security Center	271
Основной сценарий установки.....	56

Шаг 11. Определение папки общего доступа

Определите место размещения и название папки общего доступа, которая будет использоваться для следующих целей:

- хранения файлов, необходимых для удаленной установки приложений (файлы копируются на Сервер администрирования при создании инсталляционных пакетов);
- размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

К этому ресурсу будет открыт общий доступ на чтение для всех пользователей.

Вы можете выбрать один из двух вариантов:

- **Создать папку общего доступа.** Создание новой папки. Укажите путь к папке в расположенном ниже поле.
- **Выбрать существующую папку общего доступа.** Выбор папки общего доступа из числа уже существующих.

Папка общего доступа может размещаться как локально на устройстве, с которого производится установка, так и удаленно, на любом из клиентских устройств, входящих в состав сети организации. Вы можете указать папку общего доступа с помощью кнопки **Обзор** или вручную, введя в соответствующем поле UNC-путь (например, \\server\Share).

По умолчанию создается локальная папка Share в папке, заданной для установки компонентов Kaspersky Security Center.

Вы можете определить общую папку (см. раздел "Задание папки общего доступа" на стр. [227](#)) позже, если нужно.

Шаг 12. Настройка параметров подключения к Серверу администрирования

Настройте параметры подключения к Серверу администрирования:

- **Порт**
Номер порта, по которому выполняется подключение к Серверу администрирования.
По умолчанию используется порт 14000.
- **Номер SSL-порта**
Номер SSL-порта, по которому осуществляется защищенное подключение к Серверу администрирования с использованием протокола SSL.
По умолчанию используется порт 13000.

- **Длина ключа шифрования**

Выберите длину ключа шифрования 1024 бита или 2048 бит.

Ключ шифрования длиной 1024 бита оказывает меньшую нагрузку на процессор, но считается устаревшим и по техническим характеристикам может не обеспечивать надежное шифрование. Также есть вероятность, что имеющееся оборудование несовместимо с SSL-сертификатами с длиной ключа 1024 бита.

Ключ шифрования длиной 2048 бит отвечает современным стандартам шифрования. Однако использование 2048-битного ключа шифрования может привести к дополнительной нагрузке на процессор.

По умолчанию вариант выбран вариант **2048 бит (большая безопасность)**.

Также можно изменить параметры подключения к Серверу администрирования позже:

- Вы можете изменить порт и номера SSL-портов в разделе **Порты подключения** в свойствах Сервера администрирования. Дополнительную информацию о портах для подключения к Серверу администрирования см. в разделе Порты, используемые Kaspersky Security Center (см. стр. [63](#)).
- Вы можете изменить длину ключа шифрования при замене сертификата Сервера администрирования (см. раздел "Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert" на стр. [81](#)) утилитой klsetsrvcert с помощью параметра `-o RsaKeyLen:<длина ключа>`.

См. также:

Порты, используемые Kaspersky Security Center	63
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104

Шаг 13. Задание адреса Сервера администрирования

Укажите адрес Сервера администрирования одним из следующих способов:

- **Имя DNS-домена.** Этот способ используется в том случае, когда в сети присутствует DNS-сервер, и клиентские устройства могут получить с его помощью адрес Сервера администрирования.
- **NetBIOS-имя.** Этот способ используется, если клиентские устройства получают адрес Сервера администрирования с помощью протокола NetBIOS, или в сети присутствует WINS-сервер.
- **IP-адрес.** Этот способ используется, если Сервер администрирования имеет статический IP-адрес, который в дальнейшем не будет изменяться.

Если вы устанавливаете Kaspersky Security Center на активный узел отказоустойчивого кластера Kaspersky Security Center и создали виртуальный сетевой адаптер, во время подготовки узлов кластера (см. раздел "Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center" на стр. [249](#)) укажите IP-адрес этого адаптера. В противном случае введите IP-адрес стороннего балансировщика нагрузки, который вы используете.

Шаг 14. Адрес Сервера для подключения мобильных устройств

Этот шаг мастера установки доступен, если вы выбрали для установки компонент Управление мобильными устройствами.

В окне **Адрес для подключения мобильных устройств** укажите внешний адрес Сервера администрирования для подключения мобильных устройств, которые находятся за пределами локальной сети. Вы можете указать IP-адрес или DNS (Domain Name System) Сервера администрирования.

Шаг 15. Выбор плагинов управления приложениями

Выберите плагины управления приложениями "Лаборатории Касперского", которые требуется установить совместно с Kaspersky Security Center.

Для удобства поиска плагины разделены на группы в зависимости от типа защищаемых объектов.

Шаг 16. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные приложения, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые приложения будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую консоль требуется запустить для работы с Kaspersky Security Center:

- **Запустить Консоль на основе MMC**
- **Запустить как Kaspersky Security Center Web Console**

Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Завершить**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования или Kaspersky Security Center Web Console вы можете выполнить первоначальную настройку приложения (см. стр. [281](#)).

Развертывание отказоустойчивого кластера Kaspersky Security Center

Этот раздел содержит общую информацию об отказоустойчивом кластере Kaspersky Security Center, а также инструкции по подготовке и развертыванию отказоустойчивого кластера Kaspersky Security Center в вашей сети.

См. также:

Установка Сервера администрирования на отказоустойчивом кластере Windows Server.....	254
Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center	277

Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center

Отказоустойчивый кластер Kaspersky Security Center обеспечивает высокую доступность Kaspersky Security Center и минимизирует простои Сервера администрирования в случае сбоя. Отказоустойчивый кластер основан на двух идентичных экземплярах Kaspersky Security Center, установленных на двух компьютерах. Один из экземпляров работает как активный узел, а другой – как пассивный. Активный узел управляет защитой клиентских устройств, в то время как пассивный готов взять на себя все функции активного узла в случае отказа активного узла. Когда происходит сбой, пассивный узел становится активным, а активный узел становится пассивным.

Предварительные требования

У вас есть оборудование, соответствующее требованиям (см. раздел "Об отказоустойчивом кластере Kaspersky Security Center" см. стр. [246](#)) для отказоустойчивого кластера.

Этапы

Развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

а. Создание учетной записи для служб Kaspersky Security Center

Создайте доменную группу (в этом сценарии для группы используется имя "KLAdmins") и предоставьте права локального администратора группе на обоих узлах и на файловом сервере. Затем создайте две учетные записи пользователей домена (в этом сценарии для этих учетных записей используются имена "ksc" и "rightless") и добавьте учетные записи в доменную группу KLAdmins.

Добавьте учетную запись пользователя, под которой будет установлен Kaspersky Security Center, в ранее созданную доменную группу KLAdmins.

б. Подготовка файлового сервера

Подготовьте файловый сервер к работе в составе отказоустойчивого кластера Kaspersky Security Center. Убедитесь, что файловый сервер соответствует аппаратным и программным требованиям, создайте две общие папки для данных Kaspersky Security Center и настройте права доступа к общим папкам.

Инструкции: Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center (см. стр. [249](#)).

с. Подготовка активного и пассивного узлов

Подготовьте два компьютера с идентичным аппаратным и программным обеспечением для работы в качестве активного и пассивного узлов.

Инструкции: Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center (см. стр. [249](#)).

д. Установка системы управления базами данных (СУБД)

Выберите любую из поддерживаемых СУБД (см. раздел "Аппаратные и программные требования" см. стр. [29](#)) и установите СУБД на выделенный компьютер. Сведения о том, как установить СУБД, см. в документации к ней.

e. Установка Kaspersky Security Center

Установите Kaspersky Security Center в режиме отказоустойчивого кластера на оба узла. Сначала необходимо установить Kaspersky Security Center на активный узел, а затем установить его на пассивный.

Также вы можете установить Kaspersky Security Center Web Console на отдельном устройстве, не являющемся узлом кластера.

Инструкции: Установка Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center (на стр. [251](#)).

f. Тестирование отказоустойчивого кластера

Убедитесь, что вы правильно настроили отказоустойчивый кластер и правильно ли он работает. Например, вы можете остановить одну из служб Kaspersky Security Center на активном узле: kladminserver, klhagent, ksnproxy, klactprх или klwebsrv. После остановки службы управление защитой должно быть автоматически переключено на пассивный узел.

Результаты

Отказоустойчивый кластер Kaspersky Security Center развернут. Пожалуйста, ознакомьтесь с событиями, которые приводят к переключению между активными и пассивными узлами (см. раздел "Об отказоустойчивом кластере Kaspersky Security Center" см. стр. [246](#)).

См. также:

Установка Сервера администрирования на отказоустойчивом кластере Windows Server	254
Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center	277

Об отказоустойчивом кластере Kaspersky Security Center

Отказоустойчивый кластер Kaspersky Security Center обеспечивает высокую доступность Kaspersky Security Center и минимизирует простои Сервера администрирования в случае сбоя. Отказоустойчивый кластер основан на двух идентичных экземплярах Kaspersky Security Center, установленных на двух компьютерах. Один из экземпляров работает как активный узел, а другой – как пассивный. Активный узел управляет защитой клиентских устройств, в то время как пассивный готов взять на себя все функции активного узла в случае отказа активного узла. Когда происходит сбой, пассивный узел становится активным, а активный узел становится пассивным.

Аппаратные и программные требования

Для развертывания отказоустойчивого кластера Kaspersky Security Center у вас должно быть следующее оборудование:

- Два компьютера с одинаковым оборудованием и программным обеспечением. Эти компьютеры будут действовать как активный и пассивный узлы.
- Файловый сервер, поддерживающий протокол CIFS/SMB версии 2.0 или выше. Вам нужно предоставить выделенный компьютер, который будет выступать в качестве файлового сервера.

Убедитесь, что вы обеспечили высокую пропускную способность сети между файловым сервером, активным и пассивным узлами.

- Компьютер с системой управления базами данных (СУБД).

Схемы развертывания

Вы можете выбрать одну из следующих схем развертывания отказоустойчивого кластера Kaspersky Security Center:

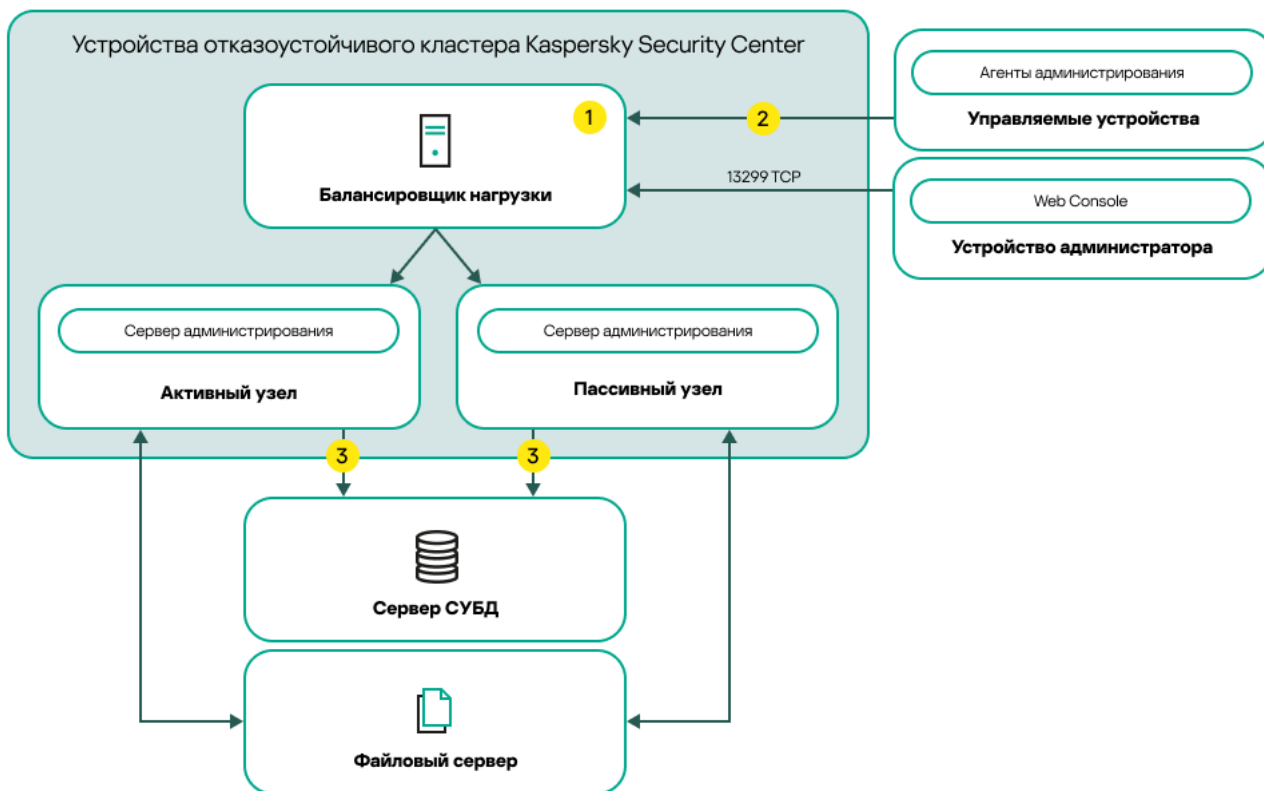
- Схема, в которой используется дополнительный сетевой адаптер.
- Схема, в которой используется сторонняя балансировка нагрузки.



Условные обозначения схемы:

- 1** Сервер администрирования передает данные в базу данных. Откройте необходимые порты на устройстве, на котором расположена база данных, например порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server. Подробную информацию см. в документации СУБД.

- 2** На управляемых устройствах откройте следующие порты: TCP 13000, UDP 13000 и TCP 17000.



Условные обозначения схемы:

- 1** На сервере устройства балансировки нагрузки откройте все порты Сервера администрирования: TCP 13000, UDP 13000, TCP 13291, TCP 13299 и TCP 17000.
- 2** На управляемых устройствах откройте следующие порты: TCP 13000, UDP 13000 и TCP 17000.
- 3** Сервер администрирования передает данные в базу данных. Откройте необходимые порты на устройстве, на котором расположена база данных, например порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server. Подробную информацию см. в документации СУБД.

Условия переключения

Отказоустойчивый кластер переключает управление защитой клиентских устройств с активного узла на пассивный, если на активном узле происходит любое из следующих событий:

- Активный узел сломан из-за программного или аппаратного сбоя.
- Активный узел был временно остановлен для проведения технических работ (см. раздел "Запуск и остановка узла кластера вручную" см. стр. [252](#)).
- По крайней мере, одна из служб (или процессов) Kaspersky Security Center завершилась с ошибкой или была намеренно остановлена пользователем. К службам Kaspersky Security Center относятся: kladminserver, klnagent, klactprx и klwebsrv.
- Сетевое соединение между активным узлом и хранилищем на файловом сервере было прервано или разорвано.

См. также:

Установка Сервера администрирования на отказоустойчивом кластере Windows Server.....	254
Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center	277

Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center

Файловый сервер работает как обязательный компонент отказоустойчивого кластера Kaspersky Security Center (см. раздел "Об отказоустойчивом кластере Kaspersky Security Center" см. стр. [246](#)).

► Чтобы подготовить файловый сервер:

1. Убедитесь, что файловый сервер соответствует аппаратным и программным требованиям (см. раздел "Об отказоустойчивом кластере Kaspersky Security Center" см. стр. [246](#)).
2. Убедитесь, что либо файловый сервер и оба узла (активный и пассивный) включены в один домен, либо файловый сервер является контроллером домена.
3. На файловом сервере создайте две общие папки. Один из них используется для хранения информации о состоянии отказоустойчивого кластера. Другая используется для хранения данных и параметров Kaspersky Security Center. Вам нужно будет указать пути к общим папкам при установке Kaspersky Security Center (см. раздел "Установка Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center" на стр. [251](#)).
4. Предоставьте права полного доступа (как права общего доступа, так и NTFS-разрешения) к созданным общим папкам для следующих учетных записей пользователей и групп:
 - Доменная группа KLAAdmins.
 - Учетные записи пользователей \$<node1> и \$<node2>. Здесь <node1> и <node2> – это имена компьютеров активного и пассивного узлов.

Файловый сервер подготовлен. Чтобы развернуть отказоустойчивый кластер Kaspersky Security Center, следуйте инструкциям этого сценария (см. раздел "Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center" см. стр. [245](#)).

См. также:

Об отказоустойчивом кластере Kaspersky Security Center	246
Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center	245

Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center

Подготовьте два компьютера к работе в качестве активного и пассивного узла для отказоустойчивого кластера Kaspersky Security Center (см. раздел "Об отказоустойчивом кластере Kaspersky Security Center" см. стр. [246](#)).

► Чтобы подготовить узлы для отказоустойчивого кластера Kaspersky Security Center:

1. Убедитесь, что у вас есть два компьютера, соответствующих аппаратным и программным требованиям (см. раздел "Об отказоустойчивом кластере Kaspersky Security Center" см. стр. [246](#)). Эти компьютеры будут действовать как активные и пассивные узлы отказоустойчивого кластера.
2. Убедитесь, что файловый сервер и оба узла включены в один домен.
3. Выполните одно из следующих действий:

- На каждом из узлов настройте дополнительный сетевой адаптер.

Дополнительный сетевой адаптер может быть физическим или виртуальным. Если вы хотите использовать физический сетевой адаптер, подключите и настройте его с помощью стандартных инструментов операционной системы. Если вы хотите использовать виртуальный сетевой адаптер, создайте его с помощью приложений сторонних производителей.

Убедитесь, что выполняются следующие условия:

- Дополнительные сетевые адаптеры выключены.
Вы можете создать дополнительные сетевые адаптеры в отключенном состоянии или отключить их после создания.
- Дополнительные сетевые адаптеры на обоих узлах должны иметь одинаковый IP-адрес.
- Используйте сторонний балансировщик нагрузки. Например, вы можете использовать сервер nginx. В этом случае сделайте следующее:
 - a. Предоставьте выделенный компьютер с операционной системой Linux с установленным nginx.
 - b. Настройте балансировку нагрузки. Установите активный узел в качестве основного сервера и пассивный узел в качестве резервного сервера.
 - c. На сервере nginx откройте все порты Сервера администрирования: TCP 13000, UDP 13000, TCP 13291, TCP 13299 и TCP 17000.

4. Перезагрузите оба узла и файловый сервер.
5. Сопоставьте две общие папки, которые вы создали во время этапа подготовки файлового сервера (см. раздел "Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center" см. стр. [249](#)), к каждому из узлов. Вам нужно сопоставить общие папки как сетевые диски. При сопоставлении папок вы можете выбрать любые свободные буквы дисков. Для доступа к общим папкам используйте учетные данные учетной записи пользователя, которую вы создали на шаге 1 сценария (см. раздел "Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center" см. стр. [245](#)).

Узлы подготовлены. Чтобы развернуть отказоустойчивый кластер Kaspersky Security Center, следуйте инструкциям сценария (см. раздел "Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center" см. стр. [245](#)).

См. также:

Об отказоустойчивом кластере Kaspersky Security Center	246
Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center	245

Установка Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center

Kaspersky Security Center устанавливается на оба узла отказоустойчивого кластера Kaspersky Security Center по отдельности. Сначала вы устанавливаете приложение на активный узел, затем на пассивный. Во время установки вы выбираете, какой узел будет активным, а какой пассивным.

Только пользователь из доменной группы KLAAdmins может установить Kaspersky Security Center на каждый узел.

► Чтобы установить Kaspersky Security Center на активный узел отказоустойчивого кластера Kaspersky Security Center:

1. Запустите исполняемый файл ksc_15.1_<номер сборки>_full_<язык локализации>.exe.
Откроется окно с выбором приложений "Лаборатории Касперского" для установки. В окне с выбором приложений по ссылке **Установка Сервера администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
2. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:
 - **Условия и положения настоящего Лицензионного соглашения**
 - **Политику конфиденциальности, которая описывает обработку данных**Установка приложения будет продолжена после установки обоих флажков.
Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку приложения, нажав на кнопку **Отмена**.
3. Выберите **Первичный узел отказоустойчивого кластера Kaspersky Security Center**, чтобы установить приложение на активный узел.
4. В окне **Общая папка** выполните следующее:
 - В полях **Общая папка состояний** и **Общая папка данных** укажите пути к общим папкам, которые вы создали на файловом сервере во время его подготовки (см. раздел "Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center" на стр. [249](#)).
 - В полях **Общая папка состояний диска** и **Общая папка данных диска** выберите сетевые диски, к которым вы подключили общие папки во время подготовки узлов (см. раздел "Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center" на стр. [249](#)).
 - Выберите режим подключения кластера: через дополнительный сетевой адаптер или сторонний балансировщик нагрузки.
5. Выполните другие шаги выборочной установки, начиная с шага 3 (см. раздел "Шаг 3. Выбор компонентов для установки" на стр. [235](#)).

На шаге 13 (см. раздел "Шаг 13. Задание адреса Сервера администрирования" на стр. 243) укажите IP-адрес дополнительного сетевого адаптера, если вы создали адаптер, во время подготовки узлов кластера (см. раздел "Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center" на стр. 249). В противном случае введите IP-адрес стороннего балансировщика нагрузки, который вы используете.

Приложение Kaspersky Security Center установлено на активном узле.

► Чтобы установить Kaspersky Security Center на пассивный узел отказоустойчивого кластера Kaspersky Security Center:

1. Запустите исполняемый файл ksc_15.1_<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором приложений "Лаборатории Касперского" для установки. В окне с выбором приложений по ссылке **Установка Сервера администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

2. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

- **Условия и положения настоящего Лицензионного соглашения**
- **Политику конфиденциальности, которая описывает обработку данных**

Установка приложения будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку приложения, нажав на кнопку **Отмена**.

3. Выберите **Вторичный узел отказоустойчивого кластера Kaspersky Security Center**, чтобы установить приложение на пассивный узел.
4. В окне **Общая папка** в поле **Общая папка состояний** укажите путь к общей папке с информацией о состоянии кластера, который вы создали на файловом сервере во время его подготовки (см. раздел "Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center" на стр. 249).
5. Нажмите на кнопку **Установить**. После завершения установки нажмите на кнопку **Готово**.

Приложение Kaspersky Security Center установлено на пассивный узел. Теперь вы можете протестировать отказоустойчивый кластер Kaspersky Security Center, чтобы убедиться, что вы корректно его настроили и кластер работает правильно.

См. также:

Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center [277](#)

Запуск и остановка узла кластера вручную

Вам может потребоваться остановить весь отказоустойчивый кластер Kaspersky Security Center или временно отключить один из узлов кластера для обслуживания. В этом случае следуйте инструкциям этого

раздела. Не пытайтесь запускать или останавливать службы или процессы, связанные с отказоустойчивым кластером, с помощью других средств. Это может привести к потере данных.

Запуск и остановка всего отказоустойчивого кластера для обслуживания

► Чтобы запустить или остановить весь отказоустойчивый кластер:

1. На активном узле перейдите в папку <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Откройте командную строку и выполните одну из следующих команд:
 - Чтобы остановить кластер, выполните: `klfoc -stopcluster --stp klfoc`
 - Чтобы запустить кластер, выполните: `klfoc -startcluster --stp klfoc`

Отказоустойчивый кластер запускается или останавливается в зависимости от команды.

Обслуживание одного из узлов

► Для обслуживания одного из узлов:

1. На активном узле остановите отказоустойчивый кластер с помощью команды `klfoc -stopcluster --stp klfoc`.
2. На узле, который вы хотите обслуживать, перейдите в папку <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Откройте командную строку и отключите узел от кластера, выполнив команду `detach_node.cmd`.
4. На активном узле запустите отказоустойчивый кластер с помощью команды `klfoc -startcluster --stp klfoc`.
5. Выполните работы по техническому обслуживанию.
6. На активном узле остановите отказоустойчивый кластер с помощью команды `klfoc -stopcluster --stp klfoc`.
7. На обслуживаемом узле перейдите в папку <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
8. Откройте командную строку и подключите узел к кластеру, выполнив команду `attach_node.cmd`.
9. На активном узле запустите отказоустойчивый кластер с помощью команды `klfoc -startcluster --stp klfoc`.

Узел обслуживается и подключается к отказоустойчивому кластеру.

См. также:

Об отказоустойчивом кластере Kaspersky Security Center	246
Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center	245

Установка Сервера администрирования на отказоустойчивом кластере Windows Server

Процедура установки Сервера администрирования на отказоустойчивом кластере отличается как от стандартной, так и от выборочной установки на автономном устройстве.

Выполните процедуру, описанную в этом разделе, на узле, который содержит общее хранилище данных кластера.

- Чтобы установить Сервер администрирования Kaspersky Security Center на кластер, запустите исполняемый файл `ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe`.

Откроется окно с выбором приложений "Лаборатории Касперского" для установки. В окне с выбором приложений по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

В этом разделе

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности	254
Шаг 2. Выбор типа установки на кластер	255
Шаг 3. Указание имени виртуального Сервера администрирования.....	256
Шаг 4. Указание параметров сети виртуального Сервера администрирования	256
Шаг 5. Указание группы кластеров.....	256
Шаг 6. Выбор кластерного хранилища данных	256
Шаг 7. Указание учетной записи для удаленной установки.....	257
Шаг 8. Выбор компонентов для установки	257
Шаг 9. Выбор размера сети	257
Шаг 10. Выбор базы данных	258
Шаг 11. Настройка параметров SQL-сервера	259
Шаг 12. Выбор режима аутентификации	260
Шаг 13. Выбор учетной записи для запуска Сервера администрирования	260
Шаг 14. Выбор учетной записи для запуска служб Kaspersky Security Center	261
Шаг 15. Определение папки общего доступа.....	262
Шаг 16. Настройка параметров подключения к Серверу администрирования	263
Шаг 17. Задание адреса Сервера администрирования	263
Шаг 18. Адрес Сервера для подключения мобильных устройств	264
Шаг 19. Распаковка и установка файлов на жесткий диск	264

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины для управления приложениями.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, подтвердите это, установив соответствующие флажки.

Установка приложения будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку приложения, нажав на кнопку **Отмена**.

Шаг 2. Выбор типа установки на кластер

Выберите тип установки на кластере:

- **Кластер (установить на всех узлах кластера)**

Рекомендуется выбрать этот параметр. Если вы выберете этот параметр, Сервер администрирования будет установлен на всех узлах кластера одновременно.

На шаге выбора Консоли администрирования для установки (см. раздел "Шаг 3. Установка Kaspersky Security Center Web Console" на стр. [230](#)) требуется выбрать Консоль, которая будет установлена на текущем узле кластера. Если вы устанавливаете Консоль только на узле кластера, в случае сбоя узла вы потеряете доступ к Серверу администрирования. Рекомендуется на этом шаге (см. раздел "Шаг 3. Установка Kaspersky Security Center Web Console" на стр. [230](#)) выбрать Консоль администрирования на основе консоли Microsoft Management Console (MMC) для установки на все узлы кластера. После установки Сервера администрирования установите Kaspersky Security Center Web Console на отдельном устройстве, не являющемся узлом кластера. Это позволяет управлять Сервером администрирования с помощью Kaspersky Security Center Web Console в случае сбоя узла кластера.

- **Локально (установить только на это устройство)**

Если вы выберете этот параметр, Сервер администрирования будет установлен только на текущем узле, как на автономном сервере, и Сервер администрирования не будет работать как кластерное приложение. Например, вы можете выбрать этот параметр для экономии свободного пространства в общем хранилище, если отказоустойчивость не требуется для Сервера администрирования. В случае выхода из строя текущего узла вам придется установить Сервер администрирования на другой узел и восстановить состояние Сервера администрирования из резервной копии данных.

Дальнейшие действия такие же, как при использовании стандартного (см. раздел "Стандартная установка" на стр. [229](#)) или выборочного (см. раздел "Выборочная установка" на стр. [234](#)) способа установки, начиная с шага выбора способа установки.

Шаг 3. Указание имени виртуального Сервера администрирования

Укажите сетевое имя нового виртуального Сервера администрирования. Вы сможете использовать это имя для подключения Консоли администрирования или Kaspersky Security Center Web Console к Серверу администрирования.

Указанное имя должно отличаться от имени кластера.

Шаг 4. Указание параметров сети виртуального Сервера администрирования

► *Чтобы указать сетевые данные нового экземпляра виртуального Сервера администрирования:*

1. В разделе **Сеть для использования** выберите сеть домена, к которой подключен текущий узел кластера.
2. Выполните одно из следующих действий:
 - Если DHCP используется в выбранной сети для назначения IP-адресов, выберите параметр **Использовать DHCP**.
 - Если DHCP не используется в выбранной сети, укажите требуемый IP-адрес.
Указанный вами IP-адрес должен отличаться от IP-адреса кластера.
3. Нажмите на кнопку **Добавить**, чтобы применить указанные параметры.

Вы сможете использовать автоматически назначенный или указанный IP-адрес для подключения Консоли администрирования или Kaspersky Security Center Web Console к Серверу администрирования.

Шаг 5. Указание группы кластеров

Группа кластера – это особая роль отказоустойчивого кластера, которая содержит общие ресурсы для всех узлов. У вас есть два варианта:

- Создание новой кластерной группы.
Этот вариант рекомендуется в большинстве случаев. Новая группа кластера будет содержать все общие ресурсы, относящиеся к экземпляру Сервера администрирования.
- Выбор существующей группы кластеров.
Выберите этот параметр, если вы хотите использовать общий ресурс, который уже связан с существующей группой кластера. Например, вы можете использовать этот вариант, если хотите использовать хранилище, связанное с существующей группой кластера, и если нет другого доступного хранилища для новой группы кластера.

Шаг 6. Выбор кластерного хранилища данных

► *Чтобы выбрать кластерное хранилище данных:*

1. В разделе **Доступные хранилища** выберите хранилище, в которое будут установлены общие ресурсы экземпляра виртуального Сервера администрирования.

2. Если выбранное хранилище данных содержит несколько томов, в разделе **Доступные разделы на диске** выберите нужный том.
3. В поле **Путь установки** введите путь к общему хранилищу данных, в который будут установлены ресурсы экземпляра виртуального Сервера администрирования.

Хранилище данных выбрано.

Шаг 7. Указание учетной записи для удаленной установки

Укажите имя пользователя и пароль, которые будут использоваться для удаленной установки экземпляра виртуального Сервера администрирования на пассивный узел кластера.

Для указанной вами учетной записи должны быть предоставлены права администратора на всех узлах кластера.

Шаг 8. Выбор компонентов для установки

Выберите компоненты Сервера администрирования Kaspersky Security Center, которые вы хотите установить:

- **Управление мобильными устройствами.** Установите этот флажок, если требуется создать инсталляционные пакеты для мобильных устройств во время работы мастера установки Kaspersky Security Center. Вы можете также создать инсталляционные пакеты для мобильных устройств вручную, после установки Сервера администрирования средствами Консоли администрирования (см. раздел "Создание инсталляционных пакетов приложений" на стр. [850](#)).
- **Агент SNMP.** Получает статистическую информацию для Сервера администрирования по протоколу SNMP. Компонент доступен при установке приложения на устройство с установленным компонентом SNMP.

После установки Kaspersky Security Center необходимые для получения статистической информации mib-файлы будут расположены в папке установки приложения во вложенной папке SNMP.

Компоненты Агент администрирования и Консоль администрирования не отображаются в списке компонентов. Эти компоненты устанавливаются автоматически, их установку отменить невозможно.

На этом шаге мастера также следует указать папку для установки компонентов Сервера администрирования. По умолчанию компоненты устанавливаются в папку <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Если папки с таким названием нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

Шаг 9. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса приложения.

В таблице ниже перечислены параметры установки приложения и отображения интерфейса при выборе разных размеров сети.

Таблица 52. Зависимость параметров установки от выбора размеров сети

Параметры	1–100 устройств	101–1000 устройств	1001–5000 устройств	Более 5000 устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами	Отсутствует	Отсутствует	Присутствует	Присутствует
Отображение разделов Безопасность в окнах свойств Сервера и групп администрирования	Отсутствует	Отсутствует	Присутствует	Присутствует
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	Отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL 5.7 и SQL Express не рекомендуется использовать приложение для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

Шаг 10. Выбор базы данных

На этом шаге мастера выберите одну из следующих систем управления базами данных (СУБД), которая будет использоваться для хранения базы данных Сервера администрирования:

- **Microsoft SQL Server или SQL Server Express**
- **MySQL или MariaDB**
- **PostgreSQL или Postgres Pro**

Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

Структура базы данных Сервера администрирования представлена в файле klakdb.chm, который находится в папке установки Kaspersky Security Center. Этот файл также доступен в архиве на портале "Лаборатории Касперского": klakdb.zip (<https://support.kaspersky.com/help/KSC/common/klakdb.zip>).

Шаг 11. Настройка параметров SQL-сервера

На этом шаге мастера укажите следующие параметры подключения в зависимости от выбранной вами системы управления базами данных (СУБД):

- Если вы выбрали **Microsoft SQL Server или SQL Server Express** на предыдущем шаге:
 - В поле **Имя экземпляра SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

Если вы подключаетесь к SQL Server через пользовательский порт, то вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

```
SQL_Server_host_name,1433
```

Если вы защищаете соединение между Сервером администрирования и SQL Server с помощью сертификата (см. раздел "Сценарий: аутентификация Microsoft SQL Server" см. стр. 224), укажите в поле **Имя экземпляра SQL-сервера** то же имя экземпляра, которое использовалось при создании сертификата. Если вы используете именованный экземпляр SQL Server, вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

```
SQL_Server_name,1433
```

Если вы используете несколько экземпляров SQL Server на одном устройстве, дополнительно укажите через обратную косую черту имя экземпляра, например:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

Если для SQL Server в корпоративной сети включена функция Always On, укажите имя прослушивателя группы доступности в поле **Имя экземпляра SQL-сервера**. Обратите внимание, что Сервер администрирования поддерживает только режим доступности с синхронной фиксацией <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/availability-modes-always-on-availability-groups?view=sql-server-2016#SyncCommitAvMode>, когда включена функция Always On.

- В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение KAV.

Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL Server и вернитесь к установке Kaspersky Security Center.

- Если вы выбрали **MySQL или MariaDB** на предыдущем шаге:
 - В поле **Имя экземпляра SQL-сервера** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
 - В поле **Порт** укажите порт для подключения Сервера администрирования к базе данных DBMS-сервера. По умолчанию установлен порт 3306.

- В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.
- Если вы выбрали **PostgreSQL или Postgres Pro** на предыдущем шаге:
 - В поле **PostgreSQL или Postgres Pro Server** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
 - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 5432.

В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Шаг 12. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к системе управления базами данных (СУБД).

В зависимости от выбранной СУБД вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
 - **Режим аутентификации Microsoft Windows.** В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
 - **Режим аутентификации SQL-сервера.** В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.
Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Приложение проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вам нужно указать правильные учетные данные.

Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

Для MySQL, MariaDB, PostgreSQL или Postgres Pro укажите учетную запись и пароль.

Шаг 13. Выбор учетной записи для запуска Сервера администрирования

Выберите учетную запись, под которой Сервер администрирования будет запускаться как служба.

- **Создать учетную запись автоматически.** Приложение создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования kladminserver.

Вы можете выбрать этот вариант, если вы планируете разместить папку общего доступа (см. раздел "Шаг 11. Определение папки общего доступа" на стр. [242](#)) и СУБД (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)) на том же устройстве, что и Сервер администрирования.

- **Выбрать учетную запись.** Служба Сервера администрирования (kldminserver) будет запускаться под выбранной вами учетной записью.

Вам потребуется выбрать доменную учетную запись, например, если вы планируете использовать в качестве СУБД SQL-сервер любого выпуска, в том числе SQL-express (см. раздел "Шаг 6. Выбор базы данных" на стр. [237](#)), расположенный на другом устройстве, и/или если вы планируете разместить папку общего доступа (см. раздел "Шаг 11. Определение папки общего доступа" на стр. [242](#)) на другом устройстве.

Kaspersky Security Center поддерживает управляемые учетные записи службы (MSA) и групповые управляемые учетные записи службы (gMSA). Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования.

Прежде чем выбрать MSA или gMSA, необходимо установить учетную запись на том же устройстве, на котором вы хотите установить Сервер администрирования. Если учетная запись еще не установлена, отмените установку Сервера администрирования, установите учетную запись и перезапустите установку Сервера администрирования. Подробнее об установке управляемых учетных записей служб на локальном устройстве см. в официальной документации Microsoft.

Чтобы указать MSA или gMSA:

1. Нажмите на кнопку **Обзор**.
2. В появившемся окне нажмите на кнопку **Тип объекта**.
3. Выберите тип **Учетная запись для служб** и нажмите на кнопку **ОК**.
4. Выберите нужную учетную запись и нажмите на кнопку **ОК**.

Выбранная вами учетная запись должна обладать различными правами в зависимости от того, какую СУБД вы планируете использовать (см. раздел "Учетные записи для работы с СУБД" на стр. [207](#)).

Из соображений безопасности не делайте учетную запись, под которой запускается Сервер администрирования, привилегированной.

Если в дальнейшем вы захотите изменить учетную запись Сервера администрирования, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования (klsrvswch) (см. раздел "Смена учетной записи службы Сервера администрирования. Утилита klsrvswch" на стр. [712](#)). Обратите внимание, что вам нужно запустить утилиту klsrvswch на устройстве Сервера администрирования под учетной записью с правами администратора, которая использовалась для установки Сервера администрирования.

Шаг 14. Выбор учетной записи для запуска служб Kaspersky Security Center

Выберите учетную запись, под которой будут запускаться службы Kaspersky Security Center на этом

устройстве:

- **Создать учетную запись автоматически.** Kaspersky Security Center создает локальную учетную запись KIScSvc на этом устройстве в группе kladmins. Службы Kaspersky Security Center будут запускаться под созданной учетной записью.
- **Выбрать учетную запись.** Службы Kaspersky Security Center будут запускаться под выбранной вами учетной записью.

Вам потребуется выбрать доменную учетную запись, например, если вы планируете сохранять отчеты в папке, расположенной на другом устройстве, или же если этого требует политика безопасности в вашей организации. Также вам может потребоваться выбрать доменную учетную запись при установке Сервера администрирования на отказоустойчивый кластер (см. раздел "Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере" на стр. [226](#)).

Из соображений безопасности не делайте учетную запись, под которой запускаются службы, привилегированной.

Под выбранной учетной записью будут запускаться службы прокси-сервера KSN (ksnproхu), прокси-сервера активации "Лаборатории Касперского" (klactprх) и портала авторизации "Лаборатории Касперского" (klwebsrv).

Шаг 15. Определение папки общего доступа

Определите место размещения и название папки общего доступа, которая будет использоваться для следующих целей:

- хранения файлов, необходимых для удаленной установки приложений (файлы копируются на Сервер администрирования при создании инсталляционных пакетов);
- размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

К этому ресурсу будет открыт общий доступ на чтение для всех пользователей.

Вы можете выбрать один из двух вариантов:

- **Создать папку общего доступа.** Создание новой папки. Укажите путь к папке в расположенном ниже поле.
- **Выбрать существующую папку общего доступа.** Выбор папки общего доступа из числа уже существующих.

Папка общего доступа может размещаться как локально на устройстве, с которого производится установка, так и удаленно, на любом из клиентских устройств, входящих в состав сети организации. Вы можете указать папку общего доступа с помощью кнопки **Обзор** или вручную, введя в соответствующем поле UNC-путь (например, \\server\Share).

По умолчанию создается локальная папка Share в папке, заданной для установки компонентов Kaspersky Security Center.

Вы можете определить общую папку (см. раздел "Задание папки общего доступа" на стр. [227](#)) позже, если нужно.

Шаг 16. Настройка параметров подключения к Серверу администрирования

Настройте параметры подключения к Серверу администрирования:

- **Порт**

Номер порта, по которому выполняется подключение к Серверу администрирования.

По умолчанию используется порт 14000.

- **Номер SSL-порта**

Номер SSL-порта, по которому осуществляется защищенное подключение к Серверу администрирования с использованием протокола SSL.

По умолчанию используется порт 13000.

- **Длина ключа шифрования**

Выберите длину ключа шифрования 1024 бита или 2048 бит.

Ключ шифрования длиной 1024 бита оказывает меньшую нагрузку на процессор, но считается устаревшим и по техническим характеристикам может не обеспечивать надежное шифрование. Также есть вероятность, что имеющееся оборудование несовместимо с SSL-сертификатами с длиной ключа 1024 бита.

Ключ шифрования длиной 2048 бит отвечает современным стандартам шифрования. Однако использование 2048-битного ключа шифрования может привести к дополнительной нагрузке на процессор.

По умолчанию вариант выбран вариант **2048 бит (большая безопасность)**.

Также можно изменить параметры подключения к Серверу администрирования позже:

- Вы можете изменить порт и номера SSL-портов в разделе **Порты подключения** в свойствах Сервера администрирования. Дополнительную информацию о портах для подключения к Серверу администрирования см. в разделе Порты, используемые Kaspersky Security Center (см. стр. [63](#)).
- Вы можете изменить длину ключа шифрования при замене сертификата Сервера администрирования (см. раздел "Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert" на стр. [81](#)) утилитой klsetsrvcert с помощью параметра `-o RsaKeyLen:<длина ключа>`.

Шаг 17. Задание адреса Сервера администрирования

Задайте адрес Сервера администрирования. Вы можете выбрать один из следующих вариантов:

- **Имя DNS-домена.** Этот способ используется в том случае, когда в сети присутствует DNS-сервер, и клиентские устройства могут получить с его помощью адрес Сервера администрирования.

- **NetBIOS-имя.** Этот способ используется, если клиентские устройства получают адрес Сервера администрирования с помощью протокола NetBIOS, или в сети присутствует WINS-сервер.
- **IP-адрес.** Этот способ используется, если Сервер администрирования имеет статический IP-адрес, который в дальнейшем не будет изменяться.

Шаг 18. Адрес Сервера для подключения мобильных устройств

Этот шаг мастера установки доступен, если вы выбрали для установки компонент **Управление мобильными устройствами**.

В окне **Адрес для подключения мобильных устройств** укажите внешний адрес Сервера администрирования для подключения мобильных устройств, которые находятся за пределами локальной сети. Вы можете указать IP-адрес или DNS (Domain Name System) Сервера администрирования.

Шаг 19. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные приложения, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые приложения будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую консоль требуется запустить для работы с Kaspersky Security Center:

- **Запустить Консоль на основе MMC**
- **Запустить как Kaspersky Security Center Web Console**

Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Завершить**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования или Kaspersky Security Center Web Console вы можете выполнить первоначальную настройку приложения (см. стр. [281](#)).

Установка Сервера администрирования в тихом режиме

Сервер администрирования может быть установлен в тихом режиме, то есть без интерактивного ввода параметров установки.

► Чтобы установить Сервер администрирования на локальном устройстве в тихом режиме:

1. Прочитайте Лицензионное соглашение (см. раздел "О Лицензионном соглашении" см. стр. [342](#)). Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.
2. Прочитайте Политику конфиденциальности (см. раздел "Просмотр Политики конфиденциальности" см. стр. [205](#)). Используйте команду ниже, только если вы понимаете и соглашаетесь с тем, что мои данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности.
3. Выполните команду

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1
<setup_parameters>"
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (PARAM1=PARAM1VAL PARAM2=PARAM2VAL). Файл `setup.exe` расположен в папке `Server` внутри дистрибутива Kaspersky Security Center.

Имена и возможные значения параметров, которые можно использовать при установке Сервера администрирования в тихом режиме, приведены в таблице ниже.

Таблица 53. Параметры установки Сервера администрирования в тихом режиме

Имя параметра	Описание параметра	Доступные значения
EULA	Согласие с условиями Лицензионного соглашения.	• 1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
PRIVACYPOLICY	Согласие с условиями Политики конфиденциальности.	• 1 – Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Я подтверждаю, что полностью прочитал(а) и понимаю Политику конфиденциальности. • Другое значение или не задано – Я не принимаю условия Политики конфиденциальности (установка не выполняется).

Имя параметра	Описание параметра	Доступные значения
INSTALLATIONMODETYPE	Тип установки Сервера администрирования.	- Standard – стандартная установка. - Custom – выборочная установка.
INSTALLEDIR	Путь к папке установки Сервера администрирования.	Строковое значение.
ADDLOCAL	Список компонентов (через запятую) Сервера администрирования для установки.	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Минимальный достаточный для корректной установки Сервера администрирования список компонентов: ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.
NETRANGETYPE	Размер сети (количество устройств в сети).	- NRT_1_100 – от 1 до 100 устройств. - NRT_100_1000 – от 101 до 1000 устройств. - NRT_GREATER_1000 – более 1000 устройств.
SRV_ACCOUNT_TYPE	Способ задания учетной записи, под которой Сервер администрирования будет запускаться как служба.	- SrvAccountDefault – учетная запись создается автоматически. - SrvAccountUser – учетная запись пользователя задана вручную. В этом случае требуется задать значения параметров SERVERACCOUNTNAME и SERVERACCOUNTPWD.
SERVERACCOUNTNAME	Имя учетной записи, под которой Сервер администрирования будет запускаться как служба. Требуется задать значение параметра, если SRV_ACCOUNT_TYPE=SrvAccountUser.	Строковое значение.

Имя параметра	Описание параметра	Доступные значения
SERVERACCOUNTPWD	Пароль учетной записи, под которой Сервер администрирования будет запускаться как служба. Требуется задать значение параметра, если SRV_ACCOUNT_TYPE=SrvAccountU ser.	Строковое значение.
SERVERCER	Длина ключа для сертификата Сервера администрирования (в битах).	• 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит. • Значение не задано – длина ключа для сертификата Сервера администрирования составляет 1024 бит.
DBTYPE	Тип базы данных, которая будет использоваться для размещения информационной базы данных Сервера администрирования. Этот параметр является обязательным.	• MySQL – будет использоваться база данных MySQL или MariaDB. В этом случае следует задать значения параметров MYSQLSERVERNAME, MYSQLSERVERPORT, MYSQLDBNAME, MYSQLACCOUNTNAME и MYSQLACCOUNTPWD. • MSSQL – будет использоваться база данных Microsoft SQL Server (SQL Express). В этом случае следует задать значения параметров MSSQLSERVERNAME, MSSQLDBNAME, MSSQLAUTHTYPE. • POSTGRES – будет использоваться база данных PostgreSQL или Postgres Pro. В этом случае следует задать значения параметров POSTGRESERVERNAME, POSTGRESERVERPORT, POSTGRESDBNAME, POSTGRESACCOUNTNAME и POSTGRESACCOUNTPWD.
MYSQLSERVERNAME	Полное имя SQL Server. Требуется задать значение параметра, если DBTYPE=MySQL.	Строковое значение.

Имя параметра	Описание параметра	Доступные значения
MYSQLSERVERPORT	Номер порта для подключения к SQL-серверу. Требуется задать значение параметра, если DBTYPE=MySQL.	Числовое значение.
MYSQLDBNAME	Имя базы данных, которая будет создана для размещения данных Сервера администрирования. Требуется задать значение параметра, если DBTYPE=MySQL.	Строковое значение.
MYSQLACCOUNTNAME	Имя учетной записи для подключения к базе. Требуется задать значение параметра, если DBTYPE=MySQL.	Строковое значение.
MYSQLACCTPWDPWD	Пароль учетной записи для подключения к базе. Требуется задать значение параметра, если DBTYPE=MySQL.	Строковое значение.
MSSQLSERVERNAME	Полное имя SQL Server. Требуется задать значение параметра, если DBTYPE=MSSQL.	Строковое значение.
MSSQLDBNAME	Имя базы данных. Требуется задать значение параметра, если DBTYPE=MSSQL.	Строковое значение.
MSSQLAUTHTYPE	Тип авторизации при подключении к SQL-серверу. Требуется задать значение параметра, если DBTYPE=MSSQL.	- Windows – режим аутентификации Microsoft Windows. - SQLServer – режим аутентификации SQL-сервера. В этом случае требуется задать значения параметров <code>MSSQLACCOUNTNAME</code> и <code>MSSQLACCTPWDPWD</code>.
MSSQLACCOUNTNAME	Имя учетной записи для подключения к SQL-серверу. Требуется задать значение параметра, если MSSQLAUTHTYPE=SQLServer.	Строковое значение.
MSSQLACCTPWDPWD	Пароль учетной записи для подключения к SQL-серверу. Требуется задать значение параметра, если MSSQLAUTHTYPE=SQLServer.	Строковое значение.

Имя параметра	Описание параметра	Доступные значения
CREATE_SHARE_TYPE	Способ задания папки общего доступа.	- Create – создать новую папку общего доступа. В этом случае требуется задать значения параметров SHARELOCALPATH и SHAREFOLDERNAME. - ChooseExisting – выбрать существующую папку. В этом случае требуется задать значение параметра EXISTSHAREFOLDERNAME.
SHARELOCALPATH	Путь к локальной папке. Требуется задать значение параметра, если CREATE_SHARE_TYPE=Create	Строковое значение.
SHAREFOLDERNAME	Сетевое имя папки общего доступа. Требуется задать значение параметра, если CREATE_SHARE_TYPE=Create.	Строковое значение.
EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа. Требуется задать значение параметра, если CREATE_SHARE_TYPE=ChooseExisting.	Строковое значение.
SERVERPORT	Номер порта для подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL	Числовое значение.
SERVERADDRESS	Адрес Сервера администрирования.	Строковое значение.
MOBILESERVERADDRESS	Адрес Сервера для подключения мобильных устройств.	Строковое значение.

Подробно параметры установки Сервера администрирования описаны в разделе Выборочная установка (на стр. [234](#)).

См. также:

Основной сценарий установки.....[56](#)

Установка Консоли администрирования на рабочее место администратора

Вы можете установить Консоль администрирования отдельно на рабочее место администратора и управлять Сервером администрирования по сети с помощью этой Консоли.

► Чтобы установить Консоль администрирования на рабочее место администратора:

1. Запустите исполняемый файл `setup.exe`.
Откроется окно с выбором приложений "Лаборатории Касперского" для установки.
2. В окне с выбором приложений по ссылке **Установить только Консоль администрирования Kaspersky Security Center** запустите мастер установки Консоли администрирования. Следуйте далее указаниям мастера.
3. Выберите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.
4. В завершающем окне мастера установки нажмите на кнопку **Запустить**, чтобы начать процесс установки Консоли администрирования.

По окончании работы мастера Консоль администрирования будет установлена на рабочем месте администратора.

► Чтобы установить Консоль администрирования на рабочее место администратора в тихом режиме:

1. Прочитайте Лицензионное соглашение (см. раздел "О Лицензионном соглашении" см. стр. [342](#)). Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.
2. В папке `Distrib\Console` дистрибутива Kaspersky Security Center запустите файл `setup.exe` с помощью следующей команды:

```
setup.exe /s /v"EULA=1"
```

Если вы хотите установить все плагины управления из папки `Distrib\Console\Plugins` вместе с Консолью администрирования, выполните следующую команду:

```
setup.exe /s /v"EULA=1" /pALL
```

Если вы хотите указать, какие плагины управления устанавливать из папки `Distrib\Console\Plugins` вместе с Консолью администрирования, укажите плагины управления после ключа `/p` и разделите их точкой с запятой:

```
setup.exe /s /v"EULA=1" /pP1;P2;P3
```

Здесь P1, P2, P3 – имена плагинов управления, которые соответствуют именам папок плагинов управления в папке `Distrib\Console\Plugins`. Например:

```
setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
```

Консоль администрирования и плагины управления (если они были указаны) будут установлены на рабочее место администратора.

После установки Консоли администрирования следует подключиться к Серверу администрирования. Для этого нужно запустить Консоль администрирования и в открывшемся окне указать имя устройства или IP-адрес устройства, на котором установлен Сервер администрирования, а также параметры учетной записи для подключения к нему. После установления соединения с Сервером администрирования можно управлять системой антивирусной защиты с помощью этой Консоли администрирования.

Вы можете удалить Консоль администрирования стандартными средствами установки и удаления приложений Microsoft Windows.

См. также:

Основной сценарий установки.....[56](#)

Изменения в системе после установки Kaspersky Security Center

Значок Консоли администрирования

В результате установки Консоли администрирования на вашем устройстве появится значок для запуска Консоли администрирования. Вы можете найти Консоль администрирования в меню

Пуск → Приложения → Kaspersky Security Center.

Службы Сервера администрирования и Агента администрирования

Сервер администрирования и Агент администрирования будут установлены на устройстве в качестве служб со свойствами, указанными в таблице ниже. В таблице также указаны атрибуты других служб, которые выполняются на устройстве после установки Сервера администрирования.

Таблица 54. Свойства служб Kaspersky Security Center

Компонент	Имя службы	Отображаемое имя службы	Учетная запись
Сервер администрирования	kladminserver	Сервер администрирования Kaspersky Security Center	Указанная пользователем или специальная, созданная при установке, непривилегированная учетная запись вида KL-AK-*
Агент администрирования	klagent	Агент администрирования Kaspersky Security Center	Локальная система
Веб-сервер для работы Kaspersky Security Center Web Console и организации внутреннего портала организации	klwebsrv	Веб-сервер "Лаборатории Касперского"	Специальная непривилегированная учетная запись KIScSvc
Прокси-сервер активации	klactprx	Прокси-сервер активации "Лаборатории Касперского"	Специальная непривилегированная учетная запись KIScSvc
Прокси-сервер KSN	ksnproxy	Прокси-сервер Kaspersky Security Network	Специальная непривилегированная учетная запись KIScSvc

Если вы установите Kaspersky Security Center на узлах отказоустойчивого кластера Kaspersky Security Center, станет доступна служба klfoсsvс_klfoc. Службы klagent_klfoc and klfoсsvс_klfoc запускаются под учетной записью локальной системы. Служба kladminserver_klfoc должна запускаться под учетной записью "ksc"; другие службы — под учетной записью "rightless". Учетные записи "ksc" и "rightless" необходимо добавить в группу KLAmins с правами локального администратора. Для корректной работы Kaspersky Security Center необходимо использовать для запуска служб только учетные записи "ksc" и "rightless". Не рекомендуется использовать другие учетные записи с такими же правами. В таблице ниже приведены свойства служб, которые применяются на устройстве после установки Сервера администрирования на отказоустойчивом кластере Kaspersky Security Center.

Таблица 55. Свойства служб Kaspersky Security Center, установленных на отказоустойчивом

кластере Kaspersky Security Center

Компонент	Имя службы	Отображаемое имя службы	Учетная запись
Сервер администрирования	kladminserver_klfoc	Сервер администрирования Kaspersky Security Center	ksc
Агент администрирования	klagent_klfoc	Агент администрирования Kaspersky Security Center	Локальная система
Веб-сервер для работы Kaspersky Security Center Web Console и организации внутреннего портала организации	klwebsrv_klfoc	Веб-сервер "Лаборатории Касперского"	rightless
Прокси-сервер активации	klactprx_klfoc	Прокси-сервер активации "Лаборатории Касперского"	rightless
Прокси-сервер KSN	ksnproxy_klfoc	Прокси-сервер Kaspersky Security Network	rightless
Отказоустойчивый кластер Kaspersky Security Center	klfocsvc_klfoc	Отказоустойчивый кластер Kaspersky Security Center	Локальная система

Службы Kaspersky Security Center Web Console

Если вы установите Kaspersky Security Center Web Console на устройство, то на нем будут выполняться следующие службы (см. таблицу ниже):

Таблица 56. Службы Kaspersky Security Center Web Console

Отображаемое имя службы	Учетная запись
Kaspersky Security Center Service Web Console	NT Service/KSCSvcWebConsole
Kaspersky Security Center Web Console.	Сетевая служба
Kaspersky Security Center Product Plugins Server	NT Service/KSCWebConsolePlugin
Kaspersky Security Center Web Console Management Service	Локальная система
Kaspersky Security Center Web Console Message Queue	NT Service/KSCWebConsoleMessageQueue

Серверная версия Агента администрирования

Вместе с Сервером администрирования на устройство будет установлена серверная версия Агента администрирования. Она входит в состав Сервера администрирования, устанавливается и удаляется в его составе и может взаимодействовать только с локально установленным Сервером администрирования. Настраивать параметры подключения Агента к Серверу администрирования не требуется: настройка

реализована программно с учетом того, что компоненты установлены на одном устройстве. Серверная версия Агента администрирования устанавливается с теми же атрибутами и выполняет те же функции управления приложениями, что и стандартный Агент администрирования. На эту версию будет действовать политика группы администрирования, в которую включено клиентское устройство Сервера администрирования. Для серверной версии Агента администрирования создаются все задачи, предусмотренные для Агента администрирования, за исключением задачи смены Сервера.

Отдельная установка Агента администрирования на устройство с Сервером администрирования невозможна.

Вы можете просматривать свойства служб Сервера и Агента администрирования, а также следить за их работой при помощи стандартных средств администрирования Microsoft Windows: Управление компьютером\Службы. Информация о работе службы Сервера администрирования сохраняется в системном журнале Microsoft Windows на устройстве, где установлен Сервер администрирования, в отдельной ветви журнала событий Kaspersky Event Log.

Не рекомендуется вручную запускать и отключать службы и менять учетные записи в настройках служб. При необходимости вы можете поменять учетную запись службы Сервера администрирования с помощью утилиты klsrvswch (см. раздел "Смена учетной записи службы Сервера администрирования. Утилита klsrvswch" см. стр. [712](#)). Обратите внимание, что вам нужно запустить утилиту klsrvswch на устройстве Сервера администрирования под учетной записью с правами администратора, которая использовалась для установки Сервера администрирования.

Учетные записи и группы безопасности

По умолчанию инсталлятор Сервера администрирования создает следующие учетные записи:

- KL-AK-*: учетная запись службы Сервера администрирования;
- KIScSvc: учетная запись для прочих служб из состава Сервера администрирования;
- KIPxeUser: учетная запись для развертывания операционных систем.

Если на этапе работы инсталлятора вы выбирали другие учетные записи для службы Сервера администрирования и прочих служб, то будут использованы указанные вами учетные записи.

На устройстве, где установлен Сервер администрирования, также автоматически создаются локальные группы безопасности KLAadmins и KLOperators, с их соответствующими наборами прав (см. раздел "Права доступа к Серверу администрирования и его объектам" на стр. [706](#)).

Не рекомендуется устанавливать Сервер администрирования на контроллере домена. Тем не менее, если вы устанавливаете Сервер администрирования на контроллер домена, то вы должны запустить приложение установки с правами администратора домена. В этом случае приложение установки автоматически создаст доменные группы безопасности KLAadmins и KLOperators. Если вы устанавливаете Сервер администрирования на устройство, которое не является контроллером домена, то вам нужно запустить приложение установки с правами локального администратора. В этом случае приложение установки автоматически создаст локальные группы безопасности KLAadmins и KLOperators.

При настройке уведомлений по электронной почте вам может потребоваться завести учетную запись на почтовом сервере для ESMTP-аутентификации.

См. также:

Учетные записи для работы с СУБД [207](#)

Удаление приложения

Вы можете удалить Kaspersky Security Center стандартными средствами установки и удаления приложений Microsoft Windows. Для удаления приложения запускается мастер, в результате работы которого с устройства будут удалены все компоненты приложения (включая плагины). Мастер откроет веб-страницу в вашем браузере, используемом по умолчанию, с опросом, в котором вы можете сообщить нам, почему вы решили прекратить использование Kaspersky Security Center. Если во время работы мастера вы не задали удаление папки общего доступа (Share), то после завершения всех связанных с ней задач вы можете удалить ее вручную.

После удаления приложения в системной временной папке могут оставаться файлы.

Мастер создания задачи удаления приложения предложит вам сохранить резервную копию Сервера администрирования.

При удалении приложения с операционных систем Microsoft Windows 7 и Microsoft Windows 2008 возможно преждевременное завершение работы мастера создания задачи удаления приложения. Чтобы избежать этого, отключите в операционной системе службу контроля учетных записей (UAC) и повторно запустите удаление приложения.

Об обновлении предыдущей версии Kaspersky Security Center

Этот раздел содержит информацию о том, как обновить Kaspersky Security Center с предыдущей версии. Вы можете обновить Kaspersky Security Center разными способами, в зависимости от того, был ли установлен Kaspersky Security Center локально (см. раздел "Обновление предыдущей версии Kaspersky Security Center" см. стр. [276](#)) или на узлах отказоустойчивого кластера Kaspersky Security Center (см. раздел "Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center" см. стр. [277](#)).

Во время обновления недопустимо совместное использование СУБД Сервером администрирования и каким-либо другим приложением.

Обратите внимание, если вы обновите Сервер администрирования до версии 15.1, вы не сможете создавать инсталляционные пакеты Агента администрирования версии 15 или ниже. Ранее созданные инсталляционные пакеты будут доступны.

При обновлении предыдущей версии Kaspersky Security Center все установленные плагины поддерживаемых приложений "Лаборатории Касперского" сохраняются. Плагин Сервера администрирования и плагин Агента администрирования обновляются автоматически (как для Консоли администрирования, так и для Kaspersky Security Center Web Console).

В этом разделе

Обновление предыдущей версии Kaspersky Security Center.....	276
Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center	277
Обновление Kaspersky Security Center на узлах отказоустойчивого кластера Microsoft	278

Обновление предыдущей версии Kaspersky Security Center

В следующем разделе описаны рекомендуемые этапы подготовки к обновлению: Обновление Kaspersky Security Center и управляемых приложений безопасности.

Вы можете установить Сервер администрирования версии 15.1 на устройство, на котором установлена предыдущая версия Сервера администрирования (начиная с версии 11 (11.0.0.1131b)). При обновлении до версии 15.1 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Если при установке Сервера администрирования возникли проблемы, вы можете восстановить предыдущую версию Сервера администрирования, используя созданную перед обновлением резервную копию данных Сервера.

Если в сети установлен хотя бы один Сервер администрирования новой версии, вы можете обновить другие Серверы администрирования в сети с помощью задачи удаленной установки, в которой используется инсталляционный пакет Сервера администрирования.

Если вы развернули отказоустойчивый кластер Kaspersky Security Center, вы также можете обновить Kaspersky Security Center (см. раздел "Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center" см. стр. [277](#)) на его узлах.

► Чтобы обновить Сервер администрирования предыдущей версии до версии 15.1 с помощью резервной копии данных:

1. Запустите исполняемый файл ksc_15.1_<номер сборки>_full_<язык локализации>.exe для версии 15.1 (вы можете загрузить этот файл с сайта "Лаборатории Касперского").
2. В открывшемся окне по ссылке **Установить Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
3. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

- Условия и положения настоящего Лицензионного соглашения
- Политику конфиденциальности, которая описывает обработку данных

Установка приложения будет продолжена после установки обоих флажков. Мастер установки предложит вам создать резервную копию данных Сервера администрирования для ранних версий.

Kaspersky Security Center поддерживает восстановление данных из резервной копии, сформированной более ранней версией Сервера администрирования.

4. Если вы хотите создать резервную копию данных Сервера администрирования, укажите это в открывшемся окне **Резервное копирование данных Сервера администрирования**.

Резервная копия данных создается утилитой klbackup. Эта утилита входит в состав дистрибутива приложения и располагается в корне папки установки Kaspersky Security Center (см. раздел "Резервное копирование и восстановление данных Сервера администрирования" на стр. [723](#)).

5. Установите Сервер администрирования версии 15.1, следуя указаниям мастера установки.

Если появляется сообщение о том, что служба Kaspersky Security Center Web Console занята, в окне мастера нажмите на кнопку **Пропустить**.

Не рекомендуется прерывать работу мастера установки. Прерывание процесса обновления на стадии установки Сервера администрирования может привести к неработоспособности новой версии Kaspersky Security Center.

6. Для устройств, на которых установлен Агент администрирования предыдущей версии, создайте и запустите задачу удаленной установки новой версии Агента администрирования (см. раздел "Установка приложений с помощью задачи удаленной установки" на стр. [359](#)).

Рекомендуется обновить Агент администрирования для Linux до той же версии, что и Kaspersky Security Center.

После выполнения задачи удаленной установки версия Агента администрирования обновлена.

См. также

Основной сценарий установки.....	56
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....	455

Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center

Вы можете установить Сервер администрирования версии 15.1 на каждый узел отказоустойчивого кластера Kaspersky Security Center, где установлен Сервер администрирования более ранней версии (начиная с версии 13.2). При обновлении до версии 15.1 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Если вы ранее устанавливали Kaspersky Security Center на устройства локально, вы также можете обновить Kaspersky Security Center (см. раздел "Обновление предыдущей версии Kaspersky Security Center" см. стр. [276](#)) на этих устройствах.

► *Чтобы обновить Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center:*

1. Выполните следующие действия на активном узле кластера:
 - a. Запустите исполняемый файл ksc_15.1_<номер сборки>_full_<язык локализации>.exe.
Откроется окно с выбором приложений "Лаборатории Касперского" для обновления. Перейдите по ссылке **Установка Сервера администрирования Kaspersky Security Center** для запуска мастера установки Сервера администрирования. Следуйте инструкциям мастера.
 - b. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:
 - **Условия и положения настоящего Лицензионного соглашения**
 - **Политику конфиденциальности, которая описывает обработку данных**Установите оба флажка, чтобы продолжить установку.
Если вы не принимаете Лицензионное соглашение или Политику конфиденциальности, нажмите на кнопку **Отмена** для отмены обновления.
2. Выполните на пассивном узле отказоустойчивого кластера Kaspersky Security Center те же действия, что и на активном узле.
3. Запустить кластер (см. раздел "Запуск и остановка узла кластера вручную" см. стр. [252](#)).

В результате вы установили Сервер администрирования последней версии на узлы отказоустойчивого кластера Kaspersky Security Center.

Обновление Kaspersky Security Center на узлах отказоустойчивого кластера Microsoft

Вы можете установить Сервер администрирования версии 15.1 на каждый узел отказоустойчивого кластера "Лаборатории Касперского", где установлен Сервер администрирования более ранней версии (начиная с версии 13.2). При обновлении до версии 15.1 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

► *Чтобы обновить Kaspersky Security Center на узле отказоустойчивого кластера Microsoft:*

1. Выполните следующие действия на любом узле кластера:
 - a. Запустите исполняемый файл ksc_15.1_<номер сборки>_full_<язык локализации>.exe.
Откроется окно с выбором приложений "Лаборатории Касперского" для обновления. Перейдите по ссылке **Установка Сервера администрирования Kaspersky Security Center** для запуска мастера установки Сервера администрирования. Следуйте инструкциям мастера.

- b. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

- **Условия и положения настоящего Лицензионного соглашения**
- **Политику конфиденциальности, которая описывает обработку данных**

Установите оба флажка, чтобы продолжить установку.

Если вы не принимаете Лицензионное соглашение или Политику конфиденциальности, нажмите на кнопку **Отмена** для отмены обновления.

- c. В окне **Тип установки на кластер** выберите параметр **Кластер (установить на всех узлах кластера)**.

Далее установщик настраивает и завершает обновление Сервера администрирования на всех узлах кластера. Во время обновления параметры Сервера администрирования изменить невозможно.

2. Запустить кластер (см. раздел "Запуск и остановка узла кластера вручную" см. стр. [252](#)).

В результате вы установили Сервер администрирования последней версии на узлы отказоустойчивого кластера Microsoft.

Первоначальная настройка Kaspersky Security Center

В этом разделе описаны шаги, которые необходимо выполнить после установки Kaspersky Security Center для первоначальной настройки.

В этом разделе

Руководство по усилению защиты	280
Мастер первоначальной настройки Сервера администрирования	281
Настройка подключения Консоли администрирования к Серверу администрирования	296
Подключение автономных устройств	297
Шифрование подключения TLS	317
Настройка интерфейса	320

Руководство по усилению защиты

Руководство по усилению защиты адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Security Center, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security Center.

В Руководстве по усилению защиты описаны рекомендации и особенности настройки Kaspersky Security Center и его компонентов для снижения рисков его компрометации.

Перед настройкой создайте резервную копию Сервера администрирования Kaspersky Security Center с помощью задачи Резервное копирование данных Сервера администрирования (см. раздел "Резервное копирование и восстановление параметров Сервера администрирования" на стр. [721](#)) или с помощью утилиты kbackup. Сохраните резервную копию данных в надежном месте.

Руководство по усилению защиты содержит следующую информацию:

- выбор схемы развертывания Сервера Администрирования;
- настройка безопасного подключения к Серверу Администрирования;
- настройка учетных записей для работы с Сервером администрирования;
- управление защитой Сервера администрирования и клиентских устройств;
- настройка защиты управляемых приложений;
- обслуживание Сервера администрирования;
- передача информации в сторонние системы.

Перед началом работы с Сервером администрирования, Kaspersky Security Center предложит вам ознакомиться с краткой версией Руководства по усилению защиты.

Обратите внимание, что вы не можете использовать Сервер администрирования, пока не подтвердите, что ознакомились с Руководством по усилению защиты.

► Чтобы прочитать Руководство по усилению защиты:

1. Откройте Консоль администрирования или Kaspersky Security Center Web Console и войдите в консоль. Консоль проверяет, подтвердили ли вы, что прочитали текущую версию Руководства по усилению защиты.

Если вы еще не читали Руководство по усилению защиты, откроется окно с его краткой версией.

2. Выполните одно из следующих действий:
 - Если вы хотите просмотреть краткую версию Руководства по усилению защиты в виде текстового документа, перейдите по ссылке **Открыть в новом окне**.
 - Если вы хотите просмотреть полную версию Руководства по усилению защиты (см. раздел "Руководство по усилению защиты" на стр. [117](#)), перейдите по ссылке **Открыть Руководство по усилению защиты в онлайн-справке**.
3. После прочтения Руководства по усилению защиты установите флажок **Я подтверждаю, что полностью прочитал(а) и понимаю Руководство по усилению защиты** и нажмите на кнопку **Принять**.

Теперь вы можете работать с Сервером администрирования.

При появлении новой версии Руководства по усилению защиты Kaspersky Security Center предложит вам ее прочитать.

Мастер первоначальной настройки Сервера администрирования

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

См. также:

Основной сценарий установки.....	56
В этом разделе	
О мастере первоначальной настройки	282
Запуск мастера первоначальной настройки Сервера администрирования	283
Шаг 1. Настройка параметров прокси-сервера	283
Шаг 2. Выбор способа активации приложения.....	284
Шаг 3. Выбор областей защиты и операционных систем	285
Шаг 4. Выбор плагинов для управляемых приложений	286
Шаг 5. Загрузка дистрибутивов и создание инсталляционных пакетов	286
Шаг 6. Настройка использования Kaspersky Security Network	287

Шаг 7. Настройка параметров отправки уведомлений по электронной почте	288
Шаг 8. Настройка параметров управления обновлениями	289
Шаг 9. Создание первоначальной конфигурации защиты	289
Шаг 10. Подключение мобильных устройств	290
Шаг 11. Загрузка обновлений	295
Шаг 12. Обнаружение устройств	295
Шаг 13. Завершение работы мастера первоначальной настройки	296

О мастере первоначальной настройки

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

Мастер первоначальной настройки Сервера администрирования позволяет создать минимальный набор необходимых задач и политик, настроить минимум параметров, загрузить и установить плагины для управляемых приложений "Лаборатории Касперского" и создать инсталляционные пакеты для управляемых приложений "Лаборатории Касперского". В процессе работы мастера вы можете внести в приложение следующие изменения:

- Загрузить и установить плагины для управляемых приложений. После завершения работы мастера первоначальной настройки список установленных плагинов управления отображается в разделе **Дополнительно** → **Информация об установленных плагинах управления приложениями** в окне свойств Сервера администрирования.
- Создать инсталляционные пакеты для управляемых приложений "Лаборатории Касперского". После завершения работы мастера первоначальной настройки инсталляционные пакеты Агента администрирования для Windows и управляемых программ "Лаборатории Касперского" отображаются в списке **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
- Добавить файлы ключей или ввести коды активации, которые можно автоматически распространять на устройства в группах администрирования. После завершения работы мастера первоначальной настройки информация о лицензионных ключах отображается в списке **Сервер администрирования** → **Лицензии "Лаборатории Касперского"** и в разделе **Лицензионные ключи** окна свойств Сервера администрирования.
- Настроить взаимодействие с Kaspersky Security Network (KSN).
- Настроить рассылку по электронной почте оповещений о событиях в работе Сервера администрирования и управляемых приложений (чтобы уведомление прошло успешно, на Сервере администрирования и на всех устройствах-получателях должна быть запущена служба сообщений Messenger). После завершения работы мастера первоначальной настройки параметры почтовых уведомлений отображаются в разделе **Уведомление** в окне свойств Сервера администрирования.
- Настроить параметры обновлений и закрытия уязвимостей в приложениях, установленных на устройствах.
- Сформировать политику защиты рабочих станций и серверов, а также задачи поиска вредоносного ПО, получения обновлений и резервного копирования данных для верхнего уровня иерархии управляемых устройств. После завершения работы мастера первоначальной настройки созданные

задачи отображаются в списке **Сервер администрирования** → **Задачи**, а политики, соответствующие плагинам управляемых приложений, отображаются в списке **Сервер администрирования** → **Политики**.

Мастер первоначальной настройки создает политики для управляемых приложений, таких как Kaspersky Endpoint Security для Windows, если такие политики не были созданы ранее для группы **Управляемые устройства**. Мастер первоначальной настройки создает задачи, если задач с такими же именами нет в группе **Управляемые устройства**.

В Консоли администрирования Kaspersky Security Center автоматически предлагает запустить мастер первоначальной настройки после первого запуска приложения. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

Запуск мастера первоначальной настройки Сервера администрирования

Приложение автоматически предлагает запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к Серверу. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

► *Чтобы запустить мастер первоначальной настройки вручную:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла выберите пункт **Все задачи** → **Мастер первоначальной настройки Сервера администрирования**.

Мастер предложит произвести первоначальную настройку Сервера администрирования. Следуйте далее указаниям мастера.

При повторном запуске мастера первоначальной настройки задачи и политики, созданные при предыдущем запуске мастера, не создаются повторно.

Шаг 1. Настройка параметров прокси-сервера

Укажите параметры доступа Сервера администрирования к интернету. Доступ к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Kaspersky Security Center и управляемых приложений "Лаборатории Касперского".

Выберите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

- **Адрес**
Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.
- **Номер порта**
Номер порта, по которому будет выполняться подключение Kaspersky Security Center к прокси-серверу.
- **Не использовать прокси-сервер для локальных адресов**
При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.
- **Аутентификация на прокси-сервере**

Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере. Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

- **Имя пользователя**

Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

Пароль пользователя, через учетную запись которого выполняется подключение к прокси-серверу.

Вы можете настроить доступ в интернет позднее без запуска мастера первоначальной настройки.

Шаг 2. Выбор способа активации приложения

Выберите один из следующих вариантов активации Kaspersky Security Center:

- Введите код активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security Center. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если какой-либо причине не удалось выполнить активацию с помощью кода активации, вы можете активировать приложение, указав файл ключа.

- Укажите файл ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего приложение.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

- Отложите активацию приложения

Приложение будет работать в ограниченном режиме, без поддержки мобильных устройств и без функциональности системного администрирования.

Если вы выбрали отложенную активацию приложения, вы можете добавить лицензионный ключ (см. раздел "Добавление лицензионного ключа в хранилище Сервера администрирования." на стр. [392](#)) позже в любое время.

См. также:

Основной сценарий установки.....56

Шаг 3. Выбор областей защиты и операционных систем

Выберите области защиты и операционные системы, которые используются в вашей сети. При выборе этих параметров вы указываете фильтры для плагинов управления приложениями и дистрибутивов на серверах "Лаборатории Касперского", которые вы можете загрузить для установки на клиентские устройства в вашей сети. Выберите следующие параметры:

- **Области**

Вы можете выбрать одну из следующих областей защиты:

- **Рабочие станции.** Выберите этот параметр, если вы хотите защитить рабочие станции в вашей сети. По умолчанию выбран параметр Рабочая станция.
- **Файловые серверы и системы хранения данных.** Выберите этот параметр, если вы хотите защитить файловые серверы в вашей сети.
- **Мобильные устройства.** Выберите этот параметр, если вы хотите защитить мобильные устройства, принадлежащие организации или сотрудникам организации. Если вы выбрали этот параметр, но не предоставили лицензию с возможностью Управление мобильными устройствами (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. 354), отобразится сообщение о необходимости предоставить лицензию с возможностью Управление мобильными устройствами. Без этой лицензии использование возможностей Управления мобильными устройствами невозможно.
- **Виртуальные среды.** Выберите этот параметр, если вы хотите защитить виртуальные машины в вашей сети.
- **Анти-Спам.** Выберите этот параметр, если вы хотите защитить почтовые серверы вашей организации от спама, мошенничества и доставки вредоносных приложений.
- **Банкоматы и POS-системы.** Выберите этот параметр, если вы хотите защитить встроенные системы с операционной системой Windows, например банкоматы (АТМ).
- **Промышленные сети.** Выберите этот параметр, если вы хотите контролировать данные безопасности в промышленной сети и с конечных устройств сети, защищенных приложениями "Лаборатории Касперского".
- **Промышленные конечные точки.** Выберите этот параметр, если вы хотите защитить отдельные узлы промышленной сети.

- **Операционные системы**

Можно выбрать инсталляционные пакеты приложений "Лаборатории Касперского" из списка доступных инсталляционных пакетов позднее без запуска мастера первоначальной настройки. Для упрощения поиска необходимых инсталляционных пакетов вы можете фильтровать список доступных инсталляционных пакетов (см. раздел "Работа с плагинами управления" см. стр. 368) по следующим критериям:

- область защиты;

- тип загружаемого программного обеспечения (дистрибутив, утилита, плагин или веб-плагин);
- версия приложения "Лаборатории Касперского";
- язык локализации приложения "Лаборатории Касперского".

Шаг 4. Выбор плагинов для управляемых приложений

Выберите плагины для управляемых приложений для установки. Отображается список плагинов, расположенных на серверах "Лаборатории Касперского". Список отфильтрован в соответствии с параметрами, выбранными на предыдущем шаге (см. раздел "Шаг 3. Выбор областей защиты и операционных систем" на стр. [285](#)) мастера. По умолчанию в полный список включены плагины всех языков. Чтобы отображался только плагин на выбранном языке, выберите язык в раскрывающемся списке **Отображать язык Консоли администрирования или**. Список плагинов включает в себя следующие столбцы:

- **Название приложения.**

Выбраны подключаемые модули в зависимости от областей защиты и платформ, выбранных на предыдущем шаге.

- **Версия приложения.**

В список включены плагины всех версий, размещенных на серверах "Лаборатории Касперского". По умолчанию выбраны плагины последних версий.

- **Язык локализации.**

По умолчанию язык локализации плагина зависит от языка Kaspersky Security Center, который вы выбрали при установке. Другие языки можно выбрать в раскрывающемся списке **Отображать язык Консоли администрирования или**.

После выбора плагинов, их установка начинается автоматически в отдельном окне. Для установки некоторых плагинов вам нужно принять условия Лицензионного соглашения. Ознакомьтесь с текстом Лицензионного соглашения, выберите параметр **Я принимаю условия Лицензионного соглашения** и нажмите на кнопку **Установить**. Если вы не согласны с условиями Лицензионного соглашения, плагин не установится.

После завершения установки, закройте окно установки.

Вы также можете выбрать плагин управления (см. раздел "Работа с плагинами управления" см. стр. [368](#)) позднее без запуска мастера первоначальной настройки.

Шаг 5. Загрузка дистрибутивов и создание инсталляционных пакетов

Kaspersky Endpoint Security для Windows включает инструменты шифрования информации, хранящейся на клиентских устройствах. Чтобы загрузить дистрибутив Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.

В окне **Тип шифрования** выберите один из следующих типов шифрования:

- Strong encryption (AES256). Для этого типа шифрования используется 256-разрядный ключ.
- Lite encryption (AES56). Для этого типа шифрования используется 56-разрядный ключ.

Окно **Тип шифрования** отображается, только если в качестве области защиты выбран (см. раздел "Шаг 3. Выбор областей защиты и операционных систем" на стр. 285) вариант **Рабочие станции**, а в качестве платформы – **Microsoft Windows**.

После того, как вы выбрали тип шифрования, отобразится список дистрибутивов для обоих типов шифрования. В списке выбран дистрибутив с выбранным типом шифрования. Язык дистрибутива соответствует языку Kaspersky Security Center. Если дистрибутив Kaspersky Endpoint Security для Windows для языка Kaspersky Security Center не существует, выбирается дистрибутив на английском языке.

В раскрывающемся списке **Отображать язык Консоли администрирования или** можно выбрать языки для дистрибутива.

Для дистрибутивов управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center.

В списке вы можете выбрать дистрибутив любого типа шифрования, отличного от того, который вы выбрали в окне **Тип шифрования**. После того, как вы выбрали дистрибутив Kaspersky Endpoint Security для Windows, начинается загрузка дистрибутивов, соответствующих компонентам и платформам (см. раздел "Шаг 3. Выбор областей защиты и операционных систем" на стр. 285). Вы можете контролировать ход загрузки в графе **Состояние загрузки**. После завершения работы мастера первоначальной настройки инсталляционные пакеты Агента администрирования для Windows и управляемых программ "Лаборатории Касперского" отображаются в списке **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.

Чтобы завершить загрузку некоторых дистрибутивов вам нужно принять Лицензионное соглашение. При нажатии кнопки **Принять** отображается текст Лицензионного соглашения. Чтобы перейти к следующему шагу мастера, вам нужно принять положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского". Выберите параметры, связанные с Лицензионным соглашением и Политикой конфиденциальности "Лаборатории Касперского", и нажмите на кнопку **Принять все**. Если вы не принимаете положения и условия, загрузка пакета отменяется.

После того, как вы приняли положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского", загрузка дистрибутивов продолжается. После завершения загрузки отображается статус **Создан инсталляционный пакет**. В дальнейшем инсталляционные пакеты можно использовать для развертывания приложений "Лаборатории Касперского" на клиентских устройствах.

Вы можете создать инсталляционные пакеты (см. раздел "Создание инсталляционного пакета." на стр. 372) позднее без запуска мастера первоначальной настройки. В дереве Консоли администрирования перейдите в раздел **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.

Шаг 6. Настройка использования Kaspersky Security Network

Можно подключать репутационные базы Kaspersky Security Network (см. раздел "О KSN и KPSN" на стр. 873), чтобы обеспечить более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повысить эффективность работы некоторых компонентов защиты, а также снизить вероятность ложных срабатываний.

Прочтите Положение о KSN, которое отображается в окне. Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network. Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

Клиентские устройства под управлением Kaspersky Security Center в автоматическом режиме будут предоставлять "Лаборатории Касперского" информацию о работе установленных на них приложений "Лаборатории Касперского". Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия использования Kaspersky Security Network**

Клиентские устройства под управлением Kaspersky Security Center не будут предоставлять "Лаборатории Касперского" информацию о работе установленных на них приложений "Лаборатории Касперского".

Если вы загрузили плагин Kaspersky Endpoint Security для Windows, отобразятся оба положения о KSN: Положение о KSN для Kaspersky Security Center и Положение о KSN для Kaspersky Endpoint Security для Windows. Положения о KSN для других управляемых приложений "Лаборатории Касперского", для которых были загружены плагины, отображаются в отдельных окнах и каждое из них необходимо принять (или отклонить) отдельно.

Настроить доступ Сервера администрирования к Kaspersky Security Network (KSN) (см. раздел "Настройка доступа к KPSN" на стр. [874](#)) можно также далее в окне свойств Сервера администрирования в Консоли администрирования.

Шаг 7. Настройка параметров отправки уведомлений по электронной почте

Настройте параметры отправки уведомлений о событиях, регистрируемых при работе приложений "Лаборатории Касперского" на управляемых устройствах. Эти параметры будут использоваться в качестве значений по умолчанию для Сервера администрирования.

Для настройки рассылки оповещений о возникающих событиях приложений "Лаборатории Касперского" доступны следующие параметры:

- **Получатели (адреса электронной почты)**

Адреса электронной почты пользователей, которым приложение будет отправлять уведомления.

- **SMTP-серверы**

Адреса почтовых серверов вашей организации, введенные через точку с запятой. В качестве адреса может использоваться IP-адрес или имя устройства в сети Windows (NetBIOS-имя).

- **Порт SMTP-сервера**

Номер коммуникационного порта SMTP-сервера. По умолчанию указан порт 25.

- **Использовать ESMTP-аутентификацию**

Включение поддержки ESMTP-аутентификации. После установки флажка в полях **Имя пользователя** и **Пароль** можно указать параметры ESMTP-аутентификации. По умолчанию флажок снят, параметры ESMTP-аутентификации недоступны.

- **Параметры**

Вы можете проверить параметры уведомления о сообщениях электронной почты с помощью кнопки **Отправить тестовое сообщение**.

Вы также можете настроить уведомления о событии (см. раздел "Настройка параметров уведомлений о событиях" на стр. [311](#)) позднее без запуска мастера первоначальной настройки.

Шаг 8. Настройка параметров управления обновлениями

Настройте параметры работы с обновлениями приложений, установленных на клиентских устройствах.

Вы можете настроить эти параметры, только если вы предоставили лицензионный ключ, который предусматривает возможности Системного администрирования.

В блоке параметров **Режим поиска и установки обновлений** вы можете выбрать один из режимов поиска и установки обновлений Kaspersky Security Center:

- **Искать требуемые обновления**

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически, если она еще не создана.

По умолчанию этот вариант выбран.

- **Искать и устанавливать требующиеся обновления**

Задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* создаются автоматически, если они не были созданы ранее.

В блоке параметров **Службы Windows Server Update Services** вы можете выбрать источник синхронизации обновлений:

- **Использовать источники обновлений, заданные в политике домена**
- **Использовать Сервер администрирования в роли WSUS-сервера**

Создается задача **Синхронизация обновлений Windows Update**.

Вы можете создать (см. раздел "Создание задачи" на стр. [416](#)) задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* позднее без запуска мастера первоначальной настройки. Чтобы использовать Сервер администрирования в качестве WSUS-сервера (см. раздел "Синхронизация обновлений Windows Update с Сервером администрирования" на стр. [506](#)), вам нужно создать задачу *Синхронизация обновлений Windows Update* и выбрать параметр **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования (см. раздел "Параметры политики Агента администрирования" см. стр. [789](#)).

Шаг 9. Создание первоначальной конфигурации защиты

В окне **Создание первоначальной конфигурации защиты** отображается список политик и задач, созданных автоматически. Создаются следующие политики и задачи:

- политика Агента администрирования Kaspersky Security Center;
- политики для управляемых приложений "Лаборатории Касперского", чьи плагины управления были установлены ранее (см. раздел "Шаг 4. Выбор плагинов для управляемых приложений" на стр. [286](#));
- задача Обслуживание Сервера администрирования;

- задача Резервное копирование данных Сервера администрирования;
- задача Загрузка обновлений в хранилище Сервера администрирования;
- задача Поиск уязвимостей и требуемых обновлений;
- задача Установка обновлений.

Для перехода на следующий шаг мастера дождитесь окончания создания политик и задач.

Если вы загрузили и установили плагин для Kaspersky Endpoint Security для Windows версии 10 Service Pack 1 и выше, до версии 11.0.1, во время создания политик и задач откроется окно первоначальной настройки доверенной зоны Kaspersky Endpoint Security для Windows. Приложение предложит внести в доверенную зону проверенных "Лабораторией Касперского" поставщиков, чтобы исключить их приложения из проверки для предотвращения случайной блокировки. Вы можете создать рекомендованные исключения сейчас или создать список исключений позже, выбрав в дереве консоли **Политики** → меню свойств Kaspersky Endpoint Security → **Продвинутая защита** → **Доверенная зона** → **Настройка** → **Добавить**. Список исключений проверки доступен для редактирования в любой момент дальнейшей работы с приложением.

Работа с доверенной зоной выполняется средствами приложения Kaspersky Endpoint Security для Windows. Подробные инструкции по выполнению операций и описание особенностей шифрования приведены в онлайн-справке Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>.

Для завершения первоначальной настройки доверенной зоны и возвращения к мастеру нажмите **ОК**.

Нажмите **Далее**. Кнопка станет доступна, когда все необходимые политики и задачи будут созданы.

Также можно создать необходимые задачи (см. раздел "Создание задачи" на стр. [416](#)) и политики (см. раздел "Создание политики" см. стр. [435](#)) позднее без запуска мастера первоначальной настройки.

Шаг 10. Подключение мобильных устройств

Если ранее в параметрах мастера вы включили область защиты **Мобильные устройства** (см. раздел "**Шаг 3. Выбор областей защиты и операционных систем**" на стр. [285](#)), укажите параметры подключения корпоративных мобильных устройств управляемой организацией. Если вы не включили область защиты **Мобильные устройства**, этот шаг будет пропущен.

На этом шаге мастера выполните следующие действия:

- Настройте порты подключения мобильных устройств.
- Настройте параметры аутентификации Сервера администрирования.
- Создайте сертификаты или управлять ими.
- Настройте выпуск, автоматическое обновление и шифрование сертификатов общего типа.
- Создайте правила перемещения мобильных устройств.

► *Чтобы настроить порты подключения мобильных устройств:*

1. Нажмите на кнопку **Настроить** справа от поля **Подключение мобильных устройств**.
2. В раскрывающемся списке выберите **Настроить порты**.

Откроется окно свойств Сервера администрирования на разделе **Дополнительные порты**.

3. В разделе **Дополнительные порты** вы можете настроить параметры подключения мобильных устройств:

- **SSL-порт для прокси-сервера активации**

Номер SSL-порта для подключения Kaspersky Endpoint Security 10 для Windows к серверам активации "Лаборатории Касперского".

По умолчанию используется порт 17000.

- **Открыть порт для мобильных устройств**

Если флажок установлен, то открыт порт, по которому мобильные устройства будут подключаться к Серверу лицензирования. Вы можете задать номер порта и другие настройки в полях ниже.

Если флажок снят, то открытого порта для подключения мобильных устройств нет, и поля **Порт для мобильных устройств** и **Порт активации мобильных клиентов** недоступны для редактирования.

По умолчанию флажок установлен.

- **Порт для синхронизации мобильных устройств**

Номер порта, по которому мобильные устройства будут подключаться к Серверу администрирования и обмениваться с ним информацией. По умолчанию используется порт 13292.

Вы можете назначить другой порт, если порт 13292 используется в каких-то других целях.

- **Порт для активации мобильных устройств**

Порт подключения Kaspersky Endpoint Security для Android к серверам активации "Лаборатории Касперского".

По умолчанию используется порт 17100.

- **Открыть порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

Если флажок установлен, то устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

По умолчанию флажок установлен.

- **Порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию используется порт 13294.

- **Открыть порт для Prometheus**

4. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к мастеру первоначальной настройки.

Вам потребуется настроить аутентификацию Сервера администрирования мобильными устройствами и аутентификацию мобильных устройств Сервером администрирования. Вы можете настроить архитектуру приложения позже, независимо от мастера первоначальной настройки.

► *Чтобы настроить параметры аутентификации Сервера администрирования мобильными устройствами:*

1. Нажмите на кнопку **Настроить** справа от поля **Подключение мобильных устройств**.

2. В раскрывающемся списке выберите **Настроить аутентификацию**.

Откроется окно свойств Сервера администрирования на разделе **Сертификаты**.

3. В группе параметров **Аутентификация Сервера администрирования мобильными устройствами** выберите вариант аутентификации для мобильных устройств, а в группе параметров **Аутентификация Сервера администрирования устройствами с защитой на уровне UEFI** выберите вариант аутентификации для устройств с защитой на уровне UEFI.

Аутентификация Сервера администрирования при обмене информацией с клиентскими устройствами выполняется на основании сертификата.

По умолчанию выбрано использование сертификата, созданного при установке Сервера администрирования. При необходимости можно добавить новый сертификат.

► *Чтобы добавить новый сертификат (не обязательно):*

1. Выберите **Другой сертификат**.

Появится кнопка **Обзор**.

2. Нажмите на кнопку **Обзор**.

3. В появившемся окне настройте параметры сертификата:

- **Тип сертификата**

- Срок активации:

- **Немедленно**

Текущий сертификат будет заменен новым сертификатом сразу после нажатия на кнопку **ОК**.

Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

- **Через указанный срок (сут)**

Если выбран этот вариант, то будет сгенерирован резервный сертификат. Текущий сертификат будет заменен новым сертификатом через указанное количество дней. Дата, с которой резервный сертификат вступит в силу, отображается в разделе **Сертификаты**.

После того как текущий сертификат будет заменен новым сертификатом, ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

4. Вы можете нажать на кнопку **Свойства**, чтобы просмотреть параметры выбранного сертификата Сервера администрирования.

► *Чтобы перевыпустить сертификат, выпущенный средствами Сервера администрирования:*

1. Выберите **Сертификат выпущен средствами Сервера администрирования**.

2. Нажмите на кнопку **Перевыпустить**.

3. В открывшемся окне настройте следующие параметры:

- Адрес подключения:

- **Оставить адрес подключения прежним**

Адрес Сервера администрирования, к которому подключаются мобильные

устройства, останется прежним.

Этот вариант выбран по умолчанию.

- **Изменить адрес подключения на**

Если необходимо, чтобы мобильные устройства подключались по другому адресу, укажите в поле требуемый адрес.

При изменении адреса подключения мобильных устройств необходимо выпустить новый сертификат. Старый сертификат будет недействительным на подключенных мобильных устройствах. Ранее подключенные устройства не смогут подключиться к Серверу администрирования и перестанут быть управляемыми.

- Срок активации:

- **Немедленно**

Текущий сертификат будет заменен новым сертификатом сразу после нажатия на кнопку **ОК**.

Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

- **Через указанный срок (сут)**

Если выбран этот вариант, то будет сгенерирован резервный сертификат. Текущий сертификат будет заменен новым сертификатом через указанное количество дней. Дата, с которой резервный сертификат вступит в силу, отображается в разделе **Сертификаты**.

После того как текущий сертификат будет заменен новым сертификатом, ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

4. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к окну **Сертификаты**.

5. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к мастеру первоначальной настройки.

► *Чтобы настроить выпуск, автоматическое обновление и шифрование сертификатов общего типа для идентификации мобильных устройств Сервером администрирования:*

1. Нажмите на кнопку **Настроить** справа от поля **Аутентификация мобильных устройств**.

Откроется окно **Правила выпуска сертификатов** на разделе **Выпуск мобильных сертификатов**.

2. При необходимости настройте следующие параметры в блоке параметров **Параметры выпуска**:

- **Срок действия сертификата, дней**

Срок действия сертификата в днях. По умолчанию срок действия сертификата равен 365 дням. По истечении этого срока мобильное устройство не сможет подключаться к Серверу администрирования.

- **Источник сертификата**

Выбор источника сертификатов общего типа для мобильных устройств: сертификаты выпускает Сервер администрирования или сертификаты задаются вручную.

Вы можете изменить шаблон сертификата, если в разделе **Интеграция с PKI** настроена интеграция с инфраструктурой открытых ключей. В этом случае будут доступны следующие поля выбора шаблона:

- **Шаблон по умолчанию**

Использование сертификата, выпущенного внешним источником сертификатов – центром сертификации – по шаблону, заданному по умолчанию.

По умолчанию выбран этот вариант.

- **Другой шаблон**

Выбор шаблона, на основании которого будут выпускаться сертификаты. Шаблоны сертификатов можно задать в домене. По кнопке **Обновить список** можно обновить список шаблонов сертификатов.

3. При необходимости задайте следующие параметры автоматического выпуска сертификатов в блоке параметров **Параметры автоматического обновления**:

- **Обновлять, когда до истечения срока действия осталось (сут)**

Количество дней до истечения срока действия текущего сертификата, за которое Сервер администрирования должен выпустить новый сертификат. Например, если в поле указано значение 4, Сервер администрирования выпустит новый сертификат за четыре дня до окончания срока действия текущего сертификата. По умолчанию указано значение 7.

- **Автоматически перевыпускать сертификат, если это возможно**

При наличии возможности сертификаты будут перевыпускаться автоматически. Автоматический перевыпуск недоступен, если сертификат был задан вручную. Если флажок снят, сертификаты автоматически не перевыпускаются. По умолчанию флажок снят.

Сертификаты обновляются автоматически центром сертификации.

4. При необходимости настройте параметры расшифровки сертификатов при установке в блоке параметров **Защита паролем**.

Выберите параметр **Запрашивать пароль при установке сертификата**, чтобы при установке сертификата на мобильное устройство у пользователя запрашивался пароль. Пароль используется только один раз, при установке сертификата на мобильное устройство.

Пароль будет автоматически сгенерирован средствами Сервера администрирования и отправлен по указанному вами адресу электронной почты. Вы можете указать адрес электронной почты пользователя либо свой собственный, если хотите затем передать пользователю пароль другим способом.

Вы можете указать количество символов пароля для расшифровки сертификата с помощью ползунка.

Функция запроса пароля необходима, например, для защиты общего сертификата в автономном инсталляционном пакете Kaspersky Endpoint Security для Android. Защита паролем не позволит злоумышленнику получить доступ к общему сертификату при краже автономного инсталляционного пакета с Веб-сервера Kaspersky Security Center.

Если параметр выключен, расшифровка сертификата при установке будет проводиться автоматически и у пользователя не будет запрашиваться пароль. По умолчанию параметр выключен.

5. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к окну мастера первоначальной настройки.

Нажмите на кнопку **Отмена**, чтобы вернуться к мастеру первоначальной настройки без сохранения внесенных изменений.

- Чтобы включить функцию перемещения мобильных устройств в нужную вам группу администрирования,

В поле **Автоматически перемещать мобильные устройства** выберите параметр **Создать правило перемещения мобильных устройств**.

Если параметр **Создать правило перемещения мобильных устройств** выбран, приложение автоматически создает правило перемещения, которое перемещает устройства под управлением операционных систем Android и iOS в группу **Управляемые устройства**:

- с операционными системами Android, на которых установлен Kaspersky Endpoint Security для Android и мобильный сертификат;
- с операционными системами iOS, на которых установлен iOS MDM-профиль с общим сертификатом.

Если такое правило уже существует, то приложение не создает правило.

По умолчанию параметр выключен.

"Лаборатория Касперского" больше не поддерживает Kaspersky Safe Browser.

Шаг 11. Загрузка обновлений

Обновления антивирусных баз для Kaspersky Security Center и управляемых приложений "Лаборатории Касперского" загружаются автоматически. Обновления загружаются с серверов "Лаборатории Касперского".

Чтобы загружать обновления без запуска мастера первоначальной настройки, создайте и настройте (см. раздел "Создание задачи для загрузки обновлений в хранилище Сервера администрирования" на стр. [469](#)) задачу *Загружать обновления в хранилище Сервера администрирования*.

Шаг 12. Обнаружение устройств

В информационном окне **Опрос сети** отображается информация о статусе опроса сети Сервером администрирования.

Вы можете просмотреть обнаруженные в сети Сервером администрирования устройства и получить справку по работе с окном **Обнаружение устройств** по ссылкам в нижней части окна.

Вы можете выполнить опрос сети позднее без запуска мастера первоначальной настройки. Используйте Консоль администрирования для настройки опроса Windows-доменов (см. раздел "Опрос сети Windows" на стр. [325](#)), Active Directory (см. раздел "Опрос Active Directory" на стр. [328](#)), IP-диапазонов (см. раздел "Опрос IP-диапазонов" см. стр. [330](#)) и IPv6-сетей (см. раздел "Опрос Zeroconf" на стр. [331](#)).

См. также:

Сценарий: обнаружение сетевых устройств	322
Основной сценарий установки.....	56

Шаг 13. Завершение работы мастера первоначальной настройки

В окне завершения работы мастера первоначальной настройки выберите параметр **Запускает мастер удаленной установки**, если вы хотите запустить автоматическую установку антивирусных приложений и/или Агента администрирования на устройства в вашей сети.

Для завершения работы мастера нажмите на кнопку **Готово**.

Настройка подключения Консоли администрирования к Серверу администрирования

Консоль администрирования подключена к Серверу администрирования по SSL-порту TCP 13291. Этот же порт может использоваться объектами автоматизации klakaut.

Порт TCP 14000 может использоваться для подключения Консоли администрирования, точек распространения, подчиненных Серверов администрирования и объектов автоматизации утилиты klakaut, а также для получения данных с клиентских устройств.

Как правило, SSL-порт TCP 13000 могут использовать только Агент администрирования, подчиненный Сервер и главный Сервер администрирования, размещенный в демилитаризованной зоне. В некоторых случаях может быть необходимо подключение Консоли администрирования по SSL-порту 13000:

- если предпочтительно использовать один и тот же SSL-порт как для Консоли администрирования, так и для других активностей (для получения данных с клиентских устройств, подключения точек распространения, подключения подчиненных Серверов администрирования);
- если объект автоматизации утилиты klakaut подключается к Серверу администрирования не напрямую, а через точку распространения, размещенную в демилитаризованной зоне.

► Чтобы разрешить подключение Консоли администрирования по порту 13000:

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
 - для 32-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\core\independent\KLLIM
 - для 64-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\core\independent\KLLIM
3. Для ключа LP_ConsoleMustUsePort13291 (DWORD) установите значение 00000000.
По умолчанию для этого ключа указано значение 1.
4. Перезапустите службу Сервера администрирования.

В результате Консоль администрирования сможет подключаться к Серверу администрирования, используя порт 13000.

Подключение автономных устройств

В этом разделе описано, как подключить автономные устройства к Серверу администрирования (то есть управляемые устройства, находящиеся вне основной сети).

В этом разделе

Сценарий: подключение автономных устройств через шлюз соединения	297
Сценарий: подключение автономных устройств через подчиненный Сервер администрирования в демилитаризованной зоне	299
О подключении автономных устройств	300
Подключение внешних настольных компьютеров к Серверу администрирования	302
О профилях соединения для автономных пользователей	303
Создание профиля соединения для автономных пользователей	304
О переключении Агента администрирования на другой Сервер администрирования	307
Создание правила переключения Агента администрирования по сетевому местоположению	308
Уведомления о событиях	311

Сценарий: подключение автономных устройств через шлюз соединения

В этом сценарии описано, как подключить к Серверу администрирования управляемые устройства, находящиеся вне основной сети.

Предварительные требования

Сценарий имеет следующие предварительные требования:

- В сети вашей организации организована демилитаризованная зона (DMZ).
- Сервер администрирования Kaspersky Security Center развернут в корпоративной сети.

Этапы

Этот сценарий состоит из следующих этапов:

а. Выбор клиентского устройства в демилитаризованной зоне

Это устройство будет использоваться в качестве шлюза соединения (см. раздел "Шлюз соединения" см. стр. [54](#)). Выбранное устройство должно соответствовать требованиям для шлюзов соединения.

б. Установка Агента администрирования в роли шлюза соединения

Для установки Агента администрирования на выбранное устройство рекомендуем использовать локальную установку (см. раздел "Локальная установка Агента администрирования" на стр. [193](#)).

По умолчанию установочный файл находится по адресу: \\<Имя Сервера>\KLSHARE\PkgInst\NetAgent_<номер версии>.

В окне **Шлюз соединения** мастера установки Агента администрирования выберите параметр **Использовать в качестве шлюза соединения в демилитаризованной зоне**. Этот режим одновременно активирует роль шлюза соединения и предписывает Агенту администрирования

ждать соединений от Сервера администрирования, а не устанавливать соединения с Сервером администрирования.

Также вы можете установить Агент администрирования на устройство под управлением Linux и настроить Агент администрирования для работы в качестве шлюза соединения (см. раздел "Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне" см. стр. [691](#)). Обратите внимание на список ограничений Агента администрирования, работающего на устройствах под управлением Linux (см. раздел "Использование Агента администрирования для Windows, macOS и Linux: сравнение" см. стр. [967](#)).

с. Разрешение соединения на сетевом экране шлюза соединения

Чтобы Сервер администрирования мог подключаться к шлюзу соединения в демилитаризованной зоне, разрешите подключения к TCP-порту 13000 во всех сетевых экранах между Сервером администрирования и шлюзом соединения.

Если шлюз соединения не имеет реального IP-адреса в интернете, но вместо этого расположен за Network Address Translation (далее также NAT), настройте правило для пересылки подключений через NAT.

d. Создание группы администрирования для внешних устройств

Создайте группу (см. раздел "Создание групп администрирования" на стр. [743](#)) внутри группы **Управляемые устройства**. Эта новая группа будет содержать внешние управляемые устройства.

e. Подключение шлюза соединения к Серверу администрирования

Настроенный вами шлюз соединения ожидает соединения от Сервера администрирования. Однако Сервер администрирования не перечисляет устройство со шлюзом соединения среди управляемых устройств. Это связано с тем, что шлюз соединения не пытался установить соединение с Сервером администрирования. Следовательно, вам потребуется особая процедура, чтобы Сервер администрирования инициировал соединение со шлюзом соединения.

Выполните следующие действия:

1. Добавьте шлюз соединения в качестве точки распространения (см. раздел "Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения" см. стр. [693](#)).
2. Переместите шлюз соединения (см. раздел "Перемещение устройств в состав группы администрирования" см. стр. [761](#)) из группы **Нераспределенные устройства** в группу, которую вы создали для внешних устройств.

Шлюз соединения подключен и настроен.

f. Подключение внешних настольных компьютеров к Серверу администрирования

Обычно внешние настольные компьютеры не перемещаются внутрь периметра сети. Поэтому вам необходимо настроить их для подключения (см. раздел "Подключение внешних настольных компьютеров к Серверу администрирования" см. стр. [302](#)) к Серверу администрирования через шлюз соединения при установке Агента администрирования.

g. Настройка обновлений для внешних настольных компьютеров

Если обновления приложений безопасности настроены на загрузку с Сервера администрирования, внешние компьютеры загружают обновления через шлюз соединения. Это имеет два недостатка:

- Это лишний трафик, занимающий пропускную способность интернет-канала компании.
- Это не обязательно самый быстрый способ получать обновления. Возможно для внешних компьютеров будет удобнее получать обновления с серверов обновлений "Лаборатории Касперского".

Выполните следующие действия:

1. Переместите все внешние компьютеры в отдельную группу администрирования, (см. раздел "Перемещение устройств в состав группы администрирования" см. стр. [761](#)) которую вы создали ранее.
2. Исключить группу с внешними устройствами из задачи обновления (см. раздел "Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства" см. стр. [482](#)).
3. Создайте отдельную задачу обновления для группы с внешними устройствами (см. раздел "Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства" см. стр. [482](#)).

h. Подключение ноутбуков к Серверу администрирования

Иногда ноутбуки находятся внутри сети, а в другое время – вне сети. Для эффективного управления вам необходимо, чтобы они по-разному подключались к Серверу администрирования в зависимости от своего местоположения. Для эффективного использования трафика им также необходимо получать обновления из разных источников в зависимости от их местоположения.

Вам необходимо настроить правила для автономных пользователей (см. раздел "О переключении Агента администрирования на другой Сервер администрирования" на стр. [307](#)): профили подключения (см. раздел "Создание профиля соединения для автономных пользователей" на стр. [304](#)) и описания сетевых расположений (см. раздел "Создание правила переключения Агента администрирования по сетевому местоположению" на стр. [308](#)). Каждое правило определяет экземпляр Сервера администрирования, к которому должны подключаться ноутбуки в зависимости от их местоположения, и экземпляр Сервера администрирования, с которого они должны получать обновления.

См. также:

Доступ из интернета: Использовать в качестве шлюза соединений в демилитаризованной зоне ..[146](#)

Сценарий: подключение автономных устройств через подчиненный Сервер администрирования в демилитаризованной зоне

Если вы хотите подключить управляемые устройства (см. раздел "О подключении автономных устройств" см. стр. [300](#)), расположенные вне основной сети, к Серверу администрирования, вы можете сделать это с помощью подчиненного Сервера администрирования, расположенного в демилитаризованной зоне (DMZ).

Предварительные требования

Прежде чем приступить, убедитесь, что вы выполнили следующее:

- В сети вашей организации организована демилитаризованная зона (DMZ).
- Сервер администрирования Kaspersky Security Center развернут во внутренней сети организации.

Этапы

Этот сценарий состоит из следующих этапов:

а. Выбор клиентского устройства в демилитаризованной зоне

В демилитаризованной зоне (DMZ) выберите клиентское устройство, которое будет использоваться в качестве подчиненного Сервера администрирования.

б. Установка Сервера администрирования Kaspersky Security Center.

Установите Сервер администрирования Kaspersky Security Center (см. раздел "Установка Kaspersky Security Center" на стр. [206](#)) на этом клиентском устройстве.

с. Создание иерархии Серверов администрирования

Если вы размещаете подчиненный Сервер администрирования в демилитаризованной зоне, подчиненный Сервер администрирования должен принимать подключение от главного Сервера администрирования. Для этого добавьте новый Сервер администрирования в качестве подчиненного Сервера так, чтобы главный Сервер подключался к подчиненному Серверу (см. раздел "Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне" на стр. [112](#)) по порту 13000. При объединении Серверов в иерархию (см. раздел "Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования" на стр. [700](#)) необходимо, чтобы порт 13291 обоих Серверов был доступен. Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования.

d. Подключение автономных управляемых устройств к подчиненному Серверу администрирования

Вы можете подключить автономные устройства к Серверу администрирования в демилитаризованной зоне аналогично тому, как устанавливается соединение между Сервером администрирования и управляемыми устройствами находящимися в основной сети (см. раздел "Подключение клиентских устройств к Серверу администрирования" см. стр. [748](#)). Автономные устройства иницируют подключение через порт 13000 (см. раздел "Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете" см. стр. [101](#)).

О подключении автономных устройств

Некоторые управляемые устройства, которые всегда находятся вне основной сети (например, компьютеры в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; компьютеры в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Некоторые устройства время от времени выходят за пределы периметра сети (например, ноутбуки пользователей, которые посещают региональные филиалы или офис клиента).

Вам по-прежнему необходимо отслеживать и управлять защитой устройств вне офиса – получать актуальную информацию об их статусе защиты и поддерживать приложения безопасности на них в актуальном состоянии. Это необходимо, например, потому, что если такое устройство будет скомпрометировано, находясь вдали от основной сети, то оно может стать платформой для распространения угроз, как только подключится к основной сети. Для подключения автономных устройств к Серверу администрирования вы можете использовать два способа:

- Шлюз соединения в демилитаризованной зоне (DMZ).
См. схему трафика данных: Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения (см. стр. [96](#)).
- Сервер администрирования в демилитаризованной зоне (DMZ)
См. схему трафика данных: Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете (см. стр. [101](#)).

Шлюз соединения в демилитаризованной зоне

Рекомендуемый способ подключения автономных устройств к Серверу администрирования это создание демилитаризованной зоны в сети организации и установка шлюза соединения (см. раздел "Шлюз соединения" см. стр. [54](#)) в демилитаризованной зоне. Внешние устройства будут подключаться к шлюзу соединения, а Сервер администрирования внутри сети иницирует подключение к устройствам через шлюз соединения.

По сравнению с другим способ этот является более безопасным:

- Вам не нужно открывать доступ к Серверу администрирования извне.
- Скомпрометированный шлюз соединения не представляет большого риска для безопасности сетевых устройств. Шлюз соединения ничем не управляет и не устанавливает никаких соединений.

Кроме того, шлюз соединения не требует много аппаратных ресурсов.

Однако этот способ имеет более сложный процесс настройки:

- Чтобы устройство выполняло роль шлюза соединения в демилитаризованной зоне, вам необходимо установить Агент администрирования и подключить его к Серверу администрирования особым образом.
- Вы не сможете использовать один и тот же адрес подключения к Серверу администрирования для ситуаций. С внешней стороны периметра вам нужно будет использовать не только другой адрес (адрес шлюза соединения), но и другой режим подключения: через шлюз соединения.
- Вам также необходимо определить разные параметры подключения для ноутбуков в разных месторасположениях.

► *Чтобы добавить шлюз соединения в ранее настроенную сеть:*

1. Установите Агент администрирования в режиме шлюза соединения.
2. Переустановите Агент администрирования на устройствах, которые вы хотите подключить к вновь добавленному шлюзу соединения.

Сервер администрирования в демилитаризованной зоне (DMZ)

Другой способ это установка единого Сервера администрирования в демилитаризованной зоне.

Эта конфигурация менее безопасна, чем конфигурация первого способа. В этом случае для управления внешними ноутбуками Сервер администрирования должен принимать соединения с любого адреса из интернета. Сервер администрирования управляет всеми устройствами во внутренней сети, но из демилитаризованной зоны. Поэтому скомпрометированный Сервер может нанести огромный ущерб, несмотря на низкую вероятность такого события.

Риск значительно снижается, если Сервер администрирования в демилитаризованной зоне не управляет устройствами внутренней сети. Такая конфигурация может использоваться, например, поставщиком услуг для управления устройствами клиентов.

Вы можете использовать этот способ в следующих случаях:

- Если вы знакомы с установкой и настройкой Сервера администрирования и не хотите выполнять другую процедуру по установке и настройке шлюза соединения.
- Если вам нужно управлять большим количеством устройств. Максимальное количество устройств, которыми может управлять Сервер администрирования – 100 000 устройств, шлюз соединения может поддерживать до 10 000 устройств.

Это решение также имеет некоторые сложности:

- Серверу администрирования требуется больше аппаратных ресурсов и еще одна база данных.
- Информация об устройствах будет храниться в двух несвязанных между собой базах данных (для Сервера администрирования внутри сети и другой в демилитаризованной зоне), что усложняет контроль.

- Для управления всеми устройствами Сервер администрирования необходимо объединить в иерархию, что усложняет и контроль и управление. Экземпляр подчиненного Сервера администрирования накладывает ограничения на возможные структуры групп администрирования. Вам нужно решить, как и какие задачи и политики распространять на подчиненный Сервер администрирования.
- Настройка внешних устройств для использования Сервера администрирования в демилитаризованной зоне извне и для использования главного Сервера администрирования изнутри не проще, чем настройка подключения через шлюз.
- Высокие риски безопасности. Скомпрометированный Сервер администрирования упрощает взлом управляемых ноутбуков. Если это произойдет, хакерам просто нужно дождаться, пока один из ноутбуков вернется в корпоративную сеть, чтобы продолжить атаку на локальную сеть.

См. также:

Сервер администрирования и два устройства в демилитаризованной зоне: шлюз соединений и клиентское устройство	114
Доступ из интернета: Использовать в качестве шлюза соединений в демилитаризованной зоне ..	146
Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете.....	101
Доступ из интернета: Сервер администрирования в демилитаризованной зоне.....	145
Шлюз соединения	54

Подключение внешних настольных компьютеров к Серверу администрирования

Настольные компьютеры, которые всегда находятся вне основной сети (например, компьютеры в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; компьютеры в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Они должны быть подключены к Серверу администрирования через шлюз соединения, установленный в демилитаризованной зоне (DMZ). Такая конфигурация выполняется при установке Агента администрирования на эти устройства.

► Чтобы подключить внешние настольные компьютеры к Серверу администрирования:

1. Создание инсталляционного пакета Агента администрирования (см. раздел "Создание инсталляционного пакета." на стр. [372](#)).
2. Откройте свойства созданного инсталляционного пакета, перейдите в раздел **Дополнительно** и выберите параметр **Подключаться к Серверу администрирования через шлюз соединения**.

Параметр **Подключаться к Серверу администрирования через шлюз соединения** несовместим с параметром **Использовать в качестве шлюза соединения в демилитаризованной зоне**. Вы не можете включить оба этих параметра одновременно.

3. Укажите адрес шлюза соединения в поле **Адрес шлюза соединений**.
Если шлюз соединения расположен за Network Address Translation (NAT) и не имеет собственного общедоступного адреса, настройте правило шлюза NAT для перенаправления соединений с общедоступного адреса на внутренний адрес шлюза соединения.

4. Создайте автономный инсталляционный пакет (см. раздел "Создание автономного инсталляционного пакета" на стр. [374](#)) на основе созданного инсталляционного пакета.
 5. Доставьте автономный инсталляционный пакет на целевые компьютеры в электронном виде или на съемном диске.
 6. Установите Агент администрирования из автономного инсталляционного пакета.
- К Серверу администрирования подключены внешние настольные компьютеры.

О профилях соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также "устройства"), может потребоваться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

Использование различных адресов одного и того же Сервера администрирования

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети организации, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования нужно добавить профиль для подключения к Серверу администрирования из интернета. Добавьте профиль в свойствах политики (раздел **Подключения**, вложенный раздел **Профили соединений**). В окне создания профиля необходимо выключить параметр **Использовать только для получения обновлений** и выбрать параметр **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center, описанной в разделе Доступ из интернета: Агент администрирования в качестве шлюза соединения (см. раздел "Доступ из интернета: Использовать в качестве шлюза соединений в демилитаризованной зоне" на стр. [146](#)) в демилитаризованной зоне), в профиле подключения следует указать адрес шлюза соединения в соответствующем поле.

Переключение между Серверами администрирования в зависимости от текущей сети

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования следует создать профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения следует указать адреса соответствующих Серверов администрирования и выбрать либо выключить параметр **Использовать только для получения обновлений**:

- выбрать параметр, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;

- выключить параметр, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая "домашний офис". Смысл каждого такого условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

См. также:

Предоставление доступа к Серверу администрирования из интернета	144
Доступ из интернета: Использовать в качестве шлюза соединений в демилитаризованной зоне ..	146
Создание профиля соединения для автономных пользователей	304

Создание профиля соединения для автономных пользователей

Подключение профиля Агента администрирования к Серверу администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

► Чтобы создать профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей:

1. В дереве консоли выберите группу администрирования для клиентских устройств, которой требуется создать профиль подключения Агента администрирования к Серверу.
2. Выполните одно из следующих действий:
 - Если вы хотите создать профиль подключения для всех устройств группы, в рабочей области группы на вкладке **Политики** выберите политику Агента администрирования. Откройте окно свойств выбранной политики.
 - Если вы хотите создать профиль подключения для выбранного устройства в составе группы, в рабочей области группы на вкладке **Устройства** выберите устройство и выполните следующие действия:
 - a. Откройте окно свойств выбранного устройства.
 - b. В разделе **Приложения** окна свойств устройства выберите Агент администрирования.
 - c. Откройте окно свойств Агента администрирования.
3. В окне свойств в разделе **Подключения** выберите вложенный раздел **Профили соединений**.
4. В блоке **Профили подключения к Серверу администрирования** нажмите на кнопку **Добавить**.

По умолчанию список профилей подключения содержит профили <Офлайн-режим> и <Домашний Сервер администрирования>. Профили недоступны для изменения и удаления.

В профиле <Офлайн-режим> не указывается Сервер для подключения. При переходе к этому профилю Агент администрирования не пытается подключиться к какому-либо Серверу, а установленные на клиентских устройствах приложения используют политики для автономных пользователей. Профиль <Офлайн-режим> применяется в условиях отключения устройств от сети.

В профиле <Домашний Сервер администрирования> указан Сервер для подключения, который был задан при установке Агента администрирования. Профиль <Домашний Сервер администрирования> применяется в условиях, когда устройство, которое работало в другой сети, вновь подключается к домашнему Серверу администрирования.

5. В открывшемся окне **Новый профиль** настройте параметры профиля подключения:

- **Название профиля.**

В поле ввода можно просмотреть или изменить имя профиля подключения.

- **Сервер администрирования**

Адрес Сервера администрирования, к которому должно подключаться клиентское устройство при активации профиля.

- **Порт**

Номер порта, по которому будет выполняться подключение.

- **SSL-порт**

Номер порта, по которому будет осуществляться подключение с использованием SSL-протокола.

- **Использовать SSL**

Если флажок установлен, подключение будет выполняться через защищенный порт (с использованием SSL-протокола).

По умолчанию флажок установлен.

- По ссылке **Настроить подключение через прокси-сервер** настройте параметры профиля подключения через прокси-сервер. Выберите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

- **Адрес прокси-сервера**

Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

- **Номер порта**

Номер порта, по которому будет выполняться подключение Kaspersky Security Center к прокси-серверу.

- **Аутентификация на прокси-сервере**

Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере. Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

- **Имя пользователя** (поле доступно, если выбран параметр **Аутентификация на прокси-сервере**)

Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль** (поле доступно, если выбран параметр **Аутентификация на прокси-сервере**)

Пароль пользователя, через учетную запись которого выполняется подключение к прокси-серверу.

- **Параметры шлюза соединения**

Адрес шлюза, через который устанавливается соединение клиентских устройств с Сервером администрирования.

- **Включить автономный режим**

Если флажок установлен, при подключении через этот профиль приложения, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. раздел "О переключении Агента администрирования на другой Сервер администрирования" на стр. [307](#)). В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

Если флажок снят, приложения будут использовать активные политики.

По умолчанию флажок снят.

- **Использовать только для получения обновлений**

Если флажок установлен, профиль будет использоваться только при загрузке обновлений приложениями, установленными на клиентском устройстве. Для остальных операций подключение к Серверу администрирования будет выполняться с исходными параметрами подключения, заданными при установке Агента администрирования.

По умолчанию флажок установлен.

- **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**

Если флажок установлен, Агент администрирования подключается к Серверу администрирования, используя параметры, указанные в свойствах профиля.

Если флажок снят, Агент администрирования подключается к Серверу используя исходные параметры, указанные при установке.

Флажок доступен, если флажок **Использовать только для получения обновлений** снят.

По умолчанию флажок снят.

6. Выберите параметр **Включить автономный режим, когда Сервер администрирования недоступен**, чтобы при подключении приложения, установленные на клиентском устройстве, использовали профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. раздел "О переключении Агента администрирования на другой Сервер администрирования" на стр. [307](#)), если Сервер администрирования недоступен. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

В результате будет создан профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей. При подключении Агента администрирования к Серверу через этот профиль приложения, установленные на клиентском устройстве, будут использовать политики для устройств, находящихся в автономном режиме, или политики для автономных пользователей.

См. также:

О профилях соединения для автономных пользователей[303](#)

О переключении Агента администрирования на другой Сервер администрирования

Исходные параметры подключения Агента администрирования к Серверу задаются при установке Агента администрирования. Для переключения Агента администрирования на другие Серверы администрирования можно использовать правила переключения (см. раздел «Создание правила переключения Агента администрирования по сетевому местоположению» на стр. [308](#)). Эта функция поддерживается только для Агентов администрирования, установленных на устройствах под управлением Windows или macOS (см. раздел «Аппаратные и программные требования» см. стр. [29](#)).

Правила переключения могут срабатывать при изменении следующих параметров сети:

- Адрес шлюза соединений по умолчанию.
- IP-адрес DHCP-сервера (Dynamic Host Configuration Protocol) в сети.
- DNS-суффикс подсети.
- IP-адрес DNS-сервера в сети.
- Доступность домена Windows. Этот параметр доступен только для устройств с операционными системами Windows.
- Адрес и маска подсети.
- IP-адрес DNS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.
- DNS-имя или NetBIOS-имя клиентского устройства.
- Доступность адреса SSL-соединения.

Если сформированы правила переключения Агента администрирования на другие Серверы администрирования, Агент реагирует на изменение параметров сети следующим образом:

- Если характеристики сети соответствуют одному из сформированных правил, Агент администрирования подключается к указанному в этом правиле Серверу администрирования. Если это задано правилом, установленные на клиентских устройствах приложения переходят на политики для автономных пользователей.
- Если ни одно из правил не выполняется, Агент администрирования возвращается к исходным параметрам подключения к Серверу администрирования, заданным при установке. Установленные на клиентских устройствах приложения возвращаются к активным политикам.
- Если Сервер администрирования недоступен, Агент администрирования использует политики для автономных пользователей.

Агент администрирования переключается на политику для автономных пользователей, только если параметр **Включить автономный режим, когда Сервер администрирования недоступен** (см. раздел **"Создание профиля соединения для автономных пользователей"** на стр. [304](#)) включен в параметрах политики Агента администрирования.

Параметры подключения Агента администрирования к Серверу администрирования сохраняются в профиле подключения. В профиле подключения вы можете создавать правила перехода клиентских устройств на политики для автономных пользователей, а также настраивать профиль таким образом, чтобы он использовался только для загрузки обновлений.

См. также

Создание правила активации профиля политики.....447

Создание правила переключения Агента администрирования по сетевому местоположению

Переключение Агента администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

► Чтобы создать правило для переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети:

1. В дереве консоли выберите группу администрирования, для устройств которой требуется создать правило переключения Агента администрирования по описанию сетевого местоположения.
2. Выполните одно из следующих действий:
 - Если вы хотите создать правило для всех устройств группы, в рабочей области группы на вкладке **Политики** выберите политику Агента администрирования. Откройте окно свойств выбранной политики.
 - Если вы хотите создать правило для выбранного устройства группы, в рабочей области группы на вкладке **Устройства** выберите устройство и выполните следующие действия:
 - a. Откройте окно свойств выбранного устройства.
 - b. В разделе **Приложения** окна свойств устройства выберите Агент администрирования.
 - c. Откройте окно свойств Агента администрирования.
3. В открывшемся окне **Свойства** в разделе **Подключения** выберите вложенный раздел **Профили соединений**.
4. В разделе **Параметры сетевого местоположения** нажмите на кнопку **Добавить**.
5. В открывшемся окне **Новое описание** настройте параметры описания сетевого местоположения и правила переключения. Настройте следующие параметры описания сетевого местоположения:

- **Имя описания сетевого местоположения**

Имя описания сетевого местоположения не может превышать 255 символов и содержать специальные символы ("*<>?V:|).

- **Использовать профиль подключения**

В раскрывающемся списке можно выбрать профиль подключения Агента администрирования к Серверу администрирования. Профиль будет использоваться при выполнении условий описания сетевого местоположения. Профиль подключения содержит параметры подключения Агента администрирования к Серверу администрирования и определяет переход клиентских устройств на политики для автономных пользователей. Профиль используется только для загрузки обновлений.

6. В блоке **Условия переключения** нажмите на кнопку **Добавить**, чтобы сформировать список условий описания сетевого местоположения.

Условия правила объединяются с использованием логического оператора AND. Чтобы правило переключения по описанию сетевого местоположения сработало, все условия переключения правила должны быть выполнены.

7. В раскрывающемся списке выберите значение, соответствующее изменению характеристики сети, к которой подключено клиентское устройство:

- **Адрес шлюза соединения по умолчанию** – изменение основного шлюза сети.
- **Адрес DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.
- **DNS-домен** – изменение DNS-суффикса подсети.
- **Адрес DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
- **Доступность Windows-домена (только Windows)** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Используйте этот параметр только для устройств под управлением Windows.
- **Подсеть** – изменение адреса и маски подсети.
- **Адрес WINS-сервера (только Windows)** – изменение IP-адреса WINS-сервера в сети. Используйте этот параметр только для устройств под управлением Windows.
- **Разрешимость имен** – у клиентского устройства изменилось NetBIOS-имя или DNS-имя.
- **Доступность адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с Сервером (имя:порт). Для каждого Сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат Сервера администрирования в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается.

8. В открывшемся окне укажите значение условия переключения Агента администрирования на другой Сервер администрирования. Название окна зависит от выбора значения на предыдущем шаге. Настройте следующие параметры условия переключения:

- **Значение**

В поле можно добавить одно или несколько значений для создаваемого условия.

- **Соответствует хотя бы одному значению списка**

Если выбран этот вариант, условие будет выполняться при любом из значений, указанных в списке **Значение**.

По умолчанию выбран этот вариант.

- **Не соответствует ни одному из значений списка**

Если выбран этот вариант, условие будет выполняться, если его значение отсутствует в списке **Значение**.

9. В окне **Новое описание** выберите параметр **Описание активно**, чтобы включить использование нового описания сетевого местоположения.

В результате будет создано правило переключения по описанию сетевого местоположения, при выполнении условий которого Агент администрирования будет использовать для подключения к Серверу администрирования указанный в описании профиль подключения.

Описания сетевого местоположения проверяются на соответствие характеристикам сети в том порядке, в котором они представлены в списке. Если характеристики сети соответствуют нескольким описаниям, будет использоваться  первое из них . Вы можете изменить порядок следования правил в списке с помощью кнопок **Вверх** () и **Вниз** ().

Уведомления о событиях

В этом разделе описано, как выбрать способ уведомления администратора о событиях на клиентских устройствах, а также как настроить параметры уведомления о событиях.

Кроме того, описано, как проверить распространение уведомлений о событиях с помощью тестового "вируса" Eicar.

В этом разделе

Настройка параметров уведомлений о событиях.....	311
Проверка распространения уведомлений.....	315
Уведомление о событиях с помощью исполняемого файла	316

Настройка параметров уведомлений о событиях

Kaspersky Security Center позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений:

- **Электронная почта.** При возникновении события приложение посылает уведомление на указанные адреса электронной почты. Вы можете настроить текст уведомления.
- **SMS.** При возникновении события приложение посылает уведомления на указанные номера телефонов. Вы можете настроить отправку SMS оповещений с помощью почтового шлюза.
- **Исполняемый файл.** При возникновении события на устройстве, исполняемый файл запускается на рабочем месте администратора. С помощью исполняемого файла администратор может получать параметры произошедшего события (см. раздел "Уведомление о событиях с помощью исполняемого файла" на стр. [316](#)).

► Чтобы настроить параметры уведомлений о событиях на клиентских устройствах:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Перейдите по ссылке **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.
Откроется окно **Свойства:События**.
4. В разделе **Уведомление** выберите способ уведомления (электронная почта, SMS, исполняемый файл для запуска) и настройте параметры уведомлений:

• **Электронная почта**

На вкладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой.

Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей. По умолчанию параметр выключен.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

Вам нужно указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

- Параметры TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, проверить срок действия сертификата Сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы решите использовать значение **Всегда использовать TLS, для проверки срока действия сертификата Сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы

разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать параметры TLS для SMTP-сервера:

- Выберите файл сертификата SMTP-сервера:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

Вам нужно указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер с сертификатом в формате PKCS#12:

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

Нажмите на кнопку **Отправить тестовое сообщение** можно проверить правильность настройки сообщений. Приложение отправляет тестовые сообщения на указанные адреса электронной почты.

- **SMS**

На вкладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной

почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

Если необходимо, вы можете указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

- Параметры TLS для SMTP-сервера

Вы можете отключить использование TLS, использовать TLS, если SMTP-сервер поддерживает этот протокол, или вы можете принудительно использовать только TLS. Если вы решите использовать только TLS, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также, если вы решили использовать только TLS, вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

- Выберите файл сертификата SMTP-сервера

Вы можете получить файл со списком сертификатов от аккредитованного центра сертификации и загрузить его в Kaspersky Security Center. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован. В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления. Приложение отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

Если выбран этот способ уведомления, в поле ввода можно указать, какое приложение будет запущено при возникновении события.

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения на указанные адреса электронной почты.

1. В поле **Текст уведомления** введите текст, который приложение будет отправлять при возникновении события.

Из раскрывающегося списка, расположенного справа от текстового поля, можно добавлять в сообщение подстановочные параметры с деталями события (например, описание события, время возникновения и прочее).

Если текст уведомления содержит символ %, нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

2. По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления.

Приложение отправляет тестовое уведомление указанному получателю.

3. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Можно изменить значения параметров уведомлений для определенных событий в разделе **Настройка событий** параметров Сервера администрирования, параметров политики (см. раздел «Общие параметры политик» см. стр. [788](#)) или параметров приложения (см. раздел «Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog» см. стр. [886](#)).

См. также:

Обработка и хранение событий на Сервере администрирования	717
Сценарий: мониторинг и отчеты	593

Проверка распространения уведомлений

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового "вируса" Eiscat на клиентских устройствах.

► *Чтобы проверить распространение уведомлений о событиях:*

1. Остановите задачу постоянной защиты файловой системы на клиентском устройстве и скопируйте тестовый "вирус" Eicar на клиентское устройство. Снова включите задачу постоянной защиты файловой системы.
2. Запустите задачу проверки клиентских устройств для группы администрирования или набора устройств, в который входит клиентское устройство с "вирусом" Eicar.

Если задача проверки настроена верно, в процессе ее выполнения тестовый "вирус" будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

В рабочей области узла **Сервер администрирования** на вкладке **События** в выборке **Последние события** отобразится запись об обнаружении "вируса".

Тестовый "вирус" Eicar не содержит программного кода, который может навредить вашему устройству. При этом большинство приложений безопасности компаний-производителей идентифицируют его как вирус. Загрузить тестовый «вирус» можно с официального веб-сайта организации EICAR <https://www.eicar.org>.

Уведомление о событиях с помощью исполняемого файла

Kaspersky Security Center позволяет с помощью запуска исполняемого файла уведомлять администратора о событиях на клиентских устройствах. Исполняемый файл должен содержать другой исполняемый файл с подстановочными параметрами события, которые нужно передать администратору.

Таблица 57. Подстановочные параметры для описания события

Подстановочный параметр	Описание подстановочного параметра
%SEVERITY%	Уровень важности события
%COMPUTER%	Имя устройства, на котором произошло событие
%DOMAIN%	Домен
%EVENT%	Событие
%DESCR%	Описание события
%RISE_TIME%	Время возникновения
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Имя задачи
%KL_PRODUCT%	Агент администрирования
%KL_VERSION%	Номер версии Агента администрирования
%HOST_IP%	IP-адрес
%HOST_CONN_IP%	IP-адрес соединения

Пример:

Для уведомления о событии используется исполняемый файл (например, script1.bat), внутри которого запускается другой исполняемый файл (например, script2.bat) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл script1.bat, который, в свою очередь, запустит файл script2.bat с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

Шифрование подключения TLS

Чтобы закрыть уязвимости в сети вашей организации, вы можете включить шифрование трафика с использованием TLS-протокола. Вы можете включить протоколы шифрования TLS и поддерживаемые наборы шифрования на Сервере администрирования и Сервере iOS MDM. Kaspersky Security Center поддерживает TLS-протокол версий 1.0, 1.1, 1.2 и 1.3. Вы можете выбрать требуемый протокол шифрования и наборы шифрования.

Kaspersky Security Center использует самоподписанные сертификаты. Дополнительная настройка для iOS-устройств не требуется. Также вы можете использовать ваши собственные сертификаты. Рекомендуется использовать сертификаты, подписанные аккредитованным центром сертификации.

Сервер администрирования

- Чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования:

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Используйте флаг SrvUseStrictSslSettings, чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования. Введите следующую команду:

```
klscflag -fset -pv ".core/.independent" -s Transport -n  
SrvUseStrictSslSettings -v <value> -t d
```

Укажите параметр <value> флага SrvUseStrictSslSettings:

- 4 – включены только TLS-протоколы версий 1.2 и 1.3. Также включены наборы шифрования с TLS_RSA_WITH_AES_256_GCM_SHA384 (эти наборы шифрования необходимы для обратной совместимости с предыдущими версиями Kaspersky Security Center). Это значение по умолчанию.

Наборы шифрования поддерживаемые TLS-протоколом 1.2:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- AES256-GCM-SHA384 (с набором шифрования TLS_RSA_WITH_AES_256_GCM_SHA384)
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Наборы шифрования поддерживаемые TLS-протоколом 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

- 5 – включены только TLS-протоколы версий 1.2 и 1.3. Для TLS-протоколов версий 1.2 и 1.3 поддерживаются определенные наборы шифрования, перечисленные ниже.

Наборы шифрования поддерживаемые TLS-протоколом 1.2:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Наборы шифрования поддерживаемые TLS-протоколом 1.3:

- TLS_AES_256_GCM_SHA384

- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Не рекомендуется использовать значения 0, 1, 2 или 3 для значений параметра флага SrvUseStrictSslSettings. Эти значения параметров соответствуют небезопасным версиям TLS-протокола (протоколы TLS 1.0 и TLS 1.1) и небезопасным наборам шифрования и используются только для обратной совместимости с более ранними версиями Kaspersky Security Center.

3. Перезапустите следующие службы Kaspersky Security Center:

- службу Сервера администрирования;
- службу Веб-сервера;
- службу активации прокси-сервера.

Включается шифрование трафика с помощью TLS-протокола.

Вы можете использовать флаги KLTR_TLS12_ENABLED и KLTR_TLS13_ENABLED, чтобы включить поддержку TLS-протоколов 1.2 и 1.3 соответственно. Эти флаги включены по умолчанию.

► Чтобы включить или выключить поддержку TLS-протоколов 1.2 и 1.3:

1. Запустите утилиту klscflag.

Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Введите одну из следующих команд в командной строке Windows с правами администратора:

- Используйте эту команду, чтобы включить или выключить поддержку TLS-протокола 1.2:

```
klscflag -fset -pv ".core/.independent" -s Transport -n  
KLTR_TLS12_ENABLED -v <value> -t d
```

- Используйте эту команду, чтобы включить или выключить поддержку TLS-протокола 1.3:

```
klscflag -fset -pv ".core/.independent" -s Transport -n  
KLTR_TLS13_ENABLED -v <value> -t d
```

Укажите параметр <value> флага:

- 1 – чтобы включить поддержку TLS-протокола.
- 0 – чтобы выключить поддержку TLS-протокола.

Сервер iOS MDM

Соединение между iOS-устройствами и Сервером iOS MDM зашифровано.

► *Чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере iOS MDM:*

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер iOS MDM, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
 - для 32-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLiOSMDM\1.0.0.0\Conset
 - для 64-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\Connectors\KLiOSMDM\1.0.0.0\Conset
3. Создайте ключ с именем `StrictSslSettings`.
4. Укажите тип ключа `DWORD`.
5. Установите значение ключа:
 - 2 – включены протоколы TLS 1.0, TLS 1.1 и TLS 1.2.
 - 3 – включен только протокол TLS 1.2 (значение по умолчанию).
6. Перезапустите службу Сервера iOS MDM Kaspersky Security Center.

Настройка интерфейса

Вы можете настроить интерфейс Kaspersky Security Center:

- Отобразить и скрыть объекты в дереве консоли, рабочей области и окнах свойств объектов (папок, разделов) в зависимости от используемых функций.
- Отобразить и скрыть элементы главного окна (например, дерево консоли или стандартные меню, такие как **Действия** и **Вид**).

► *Чтобы настроить интерфейс Kaspersky Security Center в соответствии с используемым в настоящее время набором функций, выберите следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В меню главного окна приложения выберите пункт **Вид** → **Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса**, настройте отображение элементов интерфейса, используя следующие флажки:

- **Отображать Системное администрирование**

Если флажок установлен, в папке **Удаленная установка** отображается вложенная папка **Развертывание образов устройств**, а в папке **Хранилища** отображается вложенная папка **Оборудование**.

По умолчанию флажок снят.

- **Отображать шифрование и защиту данных**

Если флажок установлен, доступно управление шифрованием данных на

устройствах, подключаемых к сети. После перезапуска приложения в дереве консоли отобразится папка **Шифрование и защита данных**.

По умолчанию флажок установлен.

- **Отображать параметры контроля рабочего места**

Если флажок установлен, в разделе **Контроль безопасности** окна свойств политики Kaspersky Endpoint Security 10 для Windows отображаются следующие подразделы:

- **Контроль приложений;**
- **Мониторинг уязвимостей;**
- **Контроль устройств;**
- **Веб-Контроль.**

Если флажок снят, указанные выше подразделы не отображаются в разделе **Контроль безопасности**.

По умолчанию флажок снят.

- **Отображать Управление мобильными устройствами**

Если флажок установлен, доступна функциональность **Управление мобильными устройствами**. После перезапуска приложения в дереве консоли отобразится папка **Мобильные устройства**.

По умолчанию флажок снят.

- **Отображать подчиненные Серверы администрирования**

Если флажок установлен, в дереве консоли отображаются узлы подчиненных и виртуальных Серверов администрирования в составе групп администрирования. При этом доступна функциональность, связанная с подчиненными и виртуальными Серверами администрирования (например, создание задач удаленной установки приложений на подчиненные Серверы администрирования).

По умолчанию флажок установлен.

- **Отображать разделы с параметрами безопасности**

Если флажок установлен, в окнах свойств Сервера администрирования, групп администрирования и других объектов будет отображаться раздел **Безопасность**. Это позволит предоставлять пользователям и группам пользователей права на работу с объектами, отличные от заданных по умолчанию.

По умолчанию флажок установлен.

4. Нажмите на кнопку **ОК**.

Чтобы применить некоторые изменения, вам нужно закрыть главное окно приложения, а затем открыть его снова.

► *Чтобы настроить отображение элементов в главном окне приложения:*

1. В меню главного окна приложения выберите **Вид → Настроить**.
2. В открывшемся окне **Настройка вида** настройте отображение элементов главного окна с помощью флажков.

3. Нажмите на кнопку **ОК**.

Обнаружение устройств в сети

В этом разделе описаны шаги, которые вам нужно выполнить после установки Kaspersky Security Center.

В этом разделе

Сценарий: обнаружение сетевых устройств	322
Нераспределенные устройства	323
Инвентаризация оборудования	338

Сценарий: обнаружение сетевых устройств

Вам нужно выполнить поиск устройств перед установкой приложений безопасности. Сервер администрирования получает информацию об обнаруженных устройствах и позволяет управлять устройствами с помощью политик. Регулярные опросы сети необходимы для обновления списка устройств, доступных в сети.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Обнаружение сетевых устройств содержит следующие этапы:

а. Обнаружение устройств

Мастер первоначальной настройки выполняет начальное обнаружение устройств (см. раздел "Шаг 12. Обнаружение устройств" на стр. [295](#)) и помогает найти сетевые устройства, такие как компьютеры, планшеты и мобильные телефоны. Вы можете также запустить обнаружение устройств вручную (см. раздел "Обнаружение устройств" на стр. [324](#)).

б. Настройка расписания опросов

Определите, какой тип опроса (см. раздел "Обнаружение устройств" на стр. [324](#)) вы хотите регулярно использовать. Включите нужные типы опроса и настройте необходимое расписание опроса. Также см. рекомендации по частоте опроса сети.

в. Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)

Новые устройства появляются в сети в результате их обнаружения при опросах сети. Они автоматически попадают в группу **Нераспределенные устройства**. Можно настроить правила перемещения устройств, в соответствии с которыми устройства будут распределены в группу **Управляемые устройства**. Можно также настроить правила хранения (см. раздел "Настройка правил хранения для нераспределенных устройств" на стр. [332](#)).

Если вы пропустили шаг 3, список новых обнаруженных устройств располагается в группе **Нераспределенные устройства**. Вы можете переместить эти устройства в группу **Управляемые устройства** вручную. Если вы вручную переместили устройства в группу **Управляемые устройства**, вы можете проанализировать информацию о каждом из устройств и решить, требуется ли переместить его в группу администрирования и в какую.

Результаты

Завершение сценария дает следующее:

- Сервер администрирования Kaspersky Security Center обнаруживает устройства в сети и предоставляет информацию о них.
- Настроены будущие опросы сети и расписание их запуска.
- Новые обнаруженные устройства распределены в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

См. также:

Порты, используемые Kaspersky Security Center	63
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения	104
Основные понятия	39
Архитектура приложения	56

Нераспределенные устройства

В этом разделе представлена информация о работе с устройствами сети организации, не входящими в группы администрирования.

См. также:

Сценарий: обнаружение сетевых устройств	322
Основной сценарий установки.....	56
В этом разделе	
Обнаружение устройств	324
Работа с Windows-доменами Просмотр и изменение параметров домена	332
Настройка правил хранения для нераспределенных устройств	332
Работа с IP-диапазонами	333
Работа с группами Active Directory. Просмотр и изменение параметров группы	335
Создание правил автоматического перемещения устройств в группы администрирования	335
Использование динамического режима VDI на клиентских устройствах	335

Обнаружение устройств

В этом разделе описаны типы обнаружения устройств, доступные в Kaspersky Security Center, а также приведена информация об использовании каждого из них.

Во время регулярных опросов сети Сервер администрирования получает информацию о структуре сети и устройствах в сети. Данные записываются в базу данных Сервера администрирования. Сервер администрирования может проводить следующие типы опросов сети:

- **Опрос сети Windows.** Сервер администрирования может проводить два типа опросов сети Windows: быстрый и полный. При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. При полном опросе с каждого клиентского устройства запрашивается более подробная информация, например, имя операционной системы, IP-адрес, DNS-имя и NetBIOS-имя. По умолчанию включены быстрый и полный опрос. При опросе сети Windows может не удастся обнаружить устройства, например, если роутером или сетевым экраном закрыты порты UDP 137, UDP 138, TCP 139.
- **Опрос Active Directory.** Сервер администрирования получает информацию о структуре групп Active Directory, а также информацию о DNS-именах устройств, входящих в группы Active Directory. По умолчанию этот тип опроса включен. При использовании Active Directory рекомендуется использовать опрос Active Directory. В противном случае Сервер администрирования не сможет обнаружить устройства. Если используется Active Directory, но отдельные сетевые устройства не являются его членами, эти устройства не удастся обнаружить при опросе Active Directory.
- **Опрос IP-диапазонов.** Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов или NBNS-протоколов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows и/или опрос Active Directory.
- **Опрос Zeroconf.** Точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией <http://www.zeroconf.org/> (далее также *Zeroconf*). По умолчанию этот тип опроса

выключен. Вы можете использовать опрос Zeroconf, если точка распространения работает под управлением Linux.

Если вы настроили и включили правила перемещения устройств, новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства**. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Можно изменить параметры обнаружения устройств для каждого типа. Например, может потребоваться изменить расписание опроса или указать, нужно опрашивать весь лес доменов или только определенный домен.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

См. также:

Сценарий: обнаружение сетевых устройств	322
Основной сценарий установки.....	56

В этом разделе

Опрос сети Windows	325
Опрос Active Directory	328
Опрос IP-диапазонов	330
Опрос Zeroconf	331

Опрос сети Windows

Об опросе сети Windows

При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация:

- Имя операционной системы
- IP-адрес
- DNS-имя
- NetBIOS-имя

Как во время быстрого опроса, так и во время полного опроса необходимо:

- наличие открытых портов UDP 137/138, TCP 139, UDP 445, TCP 445;
- SMB-протокол включен;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на Сервере администрирования;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на клиентском устройстве:
 - наличие хотя бы одного устройства, если количество сетевых устройств не превышает 32;
 - наличие как минимум одного устройства на каждые 32 сетевых устройства.

Полный опрос сети может быть запущен, только если быстрый опрос был запущен как минимум один раз.

Просмотр и изменение параметров опроса сети Windows

► Чтобы изменить параметры опроса сети Windows:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Домены**.

Вы можете перейти в папку **Обнаружение устройств** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

В рабочей области подпапки **Домены** отображается список устройств.

2. Нажмите на кнопку **Опросить сейчас**.

Откроется окно свойств домена. При необходимости настройте параметры опроса сети Windows:

- **Включить опрос сети Windows**

По умолчанию этот вариант выбран. Если не требуется выполнять опрос сети Windows (например, если достаточно опроса Active Directory), можно отменить выбор данного параметра.

- **Настроить расписание быстрого опроса**

По умолчанию интервал времени составляет 15 минут.

При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети.

Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

Доступны следующие варианты расписания опроса сети:

- **Каждые N дней**

Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **Каждые N минут**

Задайте интервал, с которым повторяется опрос (в минутах), и время начала первого запуска опроса за сутки.

- **По дням недели**

Установите флажки у тех дней недели, в которые должен запускаться опрос, и

укажите время начала опроса.

- **Ежемесячно, в указанные дни выбранных недель**

Установите флажки у тех недель и дней, в которые должен запускаться опрос, и укажите время начала опроса.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

- **Настроить расписание полного опроса**

По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

Доступны следующие варианты расписания опроса сети:

- **Каждые N дней**

Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **Каждые N минут**

Задайте интервал, с которым повторяется опрос (в минутах), и время начала первого запуска опроса за сутки.

- **По дням недели**

Установите флажки у тех дней недели, в которые должен запускаться опрос, и укажите время начала опроса.

- **Ежемесячно, в указанные дни выбранных недель**

Установите флажки у тех недель и дней, в которые должен запускаться опрос, и укажите время начала опроса.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**. Будут запущены оба типа опроса.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса сети Windows осуществляется в окне свойств точки распространения, в разделе **Обнаружение устройств**.

См. также:

Работа с Windows-доменами Просмотр и изменение параметров домена	332
Сценарий: обнаружение сетевых устройств	322

Опрос Active Directory

Используйте опрос Active Directory, если вы используете Active Directory; в противном случае рекомендуется использовать другие типы опросов. Если используется Active Directory, но отдельные сетевые устройства не являются его членами, эти устройства не удастся обнаружить при опросе Active Directory.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Просмотр и изменение параметров опроса Active Directory

► Чтобы просмотреть и изменить параметры опроса групп Active Directory:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Active Directory**.
Также вы можете перейти в папку **Обнаружение устройств** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

2. Нажмите на кнопку **Настроить параметры опроса**.

В результате откроется окно свойств Active Directory. При необходимости настройте параметры опроса групп Active Directory:

- **Разрешить опрос Active Directory**

По умолчанию этот вариант выбран. Однако если Active Directory не используется, в результаты опроса ничего найдено не будет. В этом случае можно отменить выбор данного параметра.

- **Настроить расписание опроса**

По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

Доступны следующие варианты расписания опроса сети:

- **Каждые N дней**

Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **Каждые N минут**

Задайте интервал, с которым повторяется опрос (в минутах), и время начала первого запуска опроса за сутки.

- **По дням недели**

Установите флажки у тех дней недели, в которые должен запускаться опрос, и укажите время начала опроса.

- **Ежемесячно, в указанные дни выбранных недель**

Установите флажки у тех недель и дней, в которые должен запускаться опрос, и укажите время начала опроса.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

- **Дополнительно**

Можно выбрать домены Active Directory для опроса:

- Домен Active Directory, к которому относится Kaspersky Security Center.
- Лес доменов, к которому относится Kaspersky Security Center.
- Указанный список доменов Active Directory.

При выборе этого параметра можно добавлять домены в область опроса:

- Нажмите на кнопку **Добавить**.
- В соответствующих полях укажите адрес доменного контроллера, а также имя и пароль учетной записи для доступа к нему.
- Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Можно выбрать адрес доменного контроллера в списке и нажать на кнопку **Изменить** или **Удалить**, чтобы изменить или удалить его.

- Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса групп Active Directory осуществляются в окне свойств (см. раздел "Параметры политики Агента администрирования" см. стр. 789) точки распространения, в разделе **Обнаружение устройств**.

См. также:

Сценарий: обнаружение сетевых устройств [322](#)

Опрос IP-диапазонов

Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов или NBNS-протоколов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows и/или опрос Active Directory.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Просмотр и изменение параметров опроса IP-диапазонов

► Чтобы просмотреть и изменить параметры опроса групп IP-диапазона:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.
Вы можете перейти в папку **Нераспределенные устройства** из папки **Обнаружение устройств** по кнопке **Опросить сейчас**.
2. Если вы хотите, в подпапке **IP-диапазоны** нажмите на кнопку **Добавить подсеть**, чтобы добавить IP-диапазон (см. раздел "Работа с IP-диапазонами" на стр. 333) для опроса, а затем нажмите **ОК**.
3. Нажмите на кнопку **Настроить параметры опроса**.

Откроется окно свойств IP-диапазонов. Если требуется, можно поменять параметры опроса IP-диапазонов:

- **Разрешить опрос IP-диапазона**

По умолчанию этот вариант не выбран. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows и/или опрос Active Directory.

- **Настроить расписание опроса**

По умолчанию интервал времени составляет 420 минут. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

Доступны следующие варианты расписания опроса сети:

- **Каждые N дней**

Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **Каждые N минут**

Задайте интервал, с которым повторяется опрос (в минутах), и время начала первого запуска опроса за сутки.

- **По дням недели**

Установите флажки у тех дней недели, в которые должен запускаться опрос, и укажите время начала опроса.

- **Ежемесячно, в указанные дни выбранных недель**

Установите флажки у тех недель и дней, в которые должен запускаться опрос, и укажите время начала опроса.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**. Эта кнопка доступна, только если выбран параметр **Разрешить опрос IP-диапазона**.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса IP-диапазонов осуществляются в окне свойств (см. раздел "Параметры политики Агента администрирования" см. стр. 789) точки распространения, в разделе **Обнаружение устройств**. Клиентские устройства, найденные в результате опроса IP-диапазонов, отображаются в папке **Домены** виртуального Сервера.

См. также:

Сценарий: обнаружение сетевых устройств[322](#)

Опрос Zeroconf

Этот тип опроса поддерживается только для точек распространения с операционными системами Linux.

Точка распространения может опрашивать сети, в которых есть устройства с IPv6-адресами. В этом случае IP-диапазоны не указываются, и точка распространения опрашивает всю сеть, используя сеть с нулевой конфигурацией <http://www.zeroconf.org/> (далее также *Zeroconf*). Чтобы начать использовать Zeroconf, вам нужно установить утилиту avahi-browse на точке распространения.

► *Чтобы включить опрос Zeroconf:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.
Вы можете перейти в папку **Нераспределенные устройства** из папки **Обнаружение устройств** по кнопке **Опросить сейчас**.
2. Нажмите на кнопку **Настроить параметры опроса**.
3. В открывшемся окне свойств IP-диапазонов выберите **Включить опрос с помощью технологии Zeroconf**.

После этого точка распространения начинает опрашивать вашу сеть. В этом случае указанные IP-диапазоны игнорируются.

Работа с Windows-доменами Просмотр и изменение параметров домена

► *Чтобы изменить параметры домена:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Домены**.
2. Выберите домен и откройте окно его свойств одним из следующих способов:
 - В контекстном меню домена выберите пункт **Свойства**.
 - По ссылке **Показать свойства группы**.

В открывшемся окне **Свойства: <Имя домена>** можно настроить параметры выбранного домена.

См. также:

Сценарий: обнаружение сетевых устройств[322](#)

Настройка правил хранения для нераспределенных устройств

После того как опрос сети Windows завершен, обнаруженные устройства помещаются в подгруппы группы администрирования Нераспределенные устройства. Эта группа администрирования находится по следующему пути: **Дополнительно** → **Обнаружение устройств** → **Домены**. Папка **Домены** является родительской группой. Папка содержит дочерние группы, имена которых соответствуют доменам и рабочим группам, которые были обнаружены во время опроса сети. Родительская группа может также содержать группы администрирования мобильных устройств. Вы можете настроить правила хранения нераспределенных устройств для родительской группы администрирования и для каждой дочерней группы. Правила хранения не зависят от параметров опроса сети и работают, даже если опрос сети выключен.

► *Чтобы настроить правила хранения нераспределенных устройств:*

1. В дереве консоли в папке **Обнаружение устройств** выполните одно из следующих действий:

- Чтобы настроить параметры родительской группы, в контекстном меню папки **Домены** выберите пункт **Свойства**.

Откроется окно свойств родительской группы.

- Чтобы настроить параметры дочерней группы, в контекстном меню дочерней группы выберите пункт **Свойства**.

Откроется окно свойств дочерней группы.

2. В разделе **Устройства** укажите следующие параметры:

- **Удалять устройство из группы, если оно неактивно больше (сут)**

Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. По умолчанию этот параметр распространяется на дочерние группы. Временной интервал, установленный по умолчанию, составляет 7 дней.

По умолчанию параметр включен.

- **Наследовать из родительской группы**

Если этот параметр включен, период хранения для устройств в текущей группе наследуется от родительской группы и не может быть изменен.

Этот параметр доступен только для дочерних групп.

По умолчанию параметр включен.

- **Обеспечить принудительное наследование для дочерних групп**

Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

По умолчанию параметр выключен.

Ваши изменения сохранены и применены.

См. также:

Сценарий: обнаружение сетевых устройств[322](#)

Работа с IP-диапазонами

Вы можете настраивать параметры существующих IP-диапазонов, а также создавать новые IP-диапазоны.

См. также:

Сценарий: обнаружение сетевых устройств	322
В этом разделе	
Создание IP-диапазона	334
Просмотр и изменение параметров IP-диапазона	334

Создание IP-диапазона

► Чтобы создать IP-диапазон:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.
 2. В контекстном меню папки выберите пункт **Новый** → **IP-диапазон**.
 3. В открывшемся окне **Новый IP-диапазон** настройте параметры создаваемого IP-диапазона.
- В результате созданный IP-диапазон появится в составе папки **IP-диапазоны**.

См. также:

Сценарий: обнаружение сетевых устройств	322

Просмотр и изменение параметров IP-диапазона

► Чтобы изменить параметры IP-диапазона:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.
2. Выберите IP-диапазон и откройте окно его свойств одним из следующих способов:
 - В контекстном меню IP-диапазона выберите пункт **Свойства**.
 - По ссылке **Показать свойства группы**.

В открывшемся окне **Свойства: <Название IP-диапазона>** можно настроить параметры выбранного IP-диапазона.

См. также:

Сценарий: обнаружение сетевых устройств	322

Работа с группами Active Directory. Просмотр и изменение параметров группы

► Чтобы изменить параметры группы Active Directory:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Active Directory**.
2. Выберите группу Active Directory и откройте окно ее свойств одним из следующих способов:
 - В контекстном меню IP-диапазона выберите пункт **Свойства**.
 - По ссылке **Показать свойства группы**.

В открывшемся окне **Свойства: <Название группы Active Directory>** можно настроить параметры выбранной группы Active Directory.

См. также:

Сценарий: обнаружение сетевых устройств[322](#)

Создание правил автоматического перемещения устройств в группы администрирования

Вы можете настроить автоматическое перемещение устройств, обнаруживаемых при опросе сети организации, в группы администрирования.

► Чтобы настроить правила автоматического перемещения устройств в группы администрирования:

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В рабочей области папки нажмите на кнопку **Настроить правила**.

Откроется окно **Свойства:Нераспределенные устройства** устройства. Настройте правила автоматического перемещения устройств в группы администрирования в разделе **Перемещение устройств**.

На устройстве будет выполнено первое применимое правило в списке (сверху вниз в списке).

См. также:

Сценарий: обнаружение сетевых устройств[322](#)

Использование динамического режима VDI на клиентских устройствах

В сети организации может быть развернута виртуальная инфраструктура с использованием временных виртуальных машин. Kaspersky Security Center обнаруживает временные виртуальные машины и добавляет данные о них в базу данных Сервера администрирования. После завершения работы пользователя с временной виртуальной машиной машина удаляется из виртуальной инфраструктуры. Однако запись об

удаленной виртуальной машине может сохраниться в базе данных Сервера администрирования. Кроме того, несуществующие виртуальные машины могут отображаться в Консоли администрирования.

Чтобы избежать сохранения данных о несуществующих виртуальных машинах, в Kaspersky Security Center реализована поддержка динамического режима для Virtual Desktop Infrastructure (VDI). Администратор может включить поддержку динамического режима для VDI (см. раздел "Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования" на стр. [336](#)) в свойствах инсталляционного пакета Агента администрирования (см. раздел "Параметры инсталляционного пакета Агента администрирования" на стр. [201](#)), который будет установлен на временной виртуальной машине.

Во время выключения временной виртуальной машины Агент администрирования информирует Сервер администрирования о выключении. В случае успешного выключения виртуальной машины, она удаляется из списка устройств, подключенных к Серверу администрирования. Если выключение виртуальной машины выполнено некорректно и Агент администрирования не послал Серверу уведомление о выключении, используется дублирующий сценарий. Согласно этому сценарию виртуальная машина удаляется из списка устройств, подключенных к Серверу администрирования, после трех неудачных попыток синхронизации с Сервером.

См. также:

Сценарий: обнаружение сетевых устройств[322](#)

В этом разделе

Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования[336](#)

Поиск устройств, являющихся частью VDI[337](#)

Перемещение в группу администрирования устройств, являющихся частью VDI[337](#)

Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования

► Чтобы включить динамический режим VDI:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.
Откроется окно **Свойства: Агент администрирования Kaspersky Security Center**.
3. В окне **Свойства: Агент администрирования Kaspersky Security Center** выберите раздел **Дополнительно**.
4. В разделе **Дополнительно** выберите параметр **Включить динамический режим для VDI**.
Устройство, на которое устанавливается Агент администрирования, будет являться частью VDI.

См. также:

Сценарий: обнаружение сетевых устройств[322](#)

Поиск устройств, являющихся частью VDI

► Чтобы найти нераспределенные устройства, являющиеся частью VDI:

1. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Поиск**.
Чтобы просмотреть список всех устройств, входящих в Virtual Desktop Infrastructure (VDI), в контекстном меню папки **Сервер администрирования** выберите пункт **Поиск**.
2. В окне **Поиск** на вкладке **Виртуальные машины** выберите **Да** в блоке параметров **Часть Virtual Desktop Infrastructure**.
3. Нажмите на кнопку **Найти**.

Отобразится список нераспределенных устройств, которые являются частью Virtual Desktop Infrastructure (VDI).

См. также:

Перемещение в группу администрирования устройств, являющихся частью VDI[337](#)

Сценарий: обнаружение сетевых устройств[322](#)

Перемещение в группу администрирования устройств, являющихся частью VDI

► Чтобы переместить устройства, являющиеся частью VDI, в группу администрирования:

1. В рабочей области папки **Нераспределенные устройства** нажмите на кнопку **Настроить правила**.
В результате откроется окно свойств папки **Нераспределенные устройства**.
2. В окне свойств папки **Нераспределенные устройства** в разделе **Перемещение устройств** нажмите на кнопку **Добавить**.
Откроется окно **Новое правило**.
3. В окне **Новое правило** выберите раздел **Виртуальные машины**.
4. В раскрывающемся списке **Является виртуальной машиной** выберите **Да**.
Будет создано правило перемещения устройств в группу администрирования.

См. также:

Сценарий: обнаружение сетевых устройств[322](#)

Инвентаризация оборудования

В списке оборудования (**Хранилища** → **Оборудование**), который вы используете для инвентаризации оборудования, заполняется двумя способами: автоматически и вручную. После каждого опроса сети все обнаруженные компьютеры автоматически добавляются в список; однако вы также можете добавить компьютеры вручную, если не хотите опрашивать сеть. Вы можете добавить другие устройства в список вручную, например, маршрутизаторы, принтеры или компьютерное оборудование.

В свойствах устройства можно просматривать и редактировать подробную информацию об устройствах.

В списке оборудования могут присутствовать следующие типы устройств:

- компьютеры;
- мобильные устройства;
- сетевые устройства;
- виртуальные устройства;
- компьютерные комплектующие;
- компьютерная периферия;
- подключаемые устройства;
- VoIP-телефоны;
- сетевые хранилища.

Администратор может присваивать обнаруженным устройствам признак *Корпоративное оборудование*. Этот признак можно присвоить в свойствах устройства вручную или задать критерии для его автоматического присвоения. В этом случае признак *Корпоративное оборудование* присваивается по типу устройства.

Kaspersky Security Center позволяет выполнять списание оборудования. Для этого в свойствах устройства необходимо выбрать параметр **Устройство списано**. Такое устройство не отображается в списке оборудования.

Администратор может работать со списком программируемых логических контроллеров (ПЛК) в папке **Оборудование**. Подробная информация о работе со списками ПЛК приведена в *Руководстве пользователя Kaspersky Industrial CyberSecurity for Nodes*.

См. также:

Сценарий: обнаружение сетевых устройств [322](#)

В этом разделе

Добавление информации о новых устройствах [339](#)

Настройка критериев определения корпоративных устройств [339](#)

Настройка пользовательских полей [340](#)

Добавление информации о новых устройствах

► Чтобы добавить информацию о новых устройствах в сети:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** по кнопке **Добавить устройство** откройте окно **Новое устройство**.
Откроется окно **Новое устройство**.
3. В окне **Новое устройство** в раскрывающемся списке **Тип** выберите тип устройства, которое вы хотите добавить.
4. Нажмите на кнопку **ОК**.
Откроется окно свойств устройства на разделе **Общие**.
5. В разделе **Общие** заполните поля ввода данными об устройстве. В разделе **Общие** доступны следующие параметры:
 - **Корпоративное устройство**. Установите флажок, если вы хотите присвоить устройству признак *Корпоративное*. По этому признаку можно выполнять поиск устройств в папке **Оборудование**.
 - **Устройство списано**. Установите флажок, если вы не хотите, чтобы устройство отображалось в списке устройств в папке **Оборудование**.
6. Нажмите на кнопку **Применить**.
Новое устройство отобразится в рабочей области папки **Оборудование**.

См. также:

Сценарий: обнаружение сетевых устройств	322
Инвентаризация оборудования	338

Настройка критериев определения корпоративных устройств

► Чтобы настроить критерии определения корпоративных устройств:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Настроить критерии определения корпоративных устройств**.
Откроется окно свойств оборудования.
3. В окне свойств оборудования в разделе **Корпоративные устройства** выберите способ присвоения устройству признака *Корпоративное*:
 - **Вручную устанавливать для устройства признак "Корпоративное"**. Признак *Корпоративное оборудование* назначается устройству вручную в окне свойств устройства в разделе **Общие**.
 - **Автоматически устанавливать для устройства признак "Корпоративное"**. В блоке параметров **По типу устройства** укажите типы устройств, которым приложение будет автоматически присваивать признак *Корпоративное*.

Этот параметр влияет только на те устройства, которые были добавлены с помощью опроса сети. Для устройств, добавленных вручную, установите параметр *Корпоративное* вручную.

4. Нажмите на кнопку **ОК**.

Критерии обнаружения корпоративных устройств настроены.

См. также:

Сценарий: обнаружение сетевых устройств	322
Инвентаризация оборудования	338

Настройка пользовательских полей

► Чтобы настроить пользовательские поля устройств:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Настроить пользовательские поля данных**.
Откроется окно свойств оборудования.
3. В окне свойств оборудования в разделе **Пользовательские поля** нажмите на кнопку **Добавить**.
Откроется окно **Добавить поле**.
4. В окне **Добавить поле** укажите название пользовательского поля, которое будет отображаться в свойствах оборудования.
Вы можете создать несколько пользовательских полей с уникальными именами.
5. Нажмите на кнопку **ОК**.

В результате в свойствах оборудования в разделе **Пользовательские поля** будут отображаться добавленные пользовательские поля. Вы можете использовать пользовательские поля для указания специфической информации об устройствах. Например, номер внутренней заявки на приобретение оборудования.

См. также:

Сценарий: обнаружение сетевых устройств	322
Инвентаризация оборудования	338

Лицензирование

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Security Center.

См. также:

Приложения "Лаборатории Касперского": лицензирование и активация	388
Шаг 2. Выбор способа активации приложения.....	284
Основной сценарий установки.....	56

В этом разделе

События превышения лицензионного ограничения	341
О лицензировании	341
О предоставлении данных	347
Варианты лицензирования Kaspersky Security Center	354
Особенности лицензирования Kaspersky Security Center и управляемых приложений.....	355

События превышения лицензионного ограничения

Kaspersky Security Center позволяет получать информацию о событиях превышения лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах.

Уровень важности событий о превышении лицензионного ограничения определяется по следующим правилам:

- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 90%–100% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Информационное сообщение**.
- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 100%–110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Предупреждение**.
- Если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Критическое событие**.

См. также:

Настройка общих параметров Сервера администрирования	716

О лицензировании

В этом разделе содержится информация о лицензировании приложений "Лаборатории Касперского", управляемых с помощью Kaspersky Security Center.

В этом разделе

О лицензии	342
О Лицензионном соглашении	342
О лицензионном сертификате	343
О лицензионном ключе	344
О файле ключа	344
О подписке	345
О коде активации	345
Отзыв согласия с Лицензионным соглашением	346

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Security Center, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с приложением.
Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security Center прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.
Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.
- *Коммерческая* – платная лицензия.
По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Security Center вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.
Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского" в котором указано, на каких условиях вы можете использовать приложение.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

Kaspersky Security Center и его компоненты, например Агент администрирования, имеют собственные Лицензионные соглашения.

Вы можете ознакомиться с условиями Лицензионного соглашения для Kaspersky Security Center следующими способами:

- Во время установки Kaspersky Security Center.
- Прочитав документ license.txt, включенный в комплект поставки Kaspersky Security Center.
- Прочитав документ license.txt в папке установки Kaspersky Security Center.
- Загрузив файл license.txt с сайта "Лаборатории Касперского" <https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint>.

Вы можете ознакомиться с условиями Лицензионного соглашения для Агента администрирования для Windows, Агента администрирования для Mac и Агента администрирования для Linux следующими способами:

- При загрузке дистрибутива Агента администрирования с веб-серверов "Лаборатории Касперского".
- При установке дистрибутива Агента администрирования для Windows, Агента администрирования для Mac или Агента администрирования для Linux.
- Прочитав документ license.txt, входящий в состав дистрибутива Агента администрирования для Windows, Агента администрирования для Mac или Агента администрирования для Linux.
- Прочитав документ license.txt в папке установки Агента администрирования для Windows, Агента администрирования для Mac или Агента администрирования для Linux.
- Загрузив файл license.txt с сайта "Лаборатории Касперского" <https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint>.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки приложения. Если вы не согласны с условиями Лицензионного соглашения, вам нужно прервать установку приложения и не должны использовать приложение.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о приложении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы приложения требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным (или резервным).

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В приложении не может быть больше одного активного лицензионного ключа.

Дополнительный (или резервный) лицензионный ключ – лицензионный ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего приложение.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- обратиться к продавцу лицензии;
- получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.
- экспортировать файл ключа (см. раздел "Exporting a license key file" на стр. [400](#)) с другого Сервера администрирования.

О подписке

Подписка на Kaspersky Security Center – это заказ на использование приложения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Security Center можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме, или отказаться от нее.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Security Center после окончания ограниченной подписки ее требуется продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность приложения сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Security Center по подписке, требуется применить код активации, предоставленный поставщиком услуг.

Вы можете применить другой код активации для использования Kaspersky Security Center только после окончания подписки или отказа от нее.

В зависимости от поставщика услуг, наборы возможных действий для управления подпиской могут различаться. Поставщик услуг может не предоставлять льготный период для продления подписки, в течение которого функциональность приложения сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Security Center.

При использовании приложения по подписке Kaspersky Security Center автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки. Это обеспечивает синхронизацию информации о подписке с сервером активации. Если доступ к серверу через системный DNS невозможен, приложение использует публичные DNS-серверы (см. раздел "Доступ к общедоступным DNS-серверам" на стр. [919](#)). Вы можете продлить подписку на веб-сайте поставщика услуг.

Вы можете обновить информацию о подписке вручную, не дожидаясь, когда Kaspersky Security Center получит доступ к серверу активации. Например, это может быть полезно при изменении параметров подписки.

► *Чтобы обновить информацию о подписке вручную:*

1. В дереве консоли выберите папку **"Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Синхронизировать параметры подписки с Сервером лицензирования**.

Информация о подписке обновлена на сервере активации.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Security Center. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского". Если доступ к серверам через системный DNS

невозможен, приложение использует публичные DNS-серверы (см. раздел "Доступ к общедоступным DNS-серверам" на стр. [919](#)).

Если приложение было активировано с помощью кода активации, в некоторых случаях после активации приложение регулярно отправляет запросы на серверы активации "Лаборатории Касперского" для проверки текущего статуса лицензионного ключа. Для отправки запросов необходимо предоставить приложению доступ в интернет.

Если вы потеряли код активации после установки приложения, обратитесь к партнеру "Лаборатории Касперского", у которого вы приобрели лицензию.

Вы не можете использовать файлы ключей для активации управляемых приложений; вы можете применить только коды активации.

См. также:

Основной сценарий установки.....[56](#)

Отзыв согласия с Лицензионным соглашением

Если вы решили прекратить защиту клиентских устройств, вы можете удалить управляемые приложения "Лаборатории Касперского" и отозвать Лицензионное соглашение для этих приложений.

► Чтобы отозвать Лицензионное соглашение для управляемых приложений "Лаборатории Касперского":

1. В дереве консоли выберите **Сервер администрирования → Дополнительно → Принятые Лицензионные соглашения**.

Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов, установке обновлений или развертывании Kaspersky Security для мобильных устройств.

2. В списке выберите Лицензионные соглашения, которые вы хотите отозвать.

Можно просмотреть следующие свойства Лицензионных соглашений:

- Дата принятия Лицензионного соглашения.
- Имя пользователя, принявшего Лицензионное соглашение.
- Ссылка на условия Лицензионного соглашения.
- Список объектов, на которые распространяется Лицензионное соглашение: названия инсталляционных пакетов, имена обновлений, названия мобильных приложений.

3. Нажмите на кнопку **Отозвать Лицензионное соглашение**.

В открывшемся окне отобразится информация о том, что необходимо удалить приложение "Лаборатории Касперского", которому соответствует это Лицензионное соглашение.

4. Нажмите на кнопку, подтверждающую отзыв лицензии.

Kaspersky Security Center проверяет, удалены ли инсталляционные пакеты, соответствующие управляемому приложению "Лаборатории Касперского", Лицензионное соглашение которого вы отзываете.

Можно отозвать только Лицензионное соглашение для управляемого приложения "Лаборатории Касперского", для которого удален инсталляционный пакет.

Лицензионное соглашение отозвано. Оно больше не отображается в списке Лицензионных соглашений в разделе **Сервер администрирования** → **Дополнительно** → **Принятые Лицензионные соглашения**. Приложение "Лаборатории Касперского", для которого было отозвано Лицензионное соглашение, больше невозможно использовать для защиты клиентских устройств.

См. также

Сценарий: настройка защиты сети.....[403](#)

О предоставлении данных

Данные, передаваемые третьим сторонам

При использовании функциональности для управления мобильными устройствами Программным обеспечением с целью своевременной доставки команд на устройства под управлением операционной системы Android через механизм push-уведомлений используется сервис Google Firebase Cloud Messaging. Если Пользователь настроил использование службы Google Firebase Cloud Messaging, Пользователь соглашается предоставить следующую информацию службе Google Firebase Cloud Messaging в автоматическом режиме: идентификаторы установки приложений Kaspersky Endpoint Security для Android, на которые должны быть отправлены push-уведомления.

Чтобы блокировать обмен информацией со службой Google Firebase Cloud Messaging, Пользователь должен сбросить настройки использования службы Google Firebase Cloud Messaging.

При использовании функциональности для управления мобильными устройствами Программным обеспечением с целью своевременной доставки команд на устройства под управлением операционной системы iOS через механизм push-уведомлений, используется сервис Apple Push Notification Service (APNs). Если Пользователь установил APNs-сертификат на сервер iOS MDM, сформировал iOS MDM-профиль с набором параметров подключения мобильных устройств iOS к Программному обеспечению и установил этот iOS MDM-профиль на мобильные устройства, Пользователь соглашается в автоматическом режиме предоставлять в сервис APNs следующую информацию:

- Токен – push-токен устройства. Сервер использует этот токен при отправке push-уведомлений на устройство.
- PushMagic – строка, которая должна быть включена в push-уведомление. Значение строки генерируется устройством.

Данные, обрабатываемые локально

Приложение Kaspersky Security Center предназначено для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Kaspersky Security Center предоставляет администратору доступ к подробной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе приложений "Лаборатории Касперского". Kaspersky Security Center выполняет следующие основные функции:

- обнаружение устройств и их пользователей в сети организации;

- формирование иерархии групп администрирования для управления устройствами;
- установка приложений "Лаборатории Касперского" на устройства;
- управление параметрами работы и задачами установленных приложений;
- управление обновлениями приложений "Лаборатории Касперского" и других производителей, поиск и закрытие уязвимостей;
- активация приложений "Лаборатории Касперского" на устройствах;
- управление учетными записями пользователей;
- просмотр информации о работе приложений "Лаборатории Касперского" на устройствах;
- просмотр отчетов.

Для выполнения своих основных функций приложение Kaspersky Security Center может принимать, хранить и обрабатывать следующую информацию:

- Информация об устройствах в сети организации получена путем опроса Windows-домена, контроллеров домена Active Directory или Samba или путем опроса IP-диапазонов. Сервер администрирования независимо получает данные, или их передает ему Агент администрирования, который выполняет роль точки распространения.
- Информация из Active Directory и Samba об организационных подразделениях, доменах, пользователях и группах. Сервер администрирования независимо получает данные, или их передает ему Агент администрирования, который выполняет роль точки распространения.
- Данные об управляемых устройствах. Агент администрирования передает от устройства Серверу администрирования перечисленные ниже данные. Пользователь вводит отображаемое имя и описание устройства в интерфейс Консоли администрирования или интерфейс Kaspersky Security Center Web Console:
 - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: отображаемое имя и описание устройства, имя и тип (для устройств, принадлежащих Windows-домену), имя устройства в среде (для устройств, принадлежащих Windows-домену), DNS-домен и DNS-имя, IPv4-адрес, IPv6-адрес, сетевое местоположение, MAC-адрес, серийный номер, тип операционной системы, является ли устройство виртуальной машиной и тип гипервизора, является ли устройство динамической виртуальной машиной как частью VDI.
 - Прочие характеристики управляемых устройств и их компонентов, необходимые для аудита управляемых устройств и для принятия решений о применимости тех или иных патчей и обновлений: состояние агента обновлений Windows (WUA), архитектура операционной системы, поставщик операционной системы, номер сборки операционной системы, идентификатор выпуска операционной системы, папка расположения операционной системы, если устройство является виртуальной машиной, то тип виртуальной машины; имя виртуального Сервера администрирования, который управляет устройствами; данные об облачном устройстве (облачный регион, VPC, облачная зона доступности, облачная подсеть, группа размещения облачного устройства).
 - Подробные данные о действиях на управляемых устройствах: дата и время последнего обновления, время, когда устройство последний раз было видимо в сети, состояние ожидания перезапуска, время включения устройства.
 - Данные об учетных записях пользователей устройств и их сеансах работы.
- Данные, полученные при запуске удаленной диагностики на управляемом устройстве: файлы трассировки, системная информация, сведения об установленных на устройстве приложениях

"Лаборатории Касперского", файлы дампов, журналы событий, результаты запуска диагностических скриптов, полученные от Службы технической поддержки "Лаборатории Касперского".

- Статистику работы точки распространения, если устройство является точкой распространения. Агент администрирования передает данные от устройства на Сервер администрирования.
- Параметры точки распространения, которые Пользователь вводит в Консоли администрирования или в Kaspersky Security Center Web Console.
- Данные, необходимые для подключения мобильных устройств к Серверу администрирования: сертификат, порт для подключения мобильных устройств, адрес подключения к Серверу администрирования. Пользователь вводит данные в Консоли администрирования или Kaspersky Security Center Web Console.
- Данные о мобильных устройствах, передаваемые по протоколу iOS MDM. Данные перечисленные ниже передаются от мобильного устройства Серверу администрирования:
 - Технические характеристики мобильного устройства и его компонентов, необходимые для идентификации устройства: имя устройства, модель, название и номер сборки операционной системы, номер модели устройства, номер IMEI, UDID, MEID, серийный номер, объем памяти, версия прошивки модема, MAC-адрес Bluetooth, MAC-адрес Wi-Fi и данные SIM-карты (код ICCID как часть идентификатора SIM-карты).
 - Данные о мобильной сети, используемой мобильным устройством: тип мобильной сети, название используемой мобильной сети, название домашней мобильной сети, версия параметров оператора мобильной сети, статус голосового роуминга и роуминга данных, код страны для домашней сети, код страны пребывания, код страны используемой сети и уровень шифрования.
 - Параметры безопасности мобильного устройства: использование пароля и его соответствие параметрам политики, список конфигурационных профилей и provisioning-профилей, используемых для установки сторонних приложений.
 - Дата последней синхронизации с Сервером администрирования и статус управления устройством.
- Данные о приложениях "Лаборатории Касперского", установленных на устройстве. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования:
 - Название и версия приложения "Лаборатории Касперского", статус, состояние постоянной защиты, дата и время последней проверки устройства, количество обнаруженных угроз, количество объектов, для которых не удалось выполнить лечение, наличие и статус компонентов приложения, время последнего обновления и версия антивирусных баз, данные о параметрах и задачах приложения "Лаборатории Касперского", информация об активном и резервных лицензионных ключах, дата и идентификатор установки приложения.
 - Статистика работы приложения: события, связанные с изменениями статуса компонентов приложения "Лаборатории Касперского" на управляемом устройстве и с выполнением задач, инициированных компонентами приложения.
 - Состояние устройства, определенное приложением "Лаборатории Касперского".
 - Теги, передаваемые приложением "Лаборатории Касперского".
 - Набор установленных и применимых обновлений к приложению "Лаборатории Касперского".
- Данные, содержащиеся в событиях от компонентов Kaspersky Security Center и управляемых приложений "Лаборатории Касперского". Агент администрирования передает данные от устройства на Сервер администрирования.

- Данные, необходимые для интеграции Kaspersky Security Center с SIEM-системой для экспорта событий. Пользователь вводит данные в Консоли администрирования или Kaspersky Security Center Web Console.
- Настройки компонентов Kaspersky Security Center и управляемых приложений "Лаборатории Касперского", представленные в виде политик и профилей политик. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.
- Настройки задач компонентов Kaspersky Security Center и управляемых приложений "Лаборатории Касперского". Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.
- Данные, обрабатываемые функцией Системное администрирование. Агент администрирования передает от устройства Серверу администрирования перечисленные ниже данные:
 - Данные о приложениях и патчах, установленных на управляемых устройствах (Реестр приложений).
 - Информация об оборудовании, обнаруженном на управляемых устройствах (Реестр оборудования).
 - Данные об уязвимостях стороннего программного обеспечения, обнаруженных на управляемых устройствах.
 - Данные об обновлениях, доступных для сторонних приложений, установленных на управляемых устройствах.
 - Данные об обновлениях Microsoft, найденные функцией WSUS.
 - Список обновлений Microsoft, найденных функцией WSUS, которые должны быть установлены на устройство.
- Данные, которые необходимы для загрузки обновлений на изолированный Сервер администрирования для закрытия уязвимостей в приложениях сторонних производителей на управляемых устройствах. Пользователь вводит и передает данные с помощью утилиты klscflag Сервера администрирования.
- Данные, необходимые для работы Kaspersky Security Center с облачным окружением (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud). Пользователь вводит данные в Консоли администрирования или Kaspersky Security Center Web Console.
- Пользовательские категории приложений. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.
- Данные об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль приложений. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console. Полный список данных представлен в справке соответствующего приложения.
- Данные о файлах, помещенных в резервное хранилище. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные о файлах, помещенных в Карантин. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные о файлах, запрошенных специалистами "Лаборатории Касперского" для подробного анализа. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о состоянии и срабатывании правил Адаптивного контроля аномалий. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные о внешних устройствах (устройствах памяти, инструментах передачи информации, инструментах превращения информации в твердую копию, шинах подключения), установленных или подключенных к управляемому устройству и обнаруженных функцией Контроль устройств. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Информация о зашифрованных устройствах и статусе шифрования. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования.
- Данные об ошибках шифрования данных на устройствах, выполняемого функцией Шифрование данных приложений "Лаборатории Касперского". Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Список управляемых программируемых логических контроллеров (ПЛК). Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные для создания цепочки развития угроз. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Информация о попытках сотрудников организации получить доступ к облачным сервисам. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные, необходимые для интеграции Kaspersky Security Center со службой Kaspersky Managed Detection and Response (для Kaspersky Security Center Web Console должен быть установлен специальный плагин): токен инициации интеграции, токен интеграции и токен сеанса пользователя. Пользователь с помощью токена инициации интеграции входит в интерфейс Kaspersky Security Center Web Console. Служба Kaspersky MDR передает токен интеграции и токен сеанса пользователя через специальный плагин.
- Подробная информация о введенных кодах активации или указанных файлах ключей. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.
- Учетные записи пользователей: имя, описание, полное имя, адрес электронной почты, основной номер телефона, пароль, секретный ключ, сгенерированный Сервером администрирования, и одноразовый пароль для двухэтапной проверки. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.
- Данные, которые необходимы Identity and Access Manager для централизованной аутентификации и для обеспечения единого входа (SSO) между приложениями "Лаборатории Касперского", интегрированными с Kaspersky Security Center: параметры установки и конфигурации Identity и Access Manager, пользовательский сеанс Identity и Access Manager, токены Identity and Access Manager, статусы клиентских приложений и статусы серверов ресурсов. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.
- Истории ревизий объектов управления. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

- IP-адрес устройства, на котором пользователь создал ревизию. IP-адрес определяется Сервером администрирования автоматически.
- Реестр удаленных объектов управления. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.
- Инсталляционные пакеты, созданные из файла, и параметры установки. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.
- Данные, необходимые для отображения объявлений от "Лаборатории Касперского" в Kaspersky Security Center Web Console. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Данные, необходимые для работы плагинов управляемых приложений в Kaspersky Security Center Web Console и сохраняемые плагином в базе данных Сервера администрирования в процессе повседневной работы. Описание и способы предоставления данных приведены в файлах справки соответствующего приложения.
- Настройки пользователя Kaspersky Security Center Web Console: язык локализации и тема пользовательского интерфейса, настройки отображения панели мониторинга, информации о состоянии уведомлений (прочитано/не прочитано), состояние столбцов в таблицах (скрыть/показать), прогресс прохождения режима обучения. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Журнал событий Kaspersky Event Log для компонентов Kaspersky Security Center и управляемых приложений "Лаборатории Касперского". Журнал событий Kaspersky Event Log хранится на устройстве и никогда не передается на Сервер администрирования.
- Сертификат безопасного подключения управляемых устройств к компонентам Kaspersky Security Center. Пользователь вводит данные с помощью утилиты klsetsrvcert Сервера администрирования.
- Сертификаты для установки доверия к внутренним веб-ресурсам организации. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Данные, необходимые для работы Kaspersky Security Center в облачных окружениях, таких как Amazon Web Services (AWS), Microsoft Azure, Google Cloud и Yandex.Cloud. Сервер администрирования получает данные от виртуальной машины, на которой он запущен.
- Информация о принятии Пользователем условий юридических соглашений с "Лабораторией Касперского".
- Данные Сервера администрирования, которые Пользователь вводит в следующих компонентах:
 - Консоль администрирования.
 - Kaspersky Security Center Web Console.
 - Терминал командной строки при использовании утилиты klscflag.
 - Компоненты, взаимодействующие с Сервером администрирования через объекты автоматизации klakaut и OpenAPI Kaspersky Security Center.
- Любые данные, которые Пользователь вводит в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

Перечисленные выше данные могут попасть в Kaspersky Security Center следующими способами:

- Пользователь вводит данные в интерфейс следующих компонентов:
 - Консоль администрирования.
 - Kaspersky Security Center Web Console.

- Терминал командной строки при использовании утилиты klsclag.
- Компоненты, взаимодействующие с Сервером администрирования через объекты автоматизации klakaut и OpenAPI Kaspersky Security Center.
- Агент администрирования самостоятельно получает данные с устройства и передает на Сервер администрирования.
- Агент администрирования получает данные от управляемого приложения "Лаборатории Касперского" и передает их на Сервер администрирования. Перечни данных, обрабатываемых управляемыми приложениями "Лаборатории Касперского", приведены в справках соответствующих приложений.
- Сервер администрирования самостоятельно получает данные о сетевых устройствах, или их передает ему Агент администрирования, который выполняет роль точки распространения.
- Данные передаются с мобильного устройства на Сервер администрирования по протоколу iOS MDM.

Перечисленные данные хранятся в базе данных Сервера администрирования. Имена пользователей и пароли хранятся в зашифрованном виде.

Все перечисленные выше данные могут быть переданы "Лаборатории Касперского" только посредством файлов дампа, файлов трассировки или файлов журналов компонентов Kaspersky Security Center, включая файлы журналов, создаваемые инсталляторами и утилитами.

Файлы дампа, файлы трассировки и файлы журналов компонентов Kaspersky Security Center содержат случайные данные Сервера администрирования, Агента администрирования, Консоли администрирования, Сервера iOS MDM, Kaspersky Security Center Web Console. Эти файлы могут содержать персональные и конфиденциальные данные. Файлы дампа, файлы трассировки и файлы журналов хранятся в открытой форме на устройстве. Файлы дампа, файлы трассировки и файлы журналов не передаются в "Лабораторию Касперского" автоматически, однако, администратор может передать эти данные в "Лабораторию Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Kaspersky Security Center.

Переходя по ссылкам в Консоли администрирования или Kaspersky Security Center Web Console, Пользователь соглашается на автоматическую передачу следующих данных:

- код Kaspersky Security Center;
- версия Kaspersky Security Center;
- локализация Kaspersky Security Center;
- идентификатор лицензии;
- тип лицензии;
- признак покупки лицензии через партнера.

Список данных, предоставляемых по каждой ссылке, зависит от цели и местоположения ссылки.

"Лаборатория Касперского" использует полученные данные в анонимной форме и только для целей общей статистики. Сводная статистика автоматически формируется из полученной исходной информации и не содержит каких-либо персональных или прочих конфиденциальных данных. При накоплении новых данных предыдущие данные уничтожаются (один раз в год). Сводная статистика хранится неограниченное время.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Варианты лицензирования Kaspersky Security Center

Kaspersky Security Center может работать в следующих режимах:

- **Базовая функциональность Консоли администрирования**

Kaspersky Security Center работает в этом режиме до активации приложения или после истечения срока действия коммерческой лицензии. Приложение Kaspersky Security Center с поддержкой базовой функциональности Консоли администрирования поставляется в составе приложений "Лаборатории Касперского", предназначенных для защиты сети организации. Кроме того, она доступна для загрузки с веб-сайта "Лаборатории Касперского".

- **Коммерческая лицензия**

Если вам нужна дополнительная функциональность, не входящая в базовую функциональность Консоли администрирования, вам требуется приобрести коммерческую лицензию.

При добавлении лицензионного ключа в окне свойств Сервера администрирования убедитесь, что вы добавили лицензионный ключ, который позволяет использовать Kaspersky Security Center. Вы можете найти эту информацию на сайте "Лаборатории Касперского". На странице каждого решения есть список приложений, включенных в это решение. Сервер администрирования может принимать неподдерживаемые лицензионные ключи, например лицензионный ключ для Kaspersky Endpoint Security Cloud, но такие лицензионные ключи не предоставляют никаких новых функций, кроме базовой функциональности Консоли администрирования.

Функция или свойство	Режим работы Kaspersky Security Center	
	Лицензия отсутствует	Коммерческая лицензия
Базовая функциональность Консоли администрирования	✓	✓
Системное администрирование: базовая функциональность	✓	✓
Системное администрирование: расширенная функциональность	—	✓
Управление мобильными устройствами в Консоли администрирования на базе ММС.	—	✓ Лицензионный ключ необходимо добавить в свойствах Сервера администрирования.
Защита мобильных устройств в Kaspersky Security Center Web Console	—	✓ Лицензионный ключ должен быть добавлен на каждое мобильное устройство.
Управление системами	—	✓

Функция или свойство	Режим работы Kaspersky Security Center	
	Лицензия отсутствует	Коммерческая лицензия
Интеграция с облачными окружениями	—	✓
Экспорт событий в SIEM-системы с помощью формата Syslog	✓	✓

См. также:

Лицензии и возможности Kaspersky Security Center[29](#)

Особенности лицензирования Kaspersky Security Center и управляемых приложений

Лицензирование Сервера администрирования и управляемых приложений имеет следующие особенности:

- На Сервер администрирования можно добавить лицензионный ключ или действительный код активации (см. раздел "Приложения "Лаборатории Касперского": лицензирование и активация" на стр. [388](#)) для активации возможностей Системного администрирования, Управления мобильными устройствами или интеграции с SIEM-системами. Некоторые функции Kaspersky Security Center доступны только при наличии активных ключей или действительных кодов активации, добавленных на Сервер администрирования.
- В хранилище Сервера администрирования вы можете добавить несколько кодов активации и файлов ключей для управляемых приложений (см. раздел "Добавление лицензионного ключа в хранилище Сервера администрирования." на стр. [392](#)).

Особенности лицензирования Kaspersky Security Center

Например, если вы активировали с помощью файла ключа одну из возможностей (например, Управления мобильными устройствами), но вам дополнительно потребовались другие возможности (например, Системного администрирования), в этом случае необходимо приобрести ключ, который активирует обе функциональности, и активировать этим ключом Сервер администрирования.

Особенности лицензирования управляемых приложений

Для лицензирования управляемых приложений вы можете распространить код активации или ключ автоматически или другим удобным для вас способом. Существуют следующие способы распространения кода активации или файла ключа:

- Автоматическое распространение

Если вы используете разные управляемые приложения и вам важно распространить определенный файл ключа или код активации на устройства, используйте другие способы распространения кода активации или ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Для всех лицензионных ключей установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства**. На устройствах организации установлено приложение безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Приложение определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае невозможно предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

При распространении лицензионного ключа на устройства происходит подсчет устройств для данного лицензионного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение, таким устройствам будет присвоен статус *Критический*.

- Добавление файла ключа или кода активации в инсталляционный пакет управляемого приложения

В случае установки управляемого приложения с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этого приложения. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

- Распространение с помощью задачи добавления лицензионного ключа управляемого приложения

В случае использования задачи добавления лицензионного ключа управляемого приложения вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

- Добавление кода активации или файла ключа вручную на устройства

См. также:

Лицензии и возможности Kaspersky Security Center	29
Основной сценарий установки.....	56

Приложения "Лаборатории Касперского". Централизованное развертывание

В этом разделе описаны способы удаленной установки приложений "Лаборатории Касперского" и их удаления с устройств сети.

Перед началом установки приложений на клиентские устройства требуется убедиться в том, что аппаратное и программное обеспечение устройств соответствует требованиям.

Связь Сервера администрирования с клиентскими устройствами обеспечивает Агент администрирования. Поэтому его необходимо установить на каждое клиентское устройство, которое будет подключено к системе удаленного централизованного управления. На устройстве, где установлен Сервер администрирования, может использоваться только серверная версия Агента администрирования. Она входит в состав Сервера администрирования и устанавливается и удаляется вместе с ним. Устанавливать Агент администрирования на это устройство не требуется.

Установка Агента администрирования осуществляется точно так же, как и установка приложений, и может быть проведена как удаленно, так и локально. При централизованной установке приложений безопасности через Консоль администрирования вы можете установить Агент администрирования совместно с приложениями безопасности.

Агенты администрирования могут отличаться в зависимости от приложений "Лаборатории Касперского", с которыми они работают. В некоторых случаях возможна только локальная установка Агента администрирования (подробнее см. в руководствах к соответствующим приложениям). Вам нужно установить Агент администрирования на клиентское устройство только один раз.

Управление приложениями "Лаборатории Касперского" (см. раздел "Совместимые приложения и решения "Лаборатории Касперского"" на стр. [29](#)) через Консоль администрирования выполняется при помощи плагинов управления. Поэтому для получения доступа к управлению приложением через Kaspersky Security Center плагин управления этого приложения должен быть установлен на рабочее место администратора.

Вы можете выполнить удаленную установку приложений с рабочего места администратора в главном окне приложения Kaspersky Security Center.

Для удаленной установки программного обеспечения следует создать задачу удаленной установки.

Сформированная задача удаленной установки будет запускаться на выполнение в соответствии со своим расписанием. Вы можете прервать процедуру установки, остановив выполнение задачи вручную.

Если удаленная установка приложения завершается с ошибкой, вы можете проверить, чем вызвана эта проблема, и устранить ее с помощью утилиты подготовки устройства к удаленной установке (см. раздел "Подготовка устройства под управлением Windows к удаленной установке" на стр. [383](#)).

Вы можете отслеживать процесс установки приложений безопасности "Лаборатории Касперского" в сети с помощью отчета о развертывании.

Подробную информацию об управлении перечисленными приложениями через Kaspersky Security Center см. в руководствах к соответствующим приложениям.

В этом разделе

Замещение приложений безопасности сторонних производителей	358
Установка приложений с помощью задачи удаленной установки	359
Установка приложений с помощью мастера удаленной установки	363
Работа с плагинами управления	368
Просмотр отчета о развертывании защиты ...	369
Удаленная деинсталляция приложений	370
Работа с инсталляционными пакетами	371
Получение актуальных версий приложений...	381
Подготовка устройства под управлением Windows к удаленной установке	383
Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux	384
Подготовка устройства с операционной системой macOS к удаленной установке Агента администрирования	387

См. также:

Основной сценарий установки	56

Замещение приложений безопасности сторонних производителей

Для установки приложений безопасности "Лаборатории Касперского" средствами Kaspersky Security Center может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемым приложением. Kaspersky Security Center предоставляет несколько способов удаления приложений сторонних производителей.

Удаление несовместимых приложений с помощью приложения установки

Этот параметр доступен только в Консоли администрирования на основе консоли управления Microsoft Management Console.

Метод удаления несовместимых приложений поддерживается различными типами установки. Перед установкой приложения безопасности несовместимые с ним приложения удаляются автоматически, если в окне свойств инсталляционного пакета приложений безопасности (раздел **Несовместимые приложения**) выбран параметр **Удалять несовместимые приложения автоматически**.

Удаление несовместимых приложений при настройке удаленной установки приложения

Вы можете включить параметр **Удалять несовместимые приложения автоматически** во время настройки удаленной установки приложения безопасности. В Консоли администрирования на основе консоли Microsoft Management Console (MMC) этот параметр доступен в мастере удаленной установки. В приложении Kaspersky Security Center Web Console этот параметр можно найти в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center удаляет несовместимые приложения перед установкой приложения безопасности на управляемое устройство.

Инструкции:

- Консоль администрирования: Удаление несовместимых приложений с помощью мастера удаленной установки.
- Kaspersky Security Center Web Console: Удаление несовместимых приложений перед установкой.

Удаление несовместимых приложений с помощью отдельной задачи

Для удаления несовместимых приложений используется задача **Удаленная деинсталляция приложений**. Задачу следует запускать на устройствах перед задачей установки приложения безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача **Удаленная деинсталляция приложения**.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор приложения безопасности не может успешно удалить какое-либо из несовместимых приложений.

Инструкции для Консоли администрирования: Создание задачи (на стр. [416](#)).

Установка приложений с помощью задачи удаленной установки

Kaspersky Security Center позволяет удаленно устанавливать приложения на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам (до 1000 устройств), вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования.** В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка.** Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
- **Назначить задачу выборке устройств.** В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать predetermined выборку или вашу собственную выборку.
- **Назначить задачу группе администрирования.** В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

Для правильной работы задачи удаленной установки на устройстве, на котором не установлен Агент администрирования, необходимо открыть порты TCP 139 и 445, UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке (см. раздел "Подготовка устройства под управлением Windows к удаленной установке" на стр. [383](#)).

В этом разделе

Установка приложения на выбранные устройства	360
Установка приложения на клиентские устройства группы администрирования.....	360
Установка приложения с помощью групповых политик Active Directory	361
Установка приложений на подчиненные Серверы администрирования	363

Установка приложения на выбранные устройства

► Чтобы установить приложение на выбранные устройства:

1. В дереве консоли выберите папку **Задачи**.
2. Запустите мастер создания задачи по кнопке **Создать задачу**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** выберите тип задачи **Удаленная установка приложения**.

В результате работы мастера создания задачи будет создана задача удаленной установки выбранного приложения для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.

3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранное приложение будет установлено на выбранные устройства.

Установка приложения на клиентские устройства группы администрирования

► Чтобы установить приложение на клиентские устройства группы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области выберите вкладку **Задачи**.
4. Запустите мастер создания задачи по кнопке **Создать задачу**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** выберите тип задачи **Удаленная установка приложения**.

В результате работы мастера создания задачи будет создана групповая задача удаленной установки выбранного приложения. Созданная задача отображается в рабочей области группы администрирования, на вкладке **Задачи**.

5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранное приложение будет установлено на клиентские устройства группы администрирования.

Установка приложения с помощью групповых политик Active Directory

Kaspersky Security Center позволяет устанавливать приложения "Лаборатории Касперского" на управляемые устройства с помощью групповых политик Active Directory.

Установка приложений с помощью групповых политик Active Directory возможна только из инсталляционных пакетов, в состав которых входит Агент администрирования.

► Чтобы установить приложение с помощью групповых политик Active Directory:

1. Начните настройку установки приложения с помощью мастера удаленной установки (см. раздел "Установка приложений с помощью мастера удаленной установки" на стр. [363](#)).
2. В окне мастера удаленной установки **Определение параметров задачи удаленной установки** выберите параметр **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.
3. В окне мастера удаленной установки **Выбор учетных записей для доступа к устройствам** выберите параметр **Учетная запись требуется (Агент администрирования не используется)**.
4. Добавьте учетную запись с правами администратора на устройство, на котором установлен Kaspersky Security Center, или учетную запись, входящую в доменную группу Владельцы-создатели групповой политики.
5. Предоставьте разрешения выбранной учетной записи:
 - a. Перейдите в **Панель управления** → **Администрирование** и откройте **Управление групповой политикой**.
 - b. Нажмите на узел с нужным доменом.
 - c. Нажмите на раздел **Делегирование**.
 - d. В раскрывающемся списке **Права доступа** выберите **Связанные объекты GPO**.
 - e. Нажмите на кнопку **Добавить**.
 - f. В открывшемся окне **Выбор пользователя, компьютера или группы** выберите необходимую учетную запись.
 - g. Нажмите на кнопку **ОК** чтобы закрыть окно **Выбор пользователя, компьютера или группы**.
 - h. В списке **Группы и пользователи** выберите только что добавленную учетную запись и нажмите на **Дополнительно** → **Дополнительно**.
 - i. В списке **записей разрешений** дважды нажмите на только что добавленную учетную запись.

j. Предоставьте следующие разрешения:

- **создание объектов группы;**
- **удаление объектов группы;**
- **создание объектов контейнера групповой политики;**
- **удаление объектов контейнера групповой политики.**

k. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

6. Задайте другие параметры, следуя инструкциям мастера.

7. Запустите созданную задачу удаленной установки вручную или дождитесь ее запуска по расписанию.

В результате будет запущен следующий механизм удаленной установки:

1. После запуска задачи в каждом домене, которому принадлежат клиентские устройства из набора, будут созданы следующие объекты:
 - Объект групповой политики (Group policy object, GPO) с именем **Kaspersky_AK{GUID}**.
 - Группа безопасности содержит клиентские устройства, на которые распространяется задача. Эта группа безопасности содержит клиентские устройства, на которые распространяется задача. Состав группы безопасности определяет область объект групповой политики (GPO).
2. Kaspersky Security Center устанавливает выбранные приложения "Лаборатории Касперского" на клиентские устройства осуществляется непосредственно из сетевой папки общего доступа приложения Share. При этом в папке установки Kaspersky Security Center будет создана вложенная вспомогательная папка, содержащая файл с расширением msi для устанавливаемого приложения.
3. При добавлении новых устройств в область действия задачи они будут добавлены в группу безопасности после следующего запуска задачи. Если в расписании задачи выбран флажок **Запускать пропущенные задачи**, устройства будут добавлены в группу безопасности сразу.
4. При удалении устройств из области действия задачи их удаление из группы безопасности произойдет при следующем запуске задачи.
5. При удалении задачи из Active Directory будут удалены объект групповой политики (GPO), ссылка на объект групповой политики (GPO) и группа безопасности, связанная с задачей.

Если вы хотите использовать другую схему установки через Active Directory, вы можете настроить параметры установки вручную. Это может потребоваться, например, в следующих случаях:

- при отсутствии у администратора антивирусной защиты прав на внесение изменений в Active Directory некоторых доменов;
- при необходимости размещения исходного дистрибутива на отдельном сетевом ресурсе;
- для привязки групповой политики к конкретным подразделениям Active Directory.

Доступны следующие варианты использования другой схемы установки через Active Directory:

- Если установку требуется осуществлять непосредственно из папки общего доступа Kaspersky Security Center, в свойствах групповой политики Active Directory следует указать файл с расширением msi, расположенный во вложенной папке ехес в папке инсталляционного пакета нужного приложения.
- Если инсталляционный пакет нужно разместить на другом сетевом ресурсе, следует скопировать в него все содержимое папки ехес, так как помимо файла с расширением msi в ней содержатся конфигурационные файлы, сформированные при создании инсталляционного пакета. Чтобы

лицензионный ключ был установлен вместе с приложением, в эту папку следует также скопировать файл ключа.

Установка приложений на подчиненные Серверы администрирования

► *Чтобы установить приложение на подчиненные Серверы администрирования:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.
2. Убедитесь в том, что соответствующий устанавливаемому приложению инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если инсталляционного пакета нет на каком-либо из подчиненных Серверов, распространите его с помощью задачи распространения инсталляционного пакета (см. раздел "Распространение инсталляционных пакетов на подчиненные Серверы администрирования" на стр. [379](#)).
3. Запустите создание задачи установки приложения на подчиненные Серверы администрирования одним из следующих способов:
 - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи удаленной установки для этой группы (см. раздел "Установка приложения на клиентские устройства группы администрирования" на стр. [360](#)).
 - Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи удаленной установки для набора устройств (см. раздел "Установка приложения на выбранные устройства" на стр. [360](#)).

В результате запустится мастер создания задачи удаленной установки. Следуйте далее указаниям мастера.

В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная установка приложения на подчиненные Серверы администрирования**.

В результате работы мастера создания задачи будет создана задача удаленной установки выбранного приложения на выбранные подчиненные Серверы администрирования.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранное приложение будет установлено на выбранные подчиненные Серверы администрирования.

Установка приложений с помощью мастера удаленной установки

Для установки приложений "Лаборатории Касперского" вы можете воспользоваться мастером удаленной установки. Мастер удаленной установки позволяет проводить удаленную установку приложений как с использованием сформированных инсталляционных пакетов, так и с использованием дистрибутивов.

Для правильной работы задачи удаленной установки на клиентском устройстве, на котором не установлен Агент администрирования, необходимо открыть следующие порты: TCP 139 and 445; UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке (см. раздел "Подготовка устройства под управлением Windows к удаленной установке" на стр. [383](#)).

► *Чтобы установить приложение на выбранные устройства с помощью мастера удаленной установки:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В рабочей области папки выберите инсталляционный пакет приложения, которое нужно установить.
3. В контекстном меню инсталляционного пакета выберите пункт **Установить приложение**.
Запустится мастер удаленной установки.
4. В окне **Выбор устройств для установки** можно сформировать список устройств, на которые будет установлено приложение:

- **Установить на группу управляемых устройств**

Если выбран этот вариант, задача удаленной установки приложения будет создана для группы устройств.

- **Выбор устройств для установки**

Если выбран этот вариант, задача удаленной установки приложения будет создана для набора устройств. В состав набора могут входить как устройства в составе групп, так и нераспределенные устройства.

5. В окне **Определение параметров задачи удаленной установки** настройте параметры удаленной установки приложения.

В блоке параметров **Принудительно загрузить инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

- **С помощью Агента администрирования**

Если флажок установлен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

Если флажок снят, доставка инсталляционных пакетов выполняется средствами Microsoft Windows.

Рекомендуется установить флажок, если задача назначена для устройств с установленными Агентами администрирования.

По умолчанию флажок установлен.

- **Средствами операционной системы с помощью Сервера администрирования**

Если флажок установлен, доставка файлов на клиентские устройства будет осуществляться средствами Microsoft Windows с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

По умолчанию флажок установлен.

- **Средствами операционной системы с помощью точек распространения**

Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

- **Количество попыток установки**

Если при запуске задачи удаленной установки Kaspersky Security Center не удастся установить приложение на управляемое устройство за указанное в параметрах количество запусков установок, Kaspersky Security Center прекращает доставку инсталляционного пакета на это управляемое устройство и больше не запускает установку на устройстве.

Параметр [Количество попыток установки](#) позволяет вам сохранить ресурсы управляемого устройства, а также уменьшить трафик (деинсталляция, запуск файла MSI и сообщения об ошибках).

Повторяющиеся попытки запуска задачи могут указывать на проблему на устройстве, которая препятствует установке. Администратор должен решить проблему в течение указанного количества попыток установки (например, выделив достаточно места на диске, удалив несовместимые приложения или изменив параметры других приложений, препятствующих установке), и перезапустить задачу (вручную или по расписанию).

Если установка не выполнена, проблема будет считаться неразрешимой и любые дальнейшие запуски считаются дорогостоящими с точки зрения нежелательного расхода ресурсов и трафика.

После создания задачи, количество попыток установки равно 0. Каждый запуск установки, который возвращает ошибку на устройстве, увеличивает показания счетчика.

Если количество попыток установки, указанное в параметрах задачи, было превышено и устройство готово к установке приложения, вы можете увеличить значение параметра [Количество попыток установки](#) и запустить задачу по установке приложения. Также вы можете создать другую задачу удаленной установки.

Определите, какое действие выполнять с клиентскими устройствами, управляемыми другим Сервером администрирования:

- **Устанавливать на все устройства**

Приложение устанавливается даже на устройства, управляемые другими Серверами администрирования.

По умолчанию этот вариант выбран. Не нужно изменять этот параметр, если в вашей сети есть только один Сервер администрирования.

- **Устанавливать на устройства, управляемые только этим Сервером администрирования**

Приложение устанавливается только на устройства, которые управляются данным Сервером администрирования. Выберите этот параметр, если в вашей сети установлено больше одного Сервера администрирования и вы хотите избежать конфликтов (см. раздел "Избегание конфликтов между Серверами администрирования" на стр. [732](#)) между ними.

Настройте дополнительные параметры:

- **Не устанавливать приложение, если оно уже установлено**

Если флажок установлен, выбранное приложение не устанавливается заново, если оно уже установлена на клиентском устройстве.

Если флажок снят, приложение будет установлено в любом случае.

По умолчанию флажок установлен.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

Если флажок установлен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

Флажок доступен если выбран инсталляционный пакет Агента администрирования.

По умолчанию флажок снят.

1. В окне **Выбор лицензионного ключа** выберите лицензионный ключ и способ его распространения:

- **Не помещать лицензионный ключ в инсталляционный пакет (рекомендуется)**

Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

- если в свойствах ключа настроено автоматическое распространение (см. раздел "Автоматическое распространение лицензионного ключа." на стр. [398](#));
- если создана задача **Добавление ключа**.

- **Поместить лицензионный ключ в инсталляционный пакет**

Если выбран этот вариант, ключ распространяется на устройства вместе с инсталляционным пакетом.

Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу пакетов настроен общий доступ на чтение.

Окно **Выбор лицензионного ключа** отображается, если в состав инсталляционного пакета не входит лицензионный ключ.

Если в состав инсталляционного пакета входит лицензионный ключ, отображается окно **Свойства лицензионного ключа** с информацией о лицензионном ключе.

1. В окне **Выбор параметра перезагрузки операционной системы** определите, перезагружать ли устройства, если в ходе установки приложений на них потребуется перезагрузка операционной системы:

- **Не перезагружать устройство**

Если выбран этот вариант, устройство не будет перезагружаться после установки приложения защиты.

По умолчанию выбран этот вариант.

- **Перезагрузить устройство**

Если выбран этот вариант, устройство будет перезагружено после установки приложения защиты.

- **Запрашивать у пользователя**

Если выбран этот вариант, после установки приложения защиты пользователю

будет показано сообщение о необходимости перезагрузки устройства. По ссылке **Изменить** можно изменить текст сообщения, а также период отображения сообщения и время выполнения автоматической перезагрузки.

По умолчанию выбран этот вариант.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

Если флажок установлен, приложения в заблокированных устройствах будут принудительно закрываться перед перезагрузкой.

По умолчанию флажок снят.

2. В окне **Выбор учетных записей для доступа к устройствам** можно добавить учетные записи, которые будут использоваться для запуска задачи удаленной установки:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

3. В окне **Запуск установки** нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

Если в окне **Запуск установки** выбран параметр **Не запускать задачу после завершения работы мастера удаленной установки**, задача удаленной установки не будет запущена. Вы можете запустить эту задачу позже вручную. Имя задачи соответствует имени инсталляционного пакета для установки приложения: **Установка <Имя инсталляционного пакета>**.

► *Чтобы установить приложение на устройства группы администрирования с помощью мастера удаленной установки:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области группы нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите **Установить приложение**.

В результате запустится мастер удаленной установки. Следуйте далее указаниям мастера.

4. На последнем шаге мастера нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

После завершения работы мастера удаленной установки Kaspersky Security Center выполняет следующие действия:

- Создает инсталляционный пакет для установки приложения (если он не был создан раньше). Инсталляционный пакет размещается в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты** с именем, соответствующим названию и версии приложения. Вы можете использовать этот инсталляционный пакет для установки приложения в дальнейшем.
- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Сформированная задача удаленной установки размещается в папке **Задачи** или добавляется к задачам группы администрирования, для которой она была создана. Вы можете

запустить эту задачу позже вручную. Имя задачи соответствует имени инсталляционного пакета для установки приложения: **Установка <Имя инсталляционного пакета>**.

Работа с плагинами управления

Управление приложениями "Лаборатории Касперского" через Консоль администрирования выполняется при помощи плагинов управления. В состав каждого приложения "Лаборатории Касперского", которым можно управлять при помощи Kaspersky Security Center, входит плагин управления. С помощью плагина управления приложением в Консоли администрирования можно выполнять следующие действия:

- создавать и изменять политики приложений и их параметры, а также параметры задач для приложений;
- получать информацию о задачах приложений, событиях в работе приложений и статистику работы приложений, получаемой с клиентских устройств.

► Чтобы проверить список установленных плагинов и их версии:

1. В дереве Консоли администрирования нажмите правой кнопкой мыши на **Сервер администрирования <имя_сервера>** и выберите пункт **Свойства**.
2. Выберите пункт **Дополнительно** → **Информация об установленных плагинах управления приложениями**.

Список установленных плагинов управления и их версий появится в правой панели.

Вы можете установить плагины для управляемых приложений при запуске мастера первоначальной настройки (см. раздел "Шаг 4. Выбор плагинов для управляемых приложений" на стр. 286) Сервера администрирования при начальной настройке Kaspersky Security Center. Также вы можете установить плагины управления вручную.

► Чтобы установить плагин управления вручную:

1. Загрузите плагин управления приложения "Лаборатории Касперского" и необходимую версию приложения (например, Kaspersky Endpoint Security для Windows 12.6) со страницы Службы технической поддержки "Лаборатории Касперского" <https://support.kaspersky.com/ksc14/settings/host/9333#block3>.
2. Если Консоль администрирования запущена, закройте ее.
3. Разархивируйте загруженный файл плагина и запустите файл klcfginst.msi или klcfginst.exe. Следуйте инструкциям мастера установки.
4. После завершения установки запустите Консоль администрирования и убедитесь, что плагин присутствует в списке установленных плагинов, как описано в предыдущей процедуре.

При запуске Консоли администрирования после установки плагина управления, который поддерживает мастер первоначальной настройки управляемых приложений, этот мастер запускается автоматически. Вы можете выполнить шаги мастера первоначальной настройки управляемых приложений, чтобы создать политики и задачи приложений "Лаборатории Касперского" по умолчанию. Мастер запускается автоматически только при запуске Консоли администрирования после первоначальной установки плагина или после обновления плагина управления до версии, совместимой с другой версией приложения

"Лаборатории Касперского", для которого еще не созданы задачи и политики. Вы также можете запустить мастер первоначальной настройки управляемых приложений вручную.

► *Чтобы запустить мастер первоначальной настройки управляемых приложений вручную:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла Сервера администрирования выберите пункт **Все задачи → Мастер первоначальной настройки управляемых приложений**.
3. Запустится мастер первоначальной настройки управляемых приложений. Следуйте инструкциям мастера, чтобы создать политики и задачи приложений "Лаборатории Касперского" с параметрами по умолчанию.

► *Чтобы удалить плагин управления:*

1. Если Консоль администрирования запущена, закройте ее.
2. Откройте редактор реестра операционной системы Windows.
3. Найдите следующий ключ:
 - `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins` для 32-разрядной системы.
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins` для 64-разрядной системы.

Ключ содержит установленные плагины управления. Для каждого плагина значение `DisplayName` содержит имя плагина, а значение `UninstallString` содержит команду для удаления плагина.

4. Найдите ключ плагина, который вы хотите удалить, и скопируйте его значение `UninstallString` в буфер обмена.
5. Вставьте значение в командную строку и запустите ее с правами системного администратора.

Версия плагина управления не должна быть ниже, чем версия управляемого приложения "Лаборатории Касперского". При обновлении приложения "Лаборатории Касперского" на устройствах необходимо установить плагин управления той же версии.

При открытии политики, созданной в более ранней версии плагина, вам будет предложено принять Положение о Kaspersky Security Network.

При удалении Kaspersky Security Center Web Console также удаляются все плагины управления.

Если вы откроете и сохраните политику в версии плагина, более поздней, чем версия управляемого приложения, политика будет обновлена, и вы не сможете открыть ее в плагине более ранней версии.

Просмотр отчета о развертывании защиты

Для отслеживания процесса развертывания защиты в сети можно использовать отчет о развертывании защиты.

► *Чтобы просмотреть отчет о развертывании защиты:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В рабочей области узла выберите вкладку **Отчеты**.
3. В рабочей области вкладки **Отчеты** выберите шаблон отчета **Просмотреть отчет о развертывании защиты**.

В рабочей области будет сформирован отчет, содержащий информацию о развертывании защиты на всех устройствах сети.

Вы можете сформировать новый отчет о развертывании защиты и указать, информацию какого типа в него следует включать (см. раздел «Работа с отчетами» на стр. [602](#)):

- для группы администрирования;
- для набора устройств;
- для выборки устройств;
- для всех устройств.

В рамках Kaspersky Security Center считается, что на устройстве развернута защита в том случае, когда на нем установлено приложение безопасности и включена постоянная защита.

Удаленная деинсталляция приложений

Kaspersky Security Center позволяет удаленно деинсталлировать приложения с устройств с помощью задач удаленной деинсталляции. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам, вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования.** В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка.** Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
- **Назначить задачу выборке устройств.** В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать predetermined выборку или вашу собственную выборку.
- **Назначить задачу группе администрирования.** В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

В этом разделе

Удаленная деинсталляция приложения с клиентских устройств группы администрирования	371
Удаленная деинсталляция приложения с выбранных устройств	371

Удаленная деинсталляция приложения с клиентских устройств группы администрирования

► Чтобы удаленно деинсталлировать приложение с клиентских устройств группы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области выберите вкладку **Задачи**.
4. Запустите мастер создания задачи по кнопке **Новая задача**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция приложения**.

В результате работы мастера создания задачи будет создана групповая задача удаленной деинсталляции выбранного приложения. Созданная задача отображается в рабочей области группы администрирования, на вкладке **Задачи**.

5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной деинсталляции выбранное приложение будет удалено с клиентских устройств группы администрирования.

Удаленная деинсталляция приложения с выбранных устройств

► Чтобы удаленно деинсталлировать приложение с выбранных устройств:

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания задачи по кнопке **Новая задача**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция приложения**.

В результате работы мастера создания задачи будет создана задача удаленной деинсталляции выбранного приложения для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.

3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранное приложение будет удалено с выбранных устройств.

Работа с инсталляционными пакетами

При создании задач удаленной установки используются инсталляционные пакеты, которые содержат набор параметров, необходимых для установки приложения.

Инсталляционные пакеты могут содержать в себе файл ключа. Не рекомендуется размещать в открытом доступе инсталляционные пакеты, содержащие в себе файл ключа.

Вы можете использовать один и тот же инсталляционный пакет многократно.

Сформированные для Сервера администрирования инсталляционные пакеты размещаются в дереве консоли в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебной папке Packages.

В этом разделе

Создание инсталляционного пакета	372
Создание автономного инсталляционного пакета.....	374
Создание пользовательского инсталляционного пакета	376
Просмотр и изменение свойств пользовательских инсталляционных пакетов	377
Получение инсталляционного пакета Агента администрирования из комплекта поставки Kaspersky Security Center	378
Распространение инсталляционных пакетов на подчиненные Серверы администрирования.....	379
Распространение инсталляционных пакетов с помощью точек распространения	380
Передача в Kaspersky Security Center информации о результатах установки приложения.....	380
Определение адреса прокси-сервера KSN для инсталляционных пакетов	381

Создание инсталляционного пакета.

В этом разделе описана процедура создания следующих типов инсталляционных пакетов:

- инсталляционный пакет приложения "Лаборатории Касперского";
- инсталляционный пакет указанного исполняемого файла;
- инсталляционный пакет приложения из базы "Лаборатории Касперского".

Инсталляционный пакет для удаленной установки Агента администрирования не нужно создавать вручную. Он формируется автоматически при установке приложения Kaspersky Security Center и располагается в папке **Инсталляционные пакеты**. Если пакет для удаленной установки Агента администрирования был удален, то для его повторного формирования в качестве файла с описанием вам нужно выбрать файл `nagent.kud`, расположенный в папке NetAgent дистрибутива Kaspersky Security Center.

► Чтобы создать инсталляционный пакет:

1. Подключитесь к нужному Серверу администрирования.

2. В дереве консоли выберите папку **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
3. Запустите процесс создания автономного инсталляционного пакета одним из следующих способов:
 - В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Новый** → **Инсталляционный пакет**.
 - В контекстном меню пустого списка инсталляционных пакетов выберите пункт **Новый** → **Инсталляционный пакет**.
 - Перейдите по ссылке **Создать инсталляционный пакет** в блоке управления списком инсталляционных пакетов.

Запустится мастер создания инсталляционного пакета.

4. Выберите один из следующих типов инсталляционных пакетов, нажав на соответствующий значок:
 - Инсталляционный пакет приложения "Лаборатории Касперского".
 - Инсталляционный пакет указанного исполняемого файла.
 - Инсталляционный пакет приложения из базы "Лаборатории Касперского".
5. Укажите имя инсталляционного пакета, который будет создан.

Вы можете указать любое имя.

6. Выберите приложение или исполняемый файл, для которого требуется создать инсталляционный пакет, одним из следующих способов:
 - Нажмите на кнопку **Обзор** и в стандартном окне **Открыть** выберите дистрибутив нужного приложения, расположенный на доступных дисках.
Этот вариант применим, если вы выбрали создание инсталляционного пакета для приложения "Лаборатории Касперского" или для указанного исполняемого файла.
 - Нажмите на кнопку **Обзор** и в окне **Выбор приложения** выберите дистрибутив нужного приложения.
Этот вариант применим, если вы выбрали создание инсталляционного пакета для приложений из базы "Лаборатории Касперского".

Если вы создаете инсталляционный пакет для Сервера администрирования, выберите файл sc.kud. Файл sc.kud находится в корневой папке дистрибутива Kaspersky Security Center.

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

7. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности.
При создании инсталляционного пакета приложения вам может быть предложено просмотреть и принять Лицензионное соглашение и Политику конфиденциальности этого приложения.
Прочтите оба документа. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, примите их, установив соответствующие флажки.
Установка приложения на ваше устройство продолжится, и создание инсталляционного пакета возобновится.

Если вы создаете инсталляционный пакет приложения Kaspersky Endpoint Security для Mac, вы можете выбрать язык Лицензионного соглашения и Политики конфиденциальности.

8. При необходимости включите автоматическую установку компонентов системы.

Если вы создаете инсталляционный пакет приложения из базы "Лаборатории Касперского", вы можете включить автоматическую установку необходимых системных компонентов. Мастер создания инсталляционного пакета отображает список всех возможных общесистемных компонентов для выбранного приложения. Вы можете получить доступ к этому списку в свойствах инсталляционного пакета в любое время.

Если вы создаете инсталляционный пакет патча, в список будут включены все системные компоненты, необходимые для развертывания этого патча.

9. Нажмите на кнопку **Готово**, чтобы завершить создание пакета.

После завершения работы мастера созданный инсталляционный пакет отобразится в рабочей области папки **Инсталляционные пакеты**.

См. также

Основной сценарий установки.....[56](#)

Создание автономного инсталляционного пакета

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для ручной установки приложений на устройства.

Автономный инсталляционный пакет представляет собой исполняемый файл (installer.exe), который можно разместить на Веб-сервере, в общей папке или передать на клиентское устройство другим способом. Можно также отправить ссылку на автономный инсталляционный пакет по электронной почте. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки приложения без участия Kaspersky Security Center.

Убедитесь, что автономный инсталляционный пакет не доступен для неавторизованных лиц.

Вы можете создавать автономные инсталляционные пакеты как для приложений "Лаборатории Касперского", так и для приложений сторонних производителей для Windows, macOS и Linux. Чтобы создать автономный инсталляционный пакет для приложений сторонних производителей, необходимо сначала создать пользовательский инсталляционный пакет (см. раздел "Создание пользовательского инсталляционного пакета" на стр. [376](#)).

Источником для создания автономных инсталляционных пакетов являются инсталляционные пакеты в списке созданных на Сервере администрирования.

► Чтобы создать автономный инсталляционный пакет:

1. В дереве консоли выберите узел **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. В списке инсталляционных пакетов выберите инсталляционный пакет, для которого требуется создать автономный пакет.
3. В контекстном меню выберите пункт **Создать автономный инсталляционный пакет**.

В результате запускается мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На первой странице мастера, если вы выбрали инсталляционный пакет для приложения "Лаборатории Касперского" и хотите установить Агент администрирования вместе с выбранным приложением, убедитесь, что параметр **Установить Агент администрирования совместно с данным приложением** включен.

По умолчанию параметр включен. Рекомендуется включить этот параметр, если вы не уверены, установлен ли на устройстве Агент администрирования. Если Агент администрирования уже установлен на устройстве, после установки автономного инсталляционного пакета с Агентом администрирования, Агент администрирования будет обновлен до более новой версии.

Если вы выключите этот параметр, Агент администрирования не будет установлен на устройство, и устройство не будет управляемым.

Если автономный инсталляционный пакет для выбранного приложения уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вам нужно выбрать одно из следующих действий:

- **Создать автономный инсталляционный пакет.** Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии приложения, и чтобы также остался автономный инсталляционный пакет для предыдущей версии приложения, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.
- **Использовать существующий автономный инсталляционный пакет.** Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.
- **Сформировать заново существующий автономный инсталляционный пакет.** Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этого же приложения еще раз. Автономный инсталляционный пакет размещается в той же папке.

5. На следующей странице мастера выберите параметр **Переместить нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентские устройства, после установки на них Агента администрирования.

По умолчанию устройства перемещаются в группу **Управляемые устройства**.

Если вы не хотите перемещать клиентское устройство в какую-либо группу администрирования после установки Агента администрирования, выберите параметр **Не перемещать устройства**.

6. На следующей странице мастера, после завершения процесса создания автономного инсталляционного пакета, отобразится результат создания автономного инсталляционного пакета и путь к нему.

Можно перейти по ссылкам и выполнить следующие действия:

- Открыть папку с автономным инсталляционным пакетом.
- Отправить по электронной почте ссылку на созданный автономный инсталляционный пакет. Для этого необходимо, чтобы было запущено приложение для работы с электронной почтой.
- Скопировать образец HTML-кода, чтобы разместить ссылку на веб-сайте. Текстовый файл (в формате TXT) создается и открывается с помощью приложения, связанного с TXT-форматом. В файле отображается <a> HTML-тег с атрибутами.

7. Если вы хотите открыть список автономных инсталляционных пакетов, на следующей странице мастера включите параметр **Открыть список автономных пакетов**.
8. Нажмите на кнопку **Готово**.

Мастер создания автономного инсталляционного пакета закрывается.

Автономный инсталляционный пакет создан и помещен во вложенную папку PkgInst общей папки Сервера администрирования (см. раздел "Задание папки общего доступа" на стр. [227](#)). Вы можете просмотреть список автономных инсталляционных пакетов, нажав на кнопку **Просмотреть список автономных пакетов**, расположенную над списком инсталляционных пакетов.

Создание пользовательского инсталляционного пакета

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любое приложение (например, текстовый редактор) на клиентские устройства, например, с помощью задачи;
- создать автономный инсталляционный пакет (см. раздел "Создание автономного инсталляционного пакета" на стр. [374](#)).

Пользовательский инсталляционный пакет – это папка с набором файлов. Источником для создания пользовательского инсталляционного пакета является *архивный файл*. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет. Создавая пользовательский инсталляционный пакет, вы можете указать параметры командной строки, например, для установки приложения в тихом режиме.

► Чтобы создать пользовательский инсталляционный пакет:

1. В дереве консоли выберите **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
Отобразится список инсталляционных пакетов доступных на Сервере администрирования.
2. Нажмите на кнопку **Создать инсталляционный пакет** над списком инсталляционных пакетов.
Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На первой странице мастера выберите параметр **Создать инсталляционный пакет для указанного исполняемого файла**.
4. На следующей странице мастера укажите имя пользовательского инсталляционного пакета.
5. На следующей странице мастера нажмите на кнопку **Обзор** и в стандартном окне **Открыть** выберите файл архива, расположенный на доступных дисках, чтобы создать пользовательский инсталляционный пакет.
Вы можете загрузить архивный файл формата ZIP, CAB, TAR или TAR.GZ. Создать инсталляционный пакет из файла формата SFX (самораспаковывающийся архив) невозможно.
Файлы загружены на Сервер администрирования Kaspersky Security Center.
6. На следующей странице мастера укажите параметры командной строки для исполняемого файла.
Вы можете указать параметры командной строки для установки приложения из инсталляционного пакета в тихом режиме. Указывать параметры командной строки необязательно.

При необходимости настройте следующие параметры:

- Копировать всю папку в инсталляционный пакет
- Конвертировать параметры на рекомендуемые значения для приложений, распознаваемых Kaspersky Security Center

Начнется процесс создания пользовательского инсталляционного пакета.

В окне мастера отобразится информация о завершении процесса.

Если пользовательский инсталляционный пакет не создан, отобразится соответствующее сообщение.

7. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования (см. раздел "Задание папки общего доступа" на стр. [227](#)). После загрузки пользовательский инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов на Сервере администрирования можно просмотреть и изменить свойства пользовательского инсталляционного пакета (см. раздел "Просмотр и изменение свойств пользовательских инсталляционных пакетов" на стр. [377](#)).

Просмотр и изменение свойств пользовательских инсталляционных пакетов

После создания пользовательского инсталляционного пакета в окне свойств можно просмотреть общую информацию о нем и указать параметры установки.

► *Чтобы просмотреть и изменить свойства пользовательского инсталляционного пакета:*

1. В дереве консоли выберите **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. В контекстном меню инсталляционного пакета выберите пункт **Свойства**.

Откроется окно свойств выбранного инсталляционного пакета.

3. Отобразится следующая информация:

- название инсталляционного пакета;
- название приложения, упакованного в пользовательский инсталляционный пакет;
- версия приложения;
- дата создания инсталляционного пакета;
- путь к пользовательскому инсталляционному пакету на Сервере администрирования;
- параметры запуска исполняемого файла.

4. Задайте следующие параметры:

- Название инсталляционного пакета
- **Устанавливать требуемые общесистемные компоненты**

Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (прerequisites), необходимые для установки этого обновления. Например, такими prerequisites могут являться обновления операционной системы.

Если этот параметр выключен, необходимо установить пререквизиты вручную.

По умолчанию параметр выключен.

Этот параметр доступен, только если приложение, добавленное в инсталляционный пакет, было распознано Kaspersky Security Center.

- **Параметры запуска исполняемого файла**

Если приложению требуются дополнительные параметры для установки без вывода сообщений, укажите их в этом поле. Дополнительную информацию см. в документации производителя.

Вы также можете указать и другие параметры.

Этот параметр доступен только для пакетов, которые не были созданы на основе приложений "Лаборатории Касперского".

5. Нажмите на кнопку **ОК** или **Применить**, чтобы сохранить изменения.

Новые параметры сохранены.

См. также:

Создание пользовательского инсталляционного пакета[376](#)

Получение инсталляционного пакета Агента администрирования из комплекта поставки Kaspersky Security Center

Вы можете получить инсталляционный пакет Агента администрирования из комплекта поставки Kaspersky Security Center без необходимости установки Kaspersky Security Center. Затем вы можете использовать инсталляционный пакет для установки Агента администрирования на клиентские устройства.

► *Чтобы получить инсталляционный пакет Агента администрирования из комплекта поставки Kaspersky Security Center:*

1. Запустите исполняемый файл ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe из дистрибутива Kaspersky Security Center.
2. В появившемся окне перейдите по ссылке **Извлечь инсталляционные пакеты**.
3. В списке инсталляционных пакетов установите флажок рядом с инсталляционным пакетом Агента администрирования и нажмите на кнопку **Далее**.
4. При необходимости нажмите на кнопку **Обзор**, чтобы изменить отображаемую папку для извлечения инсталляционного пакета.
5. Нажмите на кнопку **Распаковать**.
Приложение извлекает инсталляционный пакет Агента администрирования.
6. После завершения процесса, нажмите на кнопку **Заккрыть**.

Инсталляционный пакет Агента администрирования распаковывается в выбранную папку.

С помощью инсталляционного пакета вы можете установить Агент администрирования одним из следующих способов:

- Локально (см. раздел "Локальная установка Агента администрирования" на стр. [193](#)) запустив файл setup.exe из извлеченной папки.
- С помощью автоматической установки (см. раздел "Установка Агента администрирования в тихом режиме (без файла ответов)" на стр. [180](#)).
- С помощью механизма групповых политик Microsoft Windows (см. раздел "Развертывание с помощью механизма групповых политик Microsoft Windows" на стр. [169](#)).

См. также:

Основной сценарий установки.....	56
Локальная установка Агента администрирования.....	193
Установка Агента администрирования в тихом режиме (без файла ответов).....	180
Развертывание с помощью механизма групповых политик Microsoft Windows	169

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

► Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.
2. Запустите создание задачи распространения инсталляционного пакета на подчиненные Серверы администрирования одним из следующих способов:
 - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи для этой группы.
 - Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи для набора устройств.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Распространение инсталляционного пакета**.

В результате работы мастера создания задачи будет создана задача распространения выбранных инсталляционных пакетов на выбранные подчиненные Серверы администрирования.

3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи выбранные инсталляционные пакеты будут скопированы на выбранные подчиненные Серверы администрирования.

Распространение инсталляционных пакетов с помощью точек распространения

Для распространения инсталляционных пакетов в пределах группы администрирования вы можете использовать точки распространения.

После получения инсталляционных пакетов с Сервера администрирования точки распространения автоматически распространяют их на клиентские устройства с помощью многоадресной IP-рассылки. IP-рассылка новых инсталляционных пакетов в пределах группы администрирования производится один раз. Если в момент рассылки клиентское устройство было отключено от сети организации, то при запуске задачи установки Агент администрирования клиентского устройства автоматически скачивает необходимый инсталляционный пакет с точки распространения.

Передача в Kaspersky Security Center информации о результатах установки приложения

После создания инсталляционного пакета приложения вы можете настроить инсталляционный пакет таким образом, чтобы диагностическая информация о результатах установки приложения передавалась в Kaspersky Security Center. Для инсталляционных пакетов приложений "Лаборатории Касперского" передача диагностической информации о результате установки приложений настроена по умолчанию, дополнительная настройка не требуется.

► *Чтобы настроить передачу в Kaspersky Security Center диагностической информации о результате установки приложения:*

1. Перейдите в папку инсталляционного пакета, сформированного средствами Kaspersky Security Center для выбранного приложения. Эта папка расположена в папке общего доступа, которая была указана при установке Kaspersky Security Center.
2. Откройте файл с расширением kpd или kud для редактирования (например, с помощью текстового редактора "Блокнот" Microsoft Windows).

Файл имеет формат обычного конфигурационного ini-файла.

3. Добавьте в файл следующие строки:

```
[SetupProcessResult]  
Wait=1
```

Эта команда настраивает приложение Kaspersky Security Center таким образом, чтобы оно ожидало окончания установки приложения, для которого сформирован инсталляционный пакет и анализировала код возврата приложения установки. Если нужно отключить передачу диагностической информации, установите для ключа Wait значение 0.

4. Внесите описание кодов возврата успешной установки. Для этого добавьте в файл следующие строки:

```
[SetupProcessResult_SuccessCodes]  
<код возврата>=[<описание>]  
<код возврата 1>=[<описание>]  
...
```

В квадратных скобках приводятся необязательные ключи.

Синтаксис строк:

- `<код возврата>`. Любое число, соответствующее коду возврата приложения установки. Количество кодов возврата может быть произвольным.
 - `<описание>`. Текстовое описание результата установки. Описание может отсутствовать.
5. Внесите описание кодов возврата для установки, завершенной с ошибкой. Для этого добавьте в файл следующие строки:

```
[SetupProcessResult_ErrorCodes]
<код возврата>=[<описание>]
<код возврата 1>=[<описание>]
...
```

Синтаксис строк соответствует синтаксису строк кодов возврата при успешной установке.

6. Закройте kpd- или kud-файл, сохранив внесенные изменения.

Информация о результатах установки приложения, указанного пользователем, будет записываться в журнал Kaspersky Security Center и отображаться в списке событий, в отчетах и в результатах выполнения задач.

Определение адреса прокси-сервера KSN для инсталляционных пакетов

В случае изменения адреса или домена Сервера администрирования вы можете указать адрес прокси-сервера KSN для инсталляционного пакета.

► *Чтобы определить адрес прокси-сервера KSN для инсталляционного пакета:*

1. В дереве консоли в папке **Удаленная установка** двойным щелчком мыши нажмите на вложенную папку **Инсталляционные пакеты**.
2. В появившемся окне нажмите на кнопку **Свойства**.
3. В отобразившемся окне свойств выберите подраздел **Общие**.
4. В подразделе **Общие** окна свойств введите адрес прокси-сервера KSN.

Инсталляционные пакеты будут использовать этот адрес по умолчанию.

Получение актуальных версий приложений

Kaspersky Security Center позволяет получать актуальные версии корпоративных приложений, хранящиеся на серверах "Лаборатории Касперского".

► *Чтобы получить актуальные версии корпоративных приложений "Лаборатории Касперского":*

1. Выполните одно из следующих действий:
 - В дереве консоли выберите узел с именем нужного вам Сервера администрирования на вкладке **Мониторинг** в разделе **Развертывание** перейдите по ссылке **Вышли новые версии приложений "Лаборатории Касперского"**.

Ссылка **Вышли новые версии приложений "Лаборатории Касперского"** становится доступна, когда Сервер администрирования обнаруживает очередную версию корпоративного приложения на интернет-сервере "Лаборатории Касперского".

- В дереве консоли выберите **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**, в рабочей области нажмите **Дополнительные действия** и в раскрывающемся списке выберите пункт **Просмотреть актуальные версии приложений "Лаборатории Касперского"**.

Появится список текущих версий приложений "Лаборатории Касперского".

2. Можно отфильтровать список приложений "Лаборатории Касперского", чтобы упростить поиск нужного приложения.

В верхней части окна **Текущие версии приложений** перейдите по ссылке **Фильтр** для фильтрации списка приложений по следующим критериям:

- **Компоненты.** Используйте этот критерий, чтобы отфильтровать список приложений "Лаборатории Касперского" по областям защиты, которые используются в вашей сети.
- **Тип ПО для загрузки.** Используйте этот критерий, чтобы отфильтровать список приложений "Лаборатории Касперского" по типу приложения.
- **Какие обновления и ПО показывать.** Используйте этот критерий, чтобы отобразить доступные приложения "Лаборатории Касперского" по определенным версиям.
- **На каких языках показывать ПО и обновления.** Используйте этот критерий для отображения приложений "Лаборатории Касперского" с определенным языком локализации.

Нажмите на кнопку **Применить**, чтобы применить изменения.

3. Выберите в списке нужное вам приложение.
4. Загрузите дистрибутив приложения по ссылке в строке **Веб-адрес дистрибутива**.

Для обновлений управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center. Если эта версия более поздняя, чем ваша текущая, эти обновления отображаются, но не могут быть одобрены. Также из таких обновлений невозможно создать инсталляционные пакеты, пока вы не обновите Kaspersky Security Center. Вам будет предложено обновить ваш экземпляр Kaspersky Security Center до необходимой минимальной версии.

Если для выбранного приложения отображается кнопка **Загрузить приложения и создать инсталляционные пакеты**, вы можете нажать на эту кнопку для загрузки дистрибутива приложения и автоматического создания инсталляционного пакета. В этом случае Kaspersky Security Center загружает дистрибутив приложения на Сервер администрирования в папку общего доступа, заданную при установке Kaspersky Security Center. Список автоматически созданных инсталляционных пакетов отображается в папке дерева консоли **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**.

После закрытия окна **Текущие версии приложений** ссылка **Вышли новые версии приложений "Лаборатории Касперского"** исчезнет из раздела **Развертывание**.

Вы можете создавать инсталляционные пакеты новых версий приложений и работать с созданными инсталляционными пакетами в папке **Удаленная установка** дерева консоли, во вложенной папке **Инсталляционные пакеты**.

Вы также можете открыть окно **Текущие версии приложений** по ссылке **Просмотреть актуальные версии приложений "Лаборатории Касперского"** в рабочей области папки **Инсталляционные пакеты**.

См. также:

Замещение приложений безопасности сторонних производителей.....	358
Установка приложений с помощью задачи удаленной установки	359
Установка приложений с помощью мастера удаленной установки	363
Работа с плагинами управления	368
Просмотр отчета о развертывании защиты	369
Удаленная деинсталляция приложений	370
Работа с инсталляционными пакетами	371
Подготовка устройства под управлением Windows к удаленной установке	383
Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux.....	384
Подготовка устройства с операционной системой macOS к удаленной установке Агента администрирования.....	387
Создание инсталляционного пакета.	372

Подготовка устройства под управлением Windows к удаленной установке

Удаленная установка приложения на клиентском устройстве может завершаться с ошибкой по следующим причинам:

- Задача ранее уже была успешно выполнена на этом устройстве.
В этом случае ее повторное выполнение не требуется.
- Во время запуска задачи устройство было выключено.
В этом случае требуется включить устройство и запустить задачу еще раз.
- Отсутствует связь между Сервером администрирования и Агентом администрирования, установленным на клиентском устройстве.
Для определения причины проблемы вы можете воспользоваться утилитой удаленной диагностики клиентского устройства (klactgui).
- Если на устройстве не установлен Агент администрирования, при удаленной установке приложения могут возникнуть следующие проблемы:
 - на клиентском устройстве включен **Отключить простой общий доступ к файлам**;
 - на клиентском устройстве не работает служба Server;

- на клиентском устройстве закрыты необходимые порты;
- у учетной записи, под которой выполняется задача, недостаточно прав.

Чтобы избежать проблем, которые могут возникнуть при установке приложения на клиентское устройство без установленного Агента администрирования, необходимо действовать, как описано в процедуре принудительного развертывания с помощью задачи удаленной установки Kaspersky Security Center (см. раздел "Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center" на стр. [171](#)).

Ранее использовалась утилита `girper` для подготовки устройства к удаленной установке. Теперь это считается устаревшим способом настройки операционных систем. Утилиту `girper` не рекомендуется использовать на операционных системах версий Windows XP и Windows Server 2003 R2 и выше.

Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux

Установка Агента администрирования состоит из двух шагов:

- Подготовка устройства с операционной системой Linux
- Удаленная установка Агента администрирования

Подготовка устройства с операционной системой Linux

► Чтобы подготовить устройство с операционной системой Linux к удаленной установке Агента администрирования:

1. Убедитесь, что на целевом устройстве с операционной системой Linux установлено следующее программное обеспечение:
 - Sudo.
 - Интерпретатор языка Perl версии 5.10 или выше.
2. Выполните проверку конфигурации устройства:
 - a. Проверьте, что возможно подключение к устройству через SSH (например, приложение PuTTY).

Если вы не можете подключиться к устройству, откройте файл `/etc/ssh/sshd_config` и убедитесь, что следующие параметры имеют значения:

```
PasswordAuthentication no
ChallengeResponseAuthentication yes
```

Не изменяйте файл `/etc/ssh/sshd_config`, если вы можете без проблем подключиться к устройству; в противном случае вы можете столкнуться с ошибкой аутентификации SSH при выполнении задачи удаленной установки.

Сохраните файл (при необходимости) и перезапустите службу SSH, используя команду `sudo service ssh restart`.

- b. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.
- c. Используйте команду `sudo visudo`, чтобы открыть конфигурационный файл `sudoers`.

В открывшемся файле найдите строку, начинающуюся с `%sudo` (или с `%wheel` если вы используете операционную систему CentOS). Под этой строкой укажите следующее: `<имя пользователя> ALL = (ALL) NOPASSWD: ALL`. В этом случае `<имя пользователя>` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH. Если вы используете операционную систему Astra Linux, в файл `/etc/sudoers` добавьте последней строку со следующим текстом: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

- d. Сохраните и закройте файл `sudoers`.
 - e. Повторно подключитесь к устройству через SSH и проверьте, что служба `sudo` не требует пароль, с помощью команды `sudo whoami`.
3. Откройте файл `/etc/systemd/logind.conf` и выполните одно из следующих действий:
 - Укажите значение 'no' для параметра `KillUserProcesses`: `KillUserProcesses=no`.
 - Для параметра `KillExcludeUsers` введите имя пользователя учетной записи, под которой будет выполняться удаленная установка, например, `KillExcludeUsers=root`.

Если целевое устройство работает под управлением Astra Linux, добавьте строку `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` в файл `/home/<имя пользователя>/.bashrc`, где `<имя пользователя>` — учетная запись пользователя, которая будет использоваться для подключения устройства с помощью SSH.

Чтобы применить измененный параметр, перезапустите устройство под управлением Linux или выполните следующую команду:

```
$ sudo systemctl restart systemd-logind.service
```

4. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет `insserv-compat` (см. раздел "Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования" см. стр. [386](#)), чтобы настроить Агент администрирования.
5. Если вы хотите установить Агент администрирования на устройства с операционной системой Astra Linux, работающей в режиме замкнутой программной среды, выполните дополнительные действия для подготовки устройств Astra Linux (см. раздел "Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования" на стр. [196](#)).

Удаленная установка Агента администрирования

- Чтобы установить Агент администрирования на устройство с операционной системой Linux:

1. Загрузите и создайте инсталляционный пакет:
 - a. Перед установкой пакета на устройство убедитесь, что на нем установлены зависимости (программы, библиотеки) для данного пакета.

Вы можете самостоятельно посмотреть зависимости для каждого пакета, используя утилиты, специфичные для того дистрибутива Linux, на который будет устанавливаться пакет. С информацией об утилитах вы можете ознакомиться в документации к вашей операционной системе.

- b. Загрузите инсталляционный пакет Агента администрирования с помощью интерфейса приложения или с веб-сайта "Лаборатории Касперского" <https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint>.
 - c. Для создания пакета удаленной установки используйте файлы:
 - `klnagent.kpd`;
 - `akinstall.sh`;
 - `deb` или `rpm` пакет Агента администрирования.
2. Создайте задачу удаленной установки приложения с параметрами:
 - В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
 - На странице **Выбор учетной записи для запуска задачи** укажите параметры учетной записи, которая используется для подключения к устройству через SSH.
 3. Запустите задачу удаленной установки приложения. Используйте параметр для команды `su`, чтобы сохранить среду: `-m, -p, --preserve-environment`.

Установка может завершиться ошибкой, если вы устанавливаете Агент администрирования с использованием протокола SSH на устройства с операционными системами Fedora версии ниже 20. В этом случае для успешной установки Агента администрирования в файле `/etc/sudoers` закомментируйте параметр `Defaults requiretty` (закройте его в синтаксис комментария, чтобы удалить его из проанализированного кода). Подробное описание того, почему параметр `Defaults requiretty` может вызывать проблемы при подключении по SSH, вы можете найти на сайте системы отслеживания проблем Bugzilla (https://bugzilla.redhat.com/show_bug.cgi?id=1020147).

Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования

- Чтобы установить Агент администрирования на устройство с операционной системой SUSE Linux Enterprise Server 15,

перед установкой Агента администрирования выполните следующую команду:

```
$ sudo zypper install insserv-compat
```

Это позволит вам установить пакет `insserv-compat` и правильно настроить Агент администрирования.

Выполните команду `rpm -q insserv-compat`, чтобы проверить, если пакет уже установлен.

Если в вашей сети много устройств под управлением SUSE Linux Enterprise Server 15, вы можете использовать специальное программное обеспечение для настройки и управления инфраструктурой компании. Используя это программное обеспечение, вы можете автоматически установить пакет `insserv-compat` сразу на все необходимые устройства. Например, вы можете использовать Puppet, Ansible, Chef, или сделать свой скрипт любым удобным для вас способом.

Если на устройстве нет ключей подписи GPG для SUSE Linux Enterprise, вы можете увидеть следующее предупреждение: `Package header is not signed!` Выберите параметр `i`, чтобы игнорировать предупреждение.

Помимо установки пакета `insserv-compat`, убедитесь, что ваши Linux-устройства полностью подготовлены (см. раздел "Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux" на стр. [384](#)). После этого разверните и установите Агент администрирования.

Подготовка устройства с операционной системой macOS к удаленной установке Агента администрирования

► Чтобы подготовить устройство с операционной системой macOS к удаленной установке Агента администрирования:

1. Убедитесь, что на целевом устройстве с операционной системой macOS установлено приложение `sudo`.
2. Выполните проверку конфигурации устройства:

- a. Убедитесь, что порт 22 открыт на клиентском устройстве. Для этого в разделе **Системные настройки** откройте панель **Обмен** и убедитесь, что установлен флажок **Удаленный вход**.

Вы можете подключиться к клиентскому устройству по протоколу Secure Shell (SSH) только через порт 22. Вы не можете изменить номер порта.

Вы можете использовать команду `ssh <имя_устройства>` для удаленного входа на устройство macOS. В панели **Общий доступ** можно использовать параметр **Разрешить доступ для** чтобы задать область действия пользователей, которым разрешен доступ к устройству macOS.

- b. Отключите пароль запроса `sudo` для учетной записи пользователя, которая используется для подключения к устройству.

Используйте команду `sudo visudo`, чтобы открыть конфигурационный файл `sudoers` в терминале. В файле, который вы открыли, в поле **Спецификация привилегий пользователя** укажите следующее: `username ALL = (ALL) NOPASSWD: ALL`. В этом случае `username` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH.

- c. Сохраните и закройте файл `sudoers`.
 - d. Повторно подключитесь к устройству через SSH и проверьте, что служба `sudo` не требует пароль, с помощью команды `sudo whoami`.
3. Загрузите и создайте инсталляционный пакет:

- a. Загрузите инсталляционный пакет Агента администрирования одним из следующих способов:
 - В дереве консоли, в контекстном меню выбрав **Удаленная установка** → **Инсталляционные пакеты** и далее **Показать текущие версии приложений**, чтобы выбрать из доступных пакетов.
 - Загрузив соответствующую версию Агента администрирования с веб-сайта Службы технической поддержки по адресу <https://support.kaspersky.ru/> <https://support.kaspersky.com>.
 - Запросив инсталляционный пакет у специалистов Службы технической поддержки.
- b. Для создания пакета удаленной установки используйте файлы:
 - `klagent.kud`
 - `install.sh`
 - `klagentmac.dmg`

4. Создайте задачу удаленной установки приложения с параметрами:

- В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
- В окне **Выбор учетной записи для запуска задачи** для запуска задачи укажите параметры учетной записи, которая используется для подключения к устройству через SSH.

Клиентское устройство готово к удаленной установке Агента администрирования с помощью соответствующей задачи, которую вы создали.

Приложения "Лаборатории Касперского": лицензирование и активация

В этом разделе описаны возможности Kaspersky Security Center по работе с лицензионными ключами управляемых приложений "Лаборатории Касперского".

Kaspersky Security Center позволяет централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

При добавлении лицензионного ключа с помощью Kaspersky Security Center свойства лицензионного ключа сохраняются на Сервере администрирования. На основании этой информации приложение формирует отчет об использовании лицензионных ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах лицензионных ключей. Вы можете настраивать параметры оповещений об использовании лицензионных ключей в составе параметров Сервера администрирования.

См. также:

Основной сценарий установки.....	56
Лицензии и возможности Kaspersky Security Center.....	29

В этом разделе

Лицензирование управляемых приложений	389
Просмотр информации об используемых лицензионных ключах	391
Добавление лицензионного ключа в хранилище Сервера администрирования.	392
Удаление лицензионного ключа Сервера администрирования	393
Распространение лицензионного ключа на клиентские устройства.	394
Автоматическое распространение лицензионного ключа.	398
Создание и просмотр отчета об использовании лицензионных ключей	399
Просмотр информации о лицензионных ключах приложения.....	400
Экспорт файла ключа	400

Лицензирование управляемых приложений

Приложения "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения файла ключа или кода активации к каждому из приложений. Файл ключа или код активации может быть распространен следующими способами:

- с помощью автоматического распространения;
- с помощью инсталляционного пакета управляемого приложения;
- с помощью задачи *Добавление лицензионного ключа* управляемого приложения;
- активация управляемого приложения вручную.

Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. Приложение "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Приложение, для которого вы добавляете лицензионный ключ, определяет, является ли ключ активным или резервным. Определение ключа не зависит от способа, который вы используете для добавления лицензионного ключа.

Автоматическое распространение

Если вы используете разные управляемые приложения и вам важно распространить определенный файл ключ или код активации на устройства, используйте другие способы распространения кода активации или ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Для всех лицензионных ключей установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства**. На устройствах организации установлено приложение безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Приложение определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае невозможно предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

При распространении лицензионного ключа на устройства происходит подсчет устройств для данного лицензионного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение (см. раздел "События превышения лицензионного ограничения" см. стр. [341](#)), таким устройствам будет присвоен статус *Критический*.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
 - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. [392](#)).

- Автоматическое распространение лицензионного ключа (на стр. [398](#)).

Или

- Kaspersky Security Center Web Console:
 - Добавление лицензионного ключа в хранилище Сервера администрирования.
 - Автоматическое распространение лицензионного ключа.

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для приложения.
- Виртуальный Сервер администрирования не имеет управляемых устройств.
- Лицензионный ключ уже используется для устройств, управляемых другим виртуальным Сервером администрирования, и достигнуто лицензионное ограничение на количество устройств.

Добавление файла ключа или кода активации в инсталляционный пакет управляемого приложения

Из соображений безопасности не рекомендуется использовать этот параметр. Файл ключа или код активации, добавленный в инсталляционный пакет, может быть скомпрометирован.

В случае установки управляемого приложения с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этого приложения. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

Инструкции:

- Консоль администрирования:
 - Создание инсталляционного пакета (на стр. [372](#)).
 - Установка приложений на клиентские устройства (на стр. [852](#)).

Или

- Kaspersky Security Center Web Console: Добавление лицензионного ключа в инсталляционный пакет.

Распространение с помощью задачи добавления лицензионного ключа управляемого приложения

В случае использования задачи *Добавление лицензионного ключа* управляемого приложения вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
 - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. [392](#)).
 - Распространение лицензионного ключа на клиентские устройства (на стр. [394](#)).

Или

- Kaspersky Security Center Web Console:
 - Добавление лицензионного ключа в хранилище Сервера администрирования.
 - Распространение лицензионного ключа на клиентские устройства.

Добавление кода активации или файла ключа вручную на устройства

Вы можете активировать установленное приложение "Лаборатории Касперского" локально, используя инструменты приложения. Дополнительную информацию см. в документации к установленным приложениям.

См. также

Просмотр информации об используемых лицензионных ключах	391
Добавление лицензионного ключа в хранилище Сервера администрирования.	392
Удаление лицензионного ключа Сервера администрирования	393
Распространение лицензионного ключа на клиентские устройства.	394
Автоматическое распространение лицензионного ключа.	398
Создание и просмотр отчета об использовании лицензионных ключей	399
Просмотр информации о лицензионных ключах приложения	400
Экспорт файла ключа	400
Лицензии и возможности Kaspersky Security Center	29

Просмотр информации об используемых лицензионных ключах

► Чтобы просмотреть информацию об используемых лицензионных ключах,

В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.

В рабочей области папки отображается перечень лицензионных ключей, используемых на клиентских устройствах.

Рядом с каждым лицензионным ключом отображается значок, соответствующий типу его использования:

-  – информация об используемом лицензионном ключе получена от подключенного к Серверу администрирования клиентского устройства. Файл этого лицензионного ключа не хранится на Сервере администрирования.
-  – лицензионный ключ находится в хранилище Сервера администрирования. Автоматическое распространение этого лицензионного ключа отключено.
-  – лицензионный ключ находится в хранилище Сервера администрирования. Включено автоматическое распространение этого лицензионного ключа.

Вы можете просмотреть информацию о том, какие лицензионные ключи используются для активации приложения на клиентском устройстве, в разделе **Приложения** окна свойств клиентского устройства (см. раздел "Просмотр и изменение локальных параметров приложения" на стр. [454](#)).

Для определения актуальных параметров лицензионных ключей виртуального Сервера администрирования Сервер администрирования отправляет запрос на серверы активации "Лаборатории Касперского" не реже одного раза в сутки. Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы (см. раздел "Доступ к общедоступным DNS-серверам" на стр. [919](#)).
Если лицензионный ключ получен с клиентского устройства, вы не можете экспортировать его в виде файла.

См. также

Лицензирование управляемых приложений	389
Добавление лицензионного ключа в хранилище Сервера администрирования.	392
Удаление лицензионного ключа Сервера администрирования	393
Распространение лицензионного ключа на клиентские устройства.	394
Автоматическое распространение лицензионного ключа.	398
Создание и просмотр отчета об использовании лицензионных ключей	399
Просмотр информации о лицензионных ключах приложения.....	400
Экспорт файла ключа	400
Лицензии и возможности Kaspersky Security Center	29

Добавление лицензионного ключа в хранилище Сервера администрирования.

► Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:

1. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
2. Запустите задачу добавления лицензионного ключа одним из следующих способов:
 - В контекстном меню лицензионного ключа выберите пункт **Добавить код активации или файл ключа**.
 - Перейдите по ссылке **Добавить код активации или файл ключа** блоке управления списком лицензионных ключей.
 - Нажмите на кнопку **Добавить код активации или файл ключа**.

Запустится Мастер добавления лицензионного ключа.
3. Выберите способ активации Сервера администрирования: с помощью кода активации или с помощью файла ключа.
4. Укажите ваш код активации или файл ключа.

5. Выберите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**, если вы хотите распространить соответствующий лицензионный ключ в своей сети немедленно. Если вы не выберете этот параметр, вы можете позже вручную распространить лицензионный ключ (см. раздел "Распространение лицензионного ключа на клиентские устройства." на стр. [394](#)).

В результате файл ключа загружается и Мастер добавления лицензионного ключа завершается. Теперь вы можете увидеть этот лицензионный ключ в списке лицензий "Лаборатории Касперского".

См. также

Лицензирование управляемых приложений	389
Просмотр информации об используемых лицензионных ключах	391
Удаление лицензионного ключа Сервера администрирования	393
Распространение лицензионного ключа на клиентские устройства.	394
Автоматическое распространение лицензионного ключа.	398
Создание и просмотр отчета об использовании лицензионных ключей	399
Просмотр информации о лицензионных ключах приложения.....	400
Экспорт файла ключа	400
Основной сценарий установки.....	56
Сценарий: настройка защиты сети.....	403
Лицензии и возможности Kaspersky Security Center	29

Удаление лицензионного ключа Сервера администрирования

► Чтобы удалить лицензионный ключ Сервера администрирования:

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования выберите раздел **Лицензионные ключи**.
3. Удалите лицензионный ключ по кнопке **Удалить**.

Лицензионный ключ будет удален.

Если был добавлен резервный лицензионный ключ, он автоматически становится активным после удаления предыдущего активного лицензионного ключа.

После удаления активного лицензионного ключа для Сервера администрирования становятся недоступными функции Системное администрирование (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. [354](#)) и Управление мобильными устройствами (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. [354](#)). Можно добавить (см. раздел "Добавление лицензионного ключа в хранилище Сервера администрирования." на стр. [392](#)) удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

См. также

Лицензирование управляемых приложений	389
Просмотр информации об используемых лицензионных ключах	391
Добавление лицензионного ключа в хранилище Сервера администрирования.	392
Распространение лицензионного ключа на клиентские устройства.	394
Автоматическое распространение лицензионного ключа.	398
Создание и просмотр отчета об использовании лицензионных ключей	399
Просмотр информации о лицензионных ключах приложения	400
Экспорт файла ключа	400
Сценарий: настройка защиты сети.....	403
Лицензии и возможности Kaspersky Security Center	29

Распространение лицензионного ключа на клиентские устройства.

Kaspersky Security Center позволяет распространить лицензионный ключ на клиентские устройства с помощью задачи *Распространение лицензионного ключа*.

Перед распространением добавьте лицензионный ключ в хранилище Сервера администрирования (см. раздел "Добавление лицензионного ключа в хранилище Сервера администрирования." на стр. [392](#)).

► Чтобы распространить лицензионный ключ на клиентские устройства:

1. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
2. Нажмите на кнопку **Автоматически распространять лицензионный ключ на управляемые устройства** в блоке управления списком лицензионных ключей.
Запустится мастер **Мастер создания задачи активации приложения**. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В списке приложений выберите приложение, для которого вы хотите создать задачу.
4. На шаге мастера **Добавить ключ** добавьте лицензионный ключ, используя один из следующих параметров:
 - Выберите параметр **Код активации**, чтобы добавить код активации из хранилища Kaspersky Security Center.
Нажмите на кнопку **Выбрать**. В открывшемся окне выберите код активации и нажмите на кнопку **ОК**.
 - Выберите параметр **Файл ключа или ключ** и выполните следующие действия:
 - a. Нажмите на кнопку **Выбрать**.
 - b. В контекстном меню выберите один из пунктов:

- **Файл ключа из папки.**

В открывшемся окне выберите файл ключа на своем устройстве и нажмите на кнопку **Открыть**.

- **Ключ из хранилища Kaspersky Security Center.**

В открывшемся окне выберите ключ из хранилища Kaspersky Security Center и нажмите на кнопку **ОК**.

5. Если вы хотите заменить активный лицензионный ключ, снимите флажок **Использовать ключ в качестве резервного**.

Например, это необходимо, когда организация меняется и на устройстве требуется ключ другой организации или если ключ был перевыпущен и срок действия новой лицензии истекает раньше, чем срок действия текущей лицензии. Чтобы избежать ошибок, снимите флажок **Использовать ключ в качестве резервного**.

Если вы хотите узнать больше о проблемах, которые могут возникнуть при добавлении лицензионного ключа в Kaspersky Security Center для Windows, и способах их решения, обратитесь к Базе знаний Kaspersky Security Center
<https://support.kaspersky.com/us/ksc/14.2/troubleshooting/other/16001>.

6. Проверьте информацию о лицензионном ключе и нажмите **Далее**.
7. На этом шаге мастера выберите устройства, которым вы хотите назначить задачу добавления ключа. Можно указать устройства (до 1000 устройств) одним из следующих способов:
 - **Выбрать устройства, обнаруженные в сети Сервером администрирования.** В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
 - **Задать адреса устройств вручную или импортировать из списка.** Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
 - **Назначить задачу выборке устройств.** В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать predetermined выборку или вашу собственную выборку.
 - **Назначить задачу группе администрирования.** В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

8. На шаге **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи:

- **Запуск по расписанию:**

- **Один раз**

- **Вручную**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **При загрузке обновлений в хранилище**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При загрузке обновлений в хранилище**, задача будет запускаться после загрузки обновлений в хранилище.

- **При обнаружении вирусной атаки**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемым списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемом списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

1. На шаге мастера **Определение названия задачи** укажите имя задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\\:|").
2. На шаге **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Задачи, сформированные при помощи мастера **Мастер создания задачи активации приложения**, являются задачами для наборов устройств и размещаются в папке **Задачи** дерева консоли.

Вы также можете создать групповую или локальную задачу распространения лицензионного ключа с помощью мастера создания задачи для группы администрирования и для клиентского устройства.

См. также

Лицензирование управляемых приложений	389
Просмотр информации об используемых лицензионных ключах	391
Добавление лицензионного ключа в хранилище Сервера администрирования.	392
Удаление лицензионного ключа Сервера администрирования	393
Автоматическое распространение лицензионного ключа.	398
Создание и просмотр отчета об использовании лицензионных ключей	399
Просмотр информации о лицензионных ключах приложения.....	400
Экспорт файла ключа	400
Основной сценарий установки.....	56
Сценарий: настройка защиты сети.....	403
Лицензии и возможности Kaspersky Security Center	29

Автоматическое распространение лицензионного ключа.

Kaspersky Security Center позволяет автоматически распространять на управляемые устройства лицензионные ключи, размещенные в хранилище ключей на Сервере администрирования. Автоматическое распространение лицензионных ключей не применяется к устройствам в папке **Нераспределенные устройства**.

► *Чтобы автоматически распространять лицензионный ключ на управляемые устройства:*

1. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
2. В рабочей области папки выберите лицензионный ключ, который вы хотите автоматически распространять на устройства.
3. Откройте окно свойств выбранного лицензионного ключа одним из следующих способов:
 - в контекстном меню лицензионного ключа выберите пункт **Свойства**;
 - по ссылке **Просмотреть свойства лицензионного ключа** в блоке работы с выбранным лицензионным ключом.
4. В открывшемся окне свойств лицензионного ключа установите флажок **Автоматически распространяемый лицензионный ключ**. Закройте окно свойств лицензионного ключа.

Лицензионный ключ будет автоматически распространяться на те устройства, для которых он подходит.

Распространение лицензионного ключа выполняется средствами Агента администрирования. Задачи распространения резервного лицензионного ключа для приложения при этом не создаются.

При автоматическом распространении лицензионного ключа учитывается лицензионное ограничение на количество устройств. Лицензионное ограничение задано в свойствах лицензионного ключа. Если лицензионное ограничение достигнуто, распространение лицензионного ключа на устройства автоматически прекращается.

Виртуальный Сервер администрирования автоматически распространяет лицензионные ключи из своего хранилища и из хранилища Сервера администрирования. Рекомендуется:

- Используйте задачу *Добавить лицензионный ключ*, чтобы выбрать лицензионный ключ, который необходимо развернуть на устройствах.
- Не выключайте параметр **Разрешить автоматическое распространение лицензионных ключей этого виртуального Сервера на его устройства** в параметрах виртуального Сервера администрирования. Иначе виртуальный Сервер администрирования не будет распространять лицензионные ключи на устройства, в том числе лицензионные ключи из хранилища Сервера администрирования.

Если вы установили флажок **Автоматически распространяемый лицензионный ключ** в окне свойств лицензионного ключа, лицензионный ключ будет немедленно распространен в вашей сети. Если вы не выберете этот параметр, вы можете позже вручную распространить лицензионный ключ (см. раздел "Распространение лицензионного ключа на клиентские устройства." на стр. [394](#)).

См. также:

Лицензирование управляемых приложений	389
Просмотр информации об используемых лицензионных ключах	391
Добавление лицензионного ключа в хранилище Сервера администрирования.	392
Удаление лицензионного ключа Сервера администрирования	393
Распространение лицензионного ключа на клиентские устройства.	394
Создание и просмотр отчета об использовании лицензионных ключей	399
Просмотр информации о лицензионных ключах приложения	400
Экспорт файла ключа	400
Основной сценарий установки.....	56
Сценарий: настройка защиты сети.....	403
Лицензии и возможности Kaspersky Security Center	29

Создание и просмотр отчета об использовании лицензионных ключей

► Чтобы создать отчет об использовании лицензионных ключей на клиентских устройствах:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. Выберите шаблон отчета **Отчет об использовании лицензионных ключей** или создайте новый шаблон отчета одноименного типа.

В результате в рабочей области отчета об использовании лицензионных ключей отображается информация об активных и резервных лицензионных ключах, используемых на клиентских устройствах. Также в отчете содержатся сведения об устройствах, на которых используются лицензионные ключи, и об ограничениях, заданных в свойствах лицензионных ключей.

См. также

Лицензирование управляемых приложений	389
Просмотр информации об используемых лицензионных ключах	391
Добавление лицензионного ключа в хранилище Сервера администрирования.	392
Удаление лицензионного ключа Сервера администрирования	393
Распространение лицензионного ключа на клиентские устройства.	394
Автоматическое распространение лицензионного ключа.	398
Просмотр информации о лицензионных ключах приложения	400
Экспорт файла ключа	400
Сценарий: мониторинг и отчеты	593
Лицензии и возможности Kaspersky Security Center	29

Просмотр информации о лицензионных ключах приложения

► Чтобы узнать, какие лицензионные ключи используются приложением "Лаборатории Касперского":

1. В дереве консоли Kaspersky Security Center выберите узел **Управляемые устройства** и перейдите на вкладку **Устройства**.
2. Откройте контекстное меню требуемого устройства по правой клавише мыши и выберите пункт **Свойства**.
3. В открывшемся окне свойств устройства выберите раздел **Приложения**.
4. В появившемся списке приложений выберите приложение, лицензионные ключи которого вы хотите просмотреть, и нажмите на кнопку **Свойства**.
5. В открывшемся окне свойств Сервера администрирования выберите раздел **Лицензионные ключи**.
Информация отображается в рабочей области этого раздела.

Экспорт файла ключа

Если ваш лицензионный ключ был случайно удален и вы хотите его восстановить, вы можете экспортировать файл ключа с другого Сервера администрирования.

Чтобы экспортировать файл ключа, вам нужно иметь право **Экспорт файла ключа** в функциональной области **Общие функции: Управление лицензионными ключами**.
Если лицензионный ключ получен с клиентского устройства, вы не можете экспортировать его.

► Чтобы экспортировать лицензионный ключ:

1. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
2. В списке выберите ключ, который вы хотите экспортировать в виде файла.
3. В открывшемся информационном окне перейдите по ссылке **Экспортировать файл**.
4. В открывшемся окне укажите путь к папке, в которой вы хотите сохранить файл ключа и укажите имя файла. Нажмите на кнопку **Сохранить**.

Файл ключа будет экспортирован в выбранную папку.

Процедура приемки

Перед вводом приложения в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

Безопасное состояние	401
Проверка работоспособности Kaspersky Security Center	401

Безопасное состояние

Приложение находится в безопасном состоянии (сертифицированной конфигурации), если выполняются следующие условия:

- Параметры приложения находятся в рамках допустимых значений, приведенных в приложении к этому документу.

Проверка работоспособности Kaspersky Security Center

После установки Kaspersky Security Center вы можете проверить его работоспособность с помощью выполнения алгоритма проверки. В таблице ниже приведен порядок действий для проверки работоспособности приложения и ожидаемые результаты выполнения этих действий.

Таблица 58. Шаги алгоритма проверки работоспособности Kaspersky Security Center

Номер шага	Действие	Результат
1	Подключитесь к Серверу администрирования с помощью Консоли Администрирования.	Консоль администрирования подключена к Серверу администрирования. В списке управляемых устройств появилось как минимум одно устройство Сервера администрирования.

Номер шага	Действие	Результат
2	Выполните первоначальную настройку Сервера администрирования с помощью мастера первоначальной настройки.	Мастер первоначальной настройки создал необходимые для развертывания защиты политики и задачи с параметрами по умолчанию.
3	Установите Агент администрирования и Kaspersky Endpoint Security для Windows на устройство.	Управляемое устройство, на которое была произведена установка приложений, присутствует в списке нераспределенных устройств. В свойствах устройства в разделе Приложения присутствуют приложения Агент администрирования и Kaspersky Endpoint Security для Windows.
4	Загрузите обновления в хранилище Сервера администрирования, запустив задачу загрузки обновлений в хранилище. Подробнее см. в Руководстве по эксплуатации, в разделе "Создание задачи загрузки обновлений в хранилище".	Задача завершена успешно и обновления загружены в хранилище.
5	Обновите приложение безопасности Kaspersky Endpoint Security для Windows. Для этого выполните задачу обновления. Подробнее см. в Руководстве по эксплуатации, в разделе "Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства".	В свойствах управляемого устройства в разделе Приложения в свойствах приложения Kaspersky Endpoint Security для Windows дата последнего обновления баз соответствует дате последнего запуска задачи обновления.
6	Внесите произвольные тестовые изменения в политику Kaspersky Endpoint Security для Windows.	Политика применена на управляемом устройстве, обнаруженном в сети: - В свойствах политики присутствует информация о том, что она применена на устройства. - Параметры приложения безопасности соответствуют параметрам политики.
7	Скопируйте на одно из управляемых устройств тестовый файл EICAR.	В журнале событий есть записи об обнаружении и ликвидации зараженного файла. В свойствах устройства в разделе Защита в поле Обнаружено вирусов значение увеличилось на один.

Настройка защиты сети

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства[405](#)

Сценарий: настройка защиты сети

Мастер первоначальной настройки создает политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться не оптимальными или даже запрещенными в организации. Поэтому рекомендуется настроить эти политики и задачи и создать дополнительные политики и задачи, если это необходимо для вашей сети.

Предварительные требования

Прежде чем приступить, убедитесь, что вы выполнили следующее:

- Установили Сервер администрирования Kaspersky Security Center (см. раздел "Стандартная установка" см. стр. [229](#)).
- Установили Kaspersky Security Center Web Console (если требуется).
- Выполнили основной сценарий установки Kaspersky Security Center (см. раздел "Основной сценарий установки" на стр. [56](#)).
- Мастер первоначальной настройки завершен или следующие политики и задачи созданы вручную в группе администрирования **Управляемые устройства**:
 - политика Kaspersky Endpoint Security;
 - групповая задача обновления Kaspersky Endpoint Security;
 - политика Агента администрирования;
 - задача *Поиск уязвимостей и требуемых обновлений*.

Настройка защиты сети состоит из следующих этапов:

а. Настройка и распространение политик и профилей политик для приложений "Лаборатории Касперского"

Для настройки и распространения параметров приложений "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью (см. раздел "Подходы к управлению безопасностью, ориентированные на устройства и на пользователей" на стр. [407](#)): ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода. Для реализации ориентированного на устройства (см. раздел "Настройка и распространение политик: подход, ориентированный на устройства" см. стр. [405](#)) метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center Web Console. Для реализации ориентированного на пользователей метода управления безопасностью подходит только Kaspersky Security Center Web Console.

b. Настройка задач для удаленного управления приложениями "Лаборатории Касперского"

Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

Инструкции:

- Консоль администрирования:
 - Настройка групповой задачи обновления Kaspersky Endpoint Security (см. раздел "Ручная настройка групповой задачи обновления Kaspersky Endpoint Security" на стр. [412](#)).
 - Настройка расписания задачи Поиск уязвимостей и требуемых обновлений (на стр. [412](#)).
- Kaspersky Security Center Web Console:
 - Настройка групповой задачи обновления Kaspersky Endpoint Security.
 - Параметры задачи поиска уязвимостей и требуемых обновлений.

При необходимости создайте дополнительные задачи (см. раздел "Управление задачами" на стр. [414](#)) управления приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

c. Оценка и ограничение загрузки событий в базу данных

Информация о событиях в работе управляемых приложений передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

Инструкции:

- Консоль администрирования: Настройка максимального количества событий (см. раздел "Настройка количества событий в хранилище событий" см. стр. [413](#)).
- Kaspersky Security Center Web Console: Настройка максимального количества событий.

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке приложений "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- Приложения "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление приложениями осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и приложений "Лаборатории Касперского" (см. раздел "Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"" см. стр. [455](#)).

Подробнее о настройке автоматического ответа на угрозы, обнаруженных Kaspersky Sandbox, см. в онлайн-справке Kaspersky Sandbox 2.0 <https://support.kaspersky.com/KSB/2.0/en-US/189425.htm>.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....	455
Основной сценарий установки.....	56

Настройка и распространение политик: подход, ориентированный на устройства

После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center (см. раздел "Стандартная установка" см. стр. [229](#)) и Kaspersky Security Center Web Console (если требуется). Если вы установили Kaspersky Security Center Web Console, вам может быть интересно также управление безопасностью, ориентированное на пользователей, в качестве альтернативы или дополнения к управлению безопасностью, ориентированному на устройства.

Этапы

Сценарий управления приложениями «Лаборатории Касперского», ориентированный на устройства, содержит следующие шаги:

а. Настройка политик приложений

Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для следующих приложений:

- Kaspersky Endpoint Security для Windows – для клиентских устройств с операционной системой Windows.
- Kaspersky Endpoint Security для Linux – для клиентских устройств с операционной системой Linux.

Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать новую политику для этого приложения. Перейдите к настройке политики Kaspersky Endpoint Security вручную (см. раздел "Ручная настройка политики Kaspersky Endpoint Security" на стр. [408](#)).

Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик (см. стр. [431](#)) позволяет эффективно управлять устройствами в группах администрирования.

Инструкции:

- Консоль администрирования: Создание политики (см. стр. [435](#)).
- Kaspersky Security Center Web Console: Создание политики.

b. Создание профилей политики (если требуется)

Если вы хотите, чтобы к устройствам из одной группы администрирования применялись разные параметры политики, создайте профили политики для этих устройств. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве.

Используя условия активации профиля, вы можете применять различные профили политики, например, к устройствам, расположенным в определенном подразделении или группе безопасности Active Directory, имеющим определенную конфигурацию программного обеспечения или имеющим заданные теги. Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *Windows*, назначить его всем устройствам под управлением операционной системы Windows, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы Windows установленные приложения "Лаборатории Касперского" будут управляться своим профилем политики.

Инструкции:

- Консоль администрирования:
 - Создание профиля политики (см. раздел "Создание профиля политики" на стр. [445](#)).
 - Создание правила активации профиля политики (см. раздел "Создание правила активации профиля политики" на стр. [447](#)).
- Kaspersky Security Center Web Console:
 - Создание профиля политики.
 - Создание правила активации профиля политики.

c. Распространение политик и профилей политик на управляемые устройства

По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно (см. раздел "О принудительной синхронизации" на стр. [764](#)). Также принудительная синхронизация выполняется после создания или изменения политики или профиля политики. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам.

Если вы используете Kaspersky Security Center Web Console, можно проверить, доставлены ли политики и профили политик на устройства. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

Инструкции:

- Консоль администрирования: Принудительная синхронизация (см. раздел "О принудительной синхронизации" на стр. [764](#)).
- Kaspersky Security Center Web Console: Принудительная синхронизация.

Результаты

После завершения сценария, ориентированного на устройства, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики приложений и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

См. также:

Основной сценарий установки.....	56
Удаление иерархии Серверов администрирования.....	41
Группы администрирования.....	44
Политики	47
Профили политик.....	48
Иерархия политик	431
Сценарий: настройка защиты сети.....	403

Подходы к управлению безопасностью, ориентированные на устройства и на пользователей

Вы можете управлять параметрами безопасности с позиции функций устройства и с позиции пользовательских ролей. Первый подход называется *управление безопасностью, ориентированное на устройства*, второй подход называется *управление безопасностью, ориентированное на пользователей*. Чтобы применить разные параметры приложений к разным устройствам, вы можете использовать один или оба типа управления в комбинации. Для реализации ориентированного на устройства метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center Web Console. Для реализации ориентированного на пользователей метода управления безопасностью подходит только Kaspersky Security Center Web Console.

Управление безопасностью, ориентированное на устройства (см. раздел "Настройка и распространение политик: подход, ориентированный на устройства" см. стр. [405](#)), позволяет вам применять различные параметры приложения безопасности к управляемым устройствам в зависимости от особенностей устройства. Например, вы можете применить различные параметры к устройствам, которые размещены в разных группах администрирования. Вы также можете разграничить устройства по использованию этих устройств в Active Directory или по характеристикам аппаратного обеспечения.

Управление безопасностью, ориентированное на пользователя, позволяет вам применять различные параметры приложений безопасности к различным ролям пользователей. Вы можете создать несколько пользовательских ролей, назначить соответствующую пользовательскую роль каждому пользователю и определить различные параметры приложения для устройств, принадлежащих пользователям с различными ролями. Например, можно применить различные параметры приложений к устройствам бухгалтеров и к устройствам специалистов отдела кадров. В результате внедрения управления безопасностью, ориентированного на пользователей, каждый отдел – отдел бухгалтерии и отдел кадров – получит свою собственную конфигурацию параметров для работы с приложениями "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры приложения могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры приложений для отдельных пользователей. Это может потребоваться, если сотруднику назначена уникальная роль в организации или если требуется проконтролировать проблемы безопасности, связанные с определенным сотрудником. В зависимости от роли этого сотрудника в компании, можно расширить или сократить его права, чтобы изменить параметры приложения. Например, может потребоваться расширить права системного администратора, управляющего клиентскими устройствами в локальном офисе.

Вы также можете комбинировать подходы к управлению безопасностью, ориентированные на пользователей и ориентированные на устройства. Например, можно настроить разные политики (на стр. [47](#)) для каждой группы администрирования, а затем дополнительно создать профили политик (на стр. [48](#)) для одной или нескольких пользовательских ролей вашей организации. В этом случае политики и профили политик применяются в следующем порядке:

1. Применяются политики, созданные для управления безопасностью, ориентированного на устройства.
2. Они модифицируются профилями политик в соответствии с параметрами профилей политик.
3. Политики модифицируются профилями политик, связанными с ролями пользователей.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security, которую создает мастер первоначальной настройки (см. раздел "Мастер первоначальной настройки Сервера администрирования" на стр. [281](#)). Вы можете выполнить настройку в окне свойств политики.

При изменении параметра следует помнить, что для того, чтобы значение параметра использовалось на рабочей станции, следует нажать на кнопку с "замком" над параметром.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства[405](#)

В этом разделе

Настройка политики в разделе Продвинутая защита[409](#)

Настройка политики в разделе Базовая защита.....[409](#)

Настройка политики в разделе Дополнительные параметры[410](#)

Настройка политики в разделе Настройка событий[410](#)

Настройка политики в разделе Продвинутая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Продвинутая защита** можно настроить использование Kaspersky Security Network для Kaspersky Endpoint Security для Windows. Можно также настроить модули Kaspersky Endpoint Security для Windows, такие как Анализ поведения, Защита от эксплойтов, Предотвращение вторжений и Откат вредоносных действий.

В подразделе **Kaspersky Security Network** рекомендуется включить параметр **Использовать прокси-сервер KSN**. Использование этого параметра поможет перераспределить и оптимизировать трафик сети. Если параметр **Использовать прокси-сервер KSN** выключен, вы можете включить прямое использование серверов KSN (см. раздел "О KSN и KPSN" на стр. [873](#)).

См. также:

Сценарий: настройка защиты сети.....[403](#)

Настройка политики в разделе Базовая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Базовая защита** окна свойств политики рекомендуется указать дополнительные параметры в подразделах **Сетевой экран** и **Защита от файловых угроз**.

Подраздел **Сетевой экран** содержит параметры, позволяющие контролировать сетевую активность приложений на клиентских устройствах. Клиентское устройство использует сеть, которой присвоен один из следующих статусов: общедоступная, локальная или доверенная. В зависимости от состояния сети Kaspersky Endpoint Security может разрешить или запретить сетевую активность на устройстве. Когда вы добавляете новую сеть в свою организацию, вам нужно присвоить ей соответствующий сетевой статус. Например, если клиентским устройством является ноутбук, рекомендуется, чтобы это устройство использовало общедоступную или доверенную сеть, так как ноутбук не всегда подключен к локальной сети. В подразделе **Сетевой экран** можно проверить, правильно ли вы присвоили статусы используемым в вашей организации сетям.

► Чтобы проверить список сетей:

1. В свойствах политики перейдите в раздел **Базовая защита** → **Сетевой экран**.
2. В блоке **Доступные сети** нажмите на кнопку **Настройка**.
3. В открывшемся окне **Сетевой экран** перейдите на вкладку **Сети** для просмотра списка сетей.

В подразделе **Защита от файловых угроз** можно отключить проверку сетевых дисков. Проверка сетевых дисков может создавать значительную нагрузку на сетевые диски. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

► *Чтобы выключить проверку сетевых дисков:*

1. В свойствах политики перейдите в раздел **Базовая защита** → **Защита от файловых угроз**.
2. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
3. В открывшемся окне **Защита от файловых угроз** на вкладке **Общие** снимите флажок **Все сетевые диски**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Настройка политики в разделе **Дополнительные параметры**

Полное описание параметров этого раздела приведено в документации **Kaspersky Endpoint Security для Windows**.

В разделе **Общие параметры** окна свойств политики, рекомендуется указать дополнительные параметры в подразделах **Отчеты и хранилища** и **Интерфейс**.

В подразделе **Отчеты и хранилища**, перейдите в раздел **Передача данных на Сервер администрирования**. Флажок **О запускаемых приложениях** указывает, сохраняется ли в базе данных Сервера администрирования информация обо всех версиях всех модулей приложений на устройствах в сети организации. Если этот флажок установлен, сохраненная информация может занимать значительный объем в базе данных Kaspersky Security Center (десятки гигабайтов). Снимите флажок **О запущенных приложениях**, если он установлен в политике верхнего уровня.

Если Консоль администрирования управляет защитой от угроз в сети организации централизованно, выключите отображение пользовательского интерфейса Kaspersky Endpoint Security для Windows на рабочих станциях. Для этого в подразделе **Интерфейс** перейдите в раздел **Взаимодействие с пользователем** и выберите параметр **Не отображать**.

Чтобы включить защиту паролем на рабочих станциях, в подразделе **Интерфейс** перейдите в раздел **Защита паролем**, нажмите на кнопку **Параметры** и установите флажок **Включить защиту паролем**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Настройка политики в разделе **Настройка событий**

В разделе **Настройка событий** следует отключить сохранение на Сервере администрирования всех

событий, за исключением перечисленных ниже:

- На вкладке **Критическое событие**:
 - Автозапуск приложения выключен.
 - Доступ запрещен.
 - Запуск приложения запрещен.
 - Лечение невозможно.
 - Нарушено Лицензионное соглашение.
 - Не удалось загрузить модуль шифрования.
 - Невозможен запуск двух задач одновременно.
 - Обнаружена активная угроза. Требуется запуск процедуры лечения.
 - Обнаружена сетевая атака.
 - Обновлено не все компоненты.
 - Ошибка активации.
 - Ошибка активации портативного режима.
 - Ошибка взаимодействия с Kaspersky Security Center.
 - Ошибка деактивации портативного режима.
 - Ошибка изменения содержимого приложения
 - Ошибка применения правил шифрования/расшифровки файлов.
 - Политика не может быть применена.
 - Процесс прерван.
 - Сетевая активность запрещена.
- На вкладке **Отказ функционирования**:
 - Ошибки параметров задачи. Параметры задачи не применены.
- На вкладке **Предупреждение**:
 - Самозащита приложения выключена.
 - Неправильный код активации резерва
 - Пользователь отказался от политики шифрования.
- На вкладке **Информационное сообщение**:
 - Запуск приложения запрещен в тестовом режиме

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Оптимальный и рекомендуемый вариант расписания для Kaspersky Endpoint Security версии 10 и выше – **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки устройства. По умолчанию для задачи выбрано расписание **Запускать по пятницам в 19:00** с автоматической рандомизацией и снят флажок **Запускать пропущенные задачи**.

Это означает, что если устройства организации выключаются по пятницам, например, в 18:30, то задача проверки устройства никогда не будет запущена. Следует настроить оптимальное расписание этой задачи исходя из принятого в организации регламента работы.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Настройка расписания задачи Поиск уязвимостей и требуемых обновлений.

Мастер первоначальной настройки создает для Агента администрирования групповую задачу *Поиск уязвимостей и требуемых обновлений*. По умолчанию для задачи выбрано расписание **Запускать по вторникам в 19:00** с автоматической рандомизацией и установлен флажок **Запускать пропущенные задачи**.

Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (в среду утром). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Сценарий: обновление приложений сторонних производителей[499](#)

Сценарий: настройка защиты сети.....[403](#)

Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей

Мастер первоначальной настройки создает для Агента администрирования групповую задачу установки обновлений и поиска уязвимостей. По умолчанию настроен запуск задачи ежедневно в 1:00 с автоматической рандомизацией, параметр **Запускать пропущенные задачи** выключен.

Если регламент работы организации предусматривает отключение устройств на ночь, то задача установки обновлений никогда не будет запущена. Следует задать оптимальное расписание задачи поиска уязвимостей исходя из принятого в организации регламента работы. Кроме того, следует учитывать, что в результате установки обновлений может потребоваться перезагрузка устройства.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Настройка количества событий в хранилище событий

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

► *Чтобы ограничить количество событий, которые можно сохранить в хранилище событий на Сервере администрирования:*

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

Откроется окно свойств Сервера администрирования.

2. В разделе **Хранилище событий** укажите максимальное количество событий, хранящихся в базе данных.
3. Нажмите на кнопку **ОК**.

Также можно изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи. Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом

таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

См. также:

Сценарий: мониторинг и отчеты.....	593
Сценарий: настройка защиты сети.....	403

Установка максимального срока хранения информации о закрытых уязвимостях

Чтобы установить максимальный срок хранения в базе данных информации об уже закрытых уязвимостях на управляемых устройствах:

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
Откроется окно свойств Сервера администрирования.
2. В разделе **Хранилище событий** укажите максимальный срок хранения информации о закрытых уязвимостях в базе данных.
Срок, заданный по умолчанию, – 90 дней.
3. Нажмите на кнопку **ОК**.

Максимальный срок хранения информации о закрытых уязвимостях ограничен указанным количеством дней. После этого задача обслуживания Сервера администрирования удалит устаревшую информацию из базы данных.

Управление задачами

Kaspersky Security Center управляет работой приложений, установленных на устройствах, путем создания и запуска различных задач. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Задачи делятся на следующие типы:

- *Групповые задачи.* Задачи, которые выполняются на устройствах выбранной группы администрирования.
- *Задачи Сервера администрирования.* Задачи, которые выполняются на Сервере администрирования.
- *Задачи для наборов устройств.* Глобальные задачи – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.
- *Локальные задачи.* Локальные задачи – это задачи, которые выполняются на конкретном устройстве.

Создание задач для приложения возможно только в случае, если на рабочее место администратора установлен плагин управления этим приложением.

Список устройств, для которых будет создана задача (до 1000 устройств), можно сформировать одним из следующих способов:

- Выбрать устройства, обнаруженные в сети Сервером администрирования.
- Задать список устройств вручную. В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя.
- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования при подключении устройств или в результате обнаружения устройств.

Для каждого приложения вы можете создавать любое количество групповых задач, задач для наборов устройств и локальных задач.

Обмен информацией о задачах между приложением, установленным на устройстве, и информационной базой Kaspersky Security Center происходит в момент соединения Агента администрирования с Сервером администрирования.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи. При остановке приложения выполнение всех запущенных задач прекращается.

Результаты выполнения задач сохраняются в журналах событий Microsoft Windows и в Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Управление задачами для приложений, поддерживающих мультитенантность

Групповая задача для мультитенантных приложений применяется к приложениям в зависимости от иерархии Серверов администрирования и клиентских устройств. Виртуальный Сервер администрирования, на котором создана задача, должен быть в той же группе администрирования, что и клиентское устройство, на котором установлено приложение, или в группе более низкого уровня.

В событиях, которые соответствуют результатам выполнения задачи, администратору поставщика услуг отображается информация об устройстве, на котором выполнена задача. В свою очередь, администратору tenants отображается **Мультитенантный узел**.

См. также:

Сценарий: настройка защиты сети.....	403
В этом разделе	
Создание задачи.....	416
Создание задачи Сервера администрирования	417
Создание задачи для набора устройств	418
Создание локальной задачи	419
Отображение унаследованной групповой задачи в рабочей области вложенной группы	419
Автоматическое включение устройств перед запуском задачи	420
Автоматическое выключение устройства после выполнения задачи.....	420
Ограничение времени выполнения задачи	421
Экспорт задачи.....	421
Импорт задачи.....	422
Конвертация задач	422
Запуск и остановка задачи вручную.....	423
Приостановка и возобновление задачи вручную.....	424
Наблюдение за ходом выполнения задачи.....	424
Просмотр результатов выполнения задач, хранящихся на Сервере администрирования	424
Настройка фильтра информации о результатах выполнения задачи	425
Изменение задачи. Откат изменений	425
Сравнение задач.....	426
Учетные записи для запуска задач	427
Мастер изменения паролей задач	428

Создание задачи

В Консоли администрирования можно создавать задачи непосредственно в папке группы администрирования, для которой создается задача, и в рабочей области папки **Задачи**.

► *Чтобы создать групповую задачу в папке группы администрирования:*

1. В дереве консоли выберите группу администрирования, для которой нужно создать задачу.
2. В рабочей области выберите вкладку **Задачи**.
3. Запустите мастер создания задачи по кнопке **Создать задачу**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

► *Чтобы создать задачу в рабочей области папки **Задачи**:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите мастер создания задачи по кнопке **Готово**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

См. также

Сценарий: мониторинг и отчеты.....	593
Сценарий: настройка защиты сети.....	403

Создание задачи Сервера администрирования

Сервер администрирования выполняет следующие функции:

- Рассылка отчетов.
- Загрузка обновлений в хранилище Сервера администрирования.
- Резервное копирование данных Сервера администрирования.
- Обслуживание Сервера администрирования.
- Выполнение синхронизации обновлений Центра обновления Windows.
- Создание инсталляционного пакета на основе образа ОС эталонного устройства.
- Удаленная установка приложений.
- Удаленная деинсталляция приложений.
- Распространять инсталляционные пакеты.
- Установка приложений на подчиненные Серверы администрирования.

На виртуальном Сервере администрирования доступна только задача автоматической рассылки отчетов и задача создания инсталляционного пакета на основе образа операционной системы эталонного устройства. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования. Резервное копирование данных виртуального Сервера осуществляется в рамках резервного копирования данных главного Сервера администрирования.

► *Чтобы создать задачу Сервера администрирования:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:

- В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать** → **Задачу**.
- В рабочей области папки **Создать задачу** нажмите на кнопку **Задачи**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Задачи Загрузка обновлений в хранилище Сервера администрирования, Синхронизация обновлений Windows Update, Обслуживание Сервера администрирования и Резервное копирование данных Сервера администрирования можно создать только в одном экземпляре. Если задачи Загрузка обновлений в хранилище Сервера администрирования, Обслуживание Сервера администрирования, Резервное копирование данных Сервера администрирования и Синхронизация обновлений Windows Update уже созданы для Сервера администрирования, то они не отображаются в окне выбора типа задачи мастера создания задачи.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Создание задачи для набора устройств

В Kaspersky Security Center можно создавать задачи для произвольно выбранного набора устройств. Устройства в наборе могут входить в разные группы администрирования или не входить ни в одну группу администрирования. Kaspersky Security Center позволяет выполнять следующие основные задачи для набора устройств:

- Удаленная установка приложений (см. раздел "Установка приложения на выбранные устройства" на стр. [360](#)).
- Отправка сообщения для пользователя (см. раздел "Отправка сообщения пользователям устройств" на стр. [765](#)).
- Смена Сервера администрирования (см. раздел "Смена Сервера администрирования для клиентских устройств" на стр. [762](#)).
- Управление устройствами (см. раздел "Удаленное включение, выключение и перезагрузка клиентских устройств" на стр. [763](#)).
- Проверка обновлений (см. раздел "Проверка полученных обновлений" на стр. [479](#)).
- Распространять инсталляционные пакеты (см. раздел "Распространение инсталляционных пакетов на подчиненные Серверы администрирования" на стр. [379](#)).
- Установка приложений на подчиненные Серверы администрирования (см. раздел "Установка приложений на подчиненные Серверы администрирования" на стр. [363](#)).
- Удаленная деинсталляция приложений (см. раздел "Удаленная деинсталляция приложений" на стр. [370](#)).

► Чтобы создать задачу для набора устройств:

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:

- В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать** → **Задачу**.
- В рабочей области папки **Создать задачу** нажмите на кнопку **Задачи**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Создание локальной задачи

► Чтобы создать локальную задачу для устройства:

1. В рабочей области группы, в состав которой входит устройство, выберите вкладку **Устройства**.
2. В списке устройств на вкладке **Устройства** выберите устройство, для которого нужно создать локальную задачу.
3. Запустите процесс создания задачи для выбранного устройства одним из следующих способов:
 - Нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите значение **Создать задачу**.
 - В рабочей области устройства перейдите по ссылке **Создать задачу**.
 - Используйте свойства устройства следующим образом:
 - a. В контекстном меню устройства выберите пункт **Свойства**.
 - b. В открывшемся окне свойств устройства выберите раздел **Задачи** и нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Подробные описания создания и настройки локальных задач приводятся в Руководствах к соответствующим приложениям "Лаборатории Касперского".

См. также:

Сценарий: настройка защиты сети.....[403](#)

Отображение унаследованной групповой задачи в рабочей области вложенной группы

► Чтобы включить отображение унаследованных задач вложенной группы в рабочей области:

1. Выберите в рабочей области вложенной группы вкладку **Задачи**.
2. В рабочей области вкладки **Задачи** нажмите на кнопку **Показывать унаследованные задачи**.

В результате унаследованные задачи отображаются в списке задач со значком:

-  – если они были унаследованы от группы, созданной на главном Сервере администрирования;
-  – если они были унаследованы от группы верхнего уровня.

При включенном режиме наследования редактирование унаследованных задач доступно только в той группе, в которой они были созданы. Редактирование унаследованных задач недоступно в той группе, которая наследует задачи.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Автоматическое включение устройств перед запуском задачи

Kaspersky Security Center не выполняет задачи на выключенных устройствах. Вы можете настроить Kaspersky Security Center на автоматическое включение этих устройств перед запуском задачи с помощью функции Wake-on-LAN.

► *Чтобы настроить автоматическое включение устройств перед запуском задачи:*

1. В окне свойств задачи выберите раздел **Расписание**.
2. Чтобы настроить действия на устройствах, перейдите по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Активировать устройства перед запуском задачи функцией Wake-on-LAN за (мин)** и укажите время в минутах.

В результате за указанное количество минут до запуска задачи, Kaspersky Security Center включает устройства и загружает операционную систему с помощью функции Wake-on-LAN. После выполнения задачи устройства автоматически выключаются, если пользователи устройств не входят в систему. Kaspersky Security Center автоматически выключает только те устройства, которые включены с помощью функции Wake-on-LAN.

Kaspersky Security Center может автоматически запускать операционные системы только на устройствах, поддерживающих стандарт Wake-on-LAN (WoL).

См. также:

Сценарий: настройка защиты сети.....[403](#)

Автоматическое выключение устройства после выполнения задачи

Kaspersky Security Center позволяет настроить параметры задачи таким образом, чтобы после ее выполнения устройства, на которые она распространяется, автоматически выключались.

► Чтобы устройства автоматически выключались после выполнения задачи:

1. В окне свойств задачи выберите раздел **Расписание**.
2. Откройте окно настройки действий с устройствами по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Выключать устройства после выполнения задачи**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Ограничение времени выполнения задачи

► Чтобы ограничить время выполнения задачи на устройствах:

1. В окне свойств задачи выберите раздел **Расписание**.
2. Откройте окно настройки действий с клиентскими устройствами по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Остановить, если задача выполняется дольше (мин)** и укажите время в минутах.

В результате, если по истечении указанного времени выполнение задачи на устройстве не будет завершено, Kaspersky Security Center автоматически остановит выполнение задачи.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Экспорт задачи

Вы можете экспортировать групповые задачи и задачи для наборов устройств в файл. Задачи Сервера администрирования (см. раздел "Создание задачи Сервера администрирования" на стр. [417](#)) также недоступны для экспорта.

► Чтобы экспортировать задачу:

1. В контекстном меню задачи выберите пункт **Все задачи** → **Экспортировать**.
2. В открывшемся окне **Сохранить как** укажите имя файла и путь для сохранения.
3. Нажмите на кнопку **Сохранить**.

Права локальных пользователей не экспортируются.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Импорт задачи

Вы можете импортировать групповые задачи и задачи для наборов устройств. Задачи Сервера администрирования (см. раздел "Создание задачи Сервера администрирования" на стр. [417](#)) недоступны для импорта.

► Чтобы импортировать задачу:

1. Выберите список задач, в который требуется импортировать задачу:
 - Если вы хотите импортировать задачу в список групповых задач, в рабочей области нужной вам группы администрирования выберите вкладку **Задачи**.
 - Если вы хотите импортировать задачу в список задач для наборов устройств, в дереве консоли выберите папку **Задачи**.
2. Выберите один из следующих способов импорта задачи:
 - В контекстном меню списка задач выберите пункт **Все задачи** → **Импортировать**.
 - По ссылке **Импортировать задачу из файла** в блоке управления списком задач.
3. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать задачу.
4. Нажмите на кнопку **Открыть**.

В результате импортированная задача отобразится в списке задач.

Если имя новой импортированной задачи идентично имени существующей задачи, имя импортированной задачи расширяется с помощью окончания вида (**<порядковый номер>**), например: **(1)**, **(2)**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Конвертация задач

С помощью Kaspersky Security Center можно конвертировать задачи предыдущих версий приложений "Лаборатории Касперского" в задачи текущих версий приложений.

Конвертация возможна для задач следующих приложений:

- Антивирус Касперского 6.0 для Windows Workstations MP4.
- Kaspersky Endpoint Security 8 для Windows.

- Kaspersky Endpoint Security 10 для Windows.

► Чтобы конвертировать задачи:

1. В дереве консоли выберите Сервер администрирования, для которого вы хотите выполнить конвертацию задач.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи** → **Мастер массовой конвертации политик и задач**.

В результате запускается мастер массовой конвертации политик и задач. Следуйте далее указаниям мастера.

В результате работы мастера формируются новые задачи, использующие параметры задач предыдущих версий приложений.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Запуск и остановка задачи вручную

Задачи можно запускать и останавливать двумя способами: из контекстного меню задачи и в окне свойств клиентского устройства, которому назначена эта задача.

Запускать групповые задачи из контекстного меню устройства могут пользователи, входящие в группу **KLAdmins** (см. раздел "**Права доступа к Серверу администрирования и его объектам**" на стр. [706](#)).

► Чтобы запустить или остановить задачу из контекстного меню или окна свойств задачи:

1. В списке задач выберите задачу.
2. Запустите или остановите задачу одним из следующих способов:
 - В контекстном меню задачи выберите пункт **Запустить** или **Остановить**.
 - В разделе **Общие** окна свойств задачи нажмите на кнопку **Запустить** или **Остановить**.

► Чтобы запустить или остановить задачу из контекстного меню или окна свойств клиентского устройства:

1. В списке устройств выберите устройство.
2. Запустите или остановите задачу одним из следующих способов:
 - В контекстном меню устройства выберите пункт **Все задачи** → **Запустить задачу**. Из списка задач выберите требуемую.
Список устройств, для которых назначена задача, будет замещен выбранным устройством. Задача будет запущена.
 - В окне свойств устройства в разделе **Задачи** нажмите на кнопку запуска () или остановки ().

См. также:

Сценарий: настройка защиты сети.....[403](#)

Приостановка и возобновление задачи вручную

► Чтобы приостановить или возобновить выполнение запущенной задачи:

1. В списке задач выберите задачу.
2. Приостановите или возобновите выполнение задачи одним из следующих способов:
 - В контекстном меню задачи выберите пункт **Приостановить** или **Возобновить**.
 - В разделе **Общие** окна свойств задачи нажмите на кнопку **Приостановить** или **Возобновить**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Наблюдение за ходом выполнения задачи

► Чтобы наблюдать за ходом выполнения задачи,

В окне свойств задачи выберите раздел **Общие**.

В средней части окна раздела **Общие** содержится информация о текущем состоянии задачи.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Kaspersky Security Center позволяет просматривать результаты выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования.

► Чтобы посмотреть результаты выполнения задачи, выполните следующие действия:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

► Чтобы просмотреть результаты задачи для подчиненного Сервера администрирования:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

3. Нажмите на **Статистика подчиненного Сервера**.
4. Выберите подчиненный Сервер, для которого вы хотите отобразить окно **Результаты выполнения задачи**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Настройка фильтра информации о результатах выполнения задачи

Kaspersky Security Center позволяет фильтровать информацию о результатах выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования. Для локальных задач фильтрация недоступна.

► *Чтобы настроить фильтр для информации о результатах выполнения задачи:*

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.
Таблица в верхней части окна содержит список всех устройств, для которых назначена задача.
Таблица в нижней части окна содержит результаты выполнения задачи на выбранном устройстве.
3. В интересующей вас таблице по правой клавише мыши откройте контекстное меню и выберите в нем пункт **Фильтр**.
4. В открывшемся окне **Применить фильтр** настройте параметры фильтра в разделах окна **События**, **Устройства** и **Время**. Нажмите на кнопку **ОК**.

В результате в окне **Результаты выполнения задачи** будет отображаться информация, удовлетворяющая параметрам, заданным в фильтре.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Изменение задачи. Откат изменений

► *Чтобы изменить задачу:*

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** выберите задачу и с помощью контекстного меню перейдите в окно свойств задачи.
3. Внесите необходимые изменения.

В разделе **Исключения из области действия задачи** можно настроить список вложенных групп, на которые не будет распространяться задача.

4. Нажмите на кнопку **Применить**.

Изменения задачи будут сохранены в окне свойств задачи, в разделе **История ревизий**.

В случае необходимости вы можете откатить изменения задачи.

► *Чтобы откатить изменения задачи:*

1. В дереве консоли выберите папку **Задачи**.
2. Выберите задачу, изменения которой нужно откатить и с помощью контекстного меню перейдите в окно свойств задачи.
3. В окне свойств задачи выберите раздел **История ревизий**.
4. В списке ревизий задачи выберите номер ревизии, к которой нужно откатить изменения.
5. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Сравнение задач

Вы можете сравнивать задачи одного типа, например, можно сравнить две задачи поиска вредоносного ПО, но невозможно сравнить задачу поиска вредоносного ПО с задачей установки обновлений. В результате сравнения задач вы получаете отчет, показывающий, какие параметры задач совпадают, а какие различаются. Вы можете распечатать отчет сравнения задач или сохранить его в файле. Сравнение задач может потребоваться в случае, когда для разных подразделений одной компании есть различные задачи одного типа. Например, для бухгалтерии есть задача поиска вредоносного ПО только на локальных дисках компьютера, а для отдела продаж, сотрудники которого переписываются с клиентами, есть задача проверять и локальные диски, и почту. Чтобы быстро увидеть такие различия, нет необходимости просматривать все параметры задачи, достаточно выполнить сравнение задач.

Сравнение можно выполнить только для задач одного типа.
Задачи можно сравнивать только попарно.

Вы можете сравнивать задачи одним из следующих способов: путем выбора одной задачи и сравнения ее с другой или путем сравнения любых двух задач из списка задач.

► *Чтобы выбрать одну задачу и сравнить ее с другой:*

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** выберите задачу, которую нужно сравнить с другой задачей.
3. В контекстном меню задачи выберите пункт **Все задачи** → **Сравнить с другой задачей**.
4. В окне **Выбор задачи** выберите задачу для сравнения.
5. Нажмите на кнопку **ОК**.

Отобразится отчет сравнения двух задач в формате HTML.

► Чтобы сравнить две задачи из списка задач:

1. В дереве консоли выберите папку **Задачи**.
2. В папке **Задачи** в списке задач с помощью клавиши **SHIFT** или **CTRL** выберите две задачи одного типа.
3. В контекстном меню выберите пункт **Сравнить**.

Отобразится отчет сравнения выбранных задач в формате HTML.

При сравнении задач, в случае если используемые пароли отличаются, в отчете сравнения задач будут отображаться символы *****.

Если в свойствах задачи был изменен пароль, в отчете сравнения ревизий задачи будут отображаться символы *****.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Учетные записи для запуска задач

Вы можете задавать учетную запись, под которой должна запускаться задача.

Например, для выполнения задач проверки по требованию необходимы права на доступ к проверяемому объекту, а для выполнения задач обновления – права авторизованного пользователя прокси-сервера. Возможность задать учетную запись для запуска задачи позволяет избежать ошибки при выполнении задач проверки по требованию и задач обновления, если у пользователя, запустившего задачу, нет необходимых прав доступа.

В задачах удаленной установки и деинсталляции приложения учетная запись используется для загрузки на клиентские устройства файлов, необходимых для установки (удаления), если на устройстве не установлен или недоступен Агент администрирования. При установленном и доступном Агенте администрирования учетная запись используется, если согласно параметрам задачи доставка файлов выполняется только средствами Microsoft Windows из папки общего доступа. В этом случае учетная запись должна обладать следующими правами на устройстве:

- правом на удаленный запуск приложений;
- правами на ресурс Admin\$;
- правом *Вход в качестве службы*.

Если доставку файлов на устройства выполняет Агент администрирования, учетная запись использоваться не будет. Все операции по копированию и установке файлов будет выполнять **Агент администрирования (Учетная запись LocalSystem)**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Мастер изменения паролей задач

Для не-локальной задачи можно указать учетную запись, с правами которой будет запускаться задача. Учетную запись можно указать во время создания задачи или в свойствах существующей задачи. Если указанная учетная запись используется в соответствии с правилами безопасности, установленными в организации, эти правила могут требовать периодического изменения пароля учетной записи. После истечения срока действия пароля учетной записи и задания нового пароля, задача не будет запускаться до тех пор, пока вы не укажете новый действующий пароль в свойствах задачи.

Мастер изменения паролей задач позволяет автоматически заменить старый пароль на новый во всех задачах, в которых указана учетная запись. Вы также можете сделать это вручную в свойствах каждой задачи.

► Чтобы запустить мастер изменения паролей задач

1. В дереве консоли выберите узел **Задачи**.
2. В контекстном меню узла Сервера администрирования выберите пункт **Мастер изменения паролей задач**.

Следуйте далее указаниям мастера.

В этом разделе

Шаг 1. Выбор учетных данных	428
Шаг 2. Выбор выполняемого действия	429
Шаг 3. Просмотр результатов	429

Шаг 1. Выбор учетных данных

В полях **Учетная запись** и **Пароль** укажите новые учетные данные, действующие в вашей системе (например, в Active Directory). При переходе на следующий шаг мастера, Kaspersky Security Center проверяет, совпадает ли имя указанной учетной записи с именем учетной записи в свойствах каждой не-локальной задачи. Если имена учетных записей совпадают, пароль в свойствах задачи автоматически меняется на новый.

При заполнении поля **Старый пароль (необязательно)** Kaspersky Security Center заменит пароль только для тех задач, для которых совпадают значения имени и старого пароля. Замена выполняется автоматически. Во всех остальных случаях необходимо выбрать действие, выполняемое на следующем шаге мастера.

См. также:

Мастер изменения паролей задач	428
Шаг 2. Выбор выполняемого действия	429
Шаг 3. Просмотр результатов	429

Шаг 2. Выбор выполняемого действия

Если на первом шаге мастера вы не указали старый пароль или указанный старый пароль не соответствует паролям задач, необходимо выбрать действие, выполняемое с этими задачами.

Для каждой задачи со статусом *Требуется одобрение* определите, хотите ли вы удалить пароль в свойствах задачи или заменить его на новый. Если вы выберете удаление пароля, задача перейдет в режим запуска с правами учетной записи, заданной по умолчанию.

См. также:

Мастер изменения паролей задач	428
Шаг 1. Выбор учетных данных	428
Шаг 3. Просмотр результатов	429

Шаг 3. Просмотр результатов

На последнем шаге мастера просмотрите результаты для каждой из обнаруженных задач. Для завершения работы мастера нажмите на кнопку **Готово**.

См. также:

Мастер изменения паролей задач	428
Шаг 1. Выбор учетных данных	428
Шаг 2. Выбор выполняемого действия	429

Создание иерархии групп администрирования, подчиненных виртуальному Серверу администрирования

После создания виртуального Сервера администрирования он по умолчанию содержит группу администрирования **Управляемые устройства**.

Процедура создания иерархии групп администрирования, подчиненных виртуальному Серверу администрирования, совпадает с процедурой создания иерархии групп администрирования, подчиненных физическому Серверу администрирования (см. раздел "Группы администрирования" см. стр. [44](#)).

В состав групп администрирования, подчиненных виртуальному Серверу администрирования, невозможно добавлять подчиненные и виртуальные Серверы администрирования. Это связано с ограничениями виртуальных Серверов администрирования (см. раздел "Виртуальные Серверы администрирования" см. стр. [150](#)).

См. также:

Управление группами администрирования	742
Сценарий: настройка защиты сети.....	403

Политики и профили политик

В Kaspersky Security Center Web Console можно создавать политики для приложений "Лаборатории Касперского" (см. раздел "Совместимые приложения и решения "Лаборатории Касперского"" на стр. [29](#)). В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

В этом разделе

Иерархия политик, использование профилей политик.....	431
Управление политиками.....	434
Управление профилями политик.....	442

См. также:

Сценарий: настройка защиты сети	403

Иерархия политик, использование профилей политик

В этом разделе содержится информация об особенностях применения политик к устройствам в группах администрирования. В этом разделе также содержится информация о профилях политик.

Иерархия политик

В Kaspersky Security Center политики предназначены для задания одинакового набора параметров на множестве устройств. Например, областью действия политики приложения Р, определенной для группы G, являются управляемые устройства с установленным приложением Р, размещенные в группе администрирования G и всех ее подгруппах, исключая те подгруппы, в свойствах которых снят флажок **Наследовать из родительской группы**.

Политика отличается от локальных параметров наличием "замков" (🔒) возле содержащихся в ней параметров. Установленный замок в свойствах политики означает, что соответствующий ему параметр (или группа параметров) должен, во-первых, быть использован при формировании эффективных параметров, во-вторых, должен быть записан в нижележащую политику.

Формирование на устройстве действующих параметров можно представить следующим образом: из политики берутся значения параметров с неустановленным замком, затем поверх них записываются значения локальных параметров, затем поверх полученных значений записываются взятые из политики значения параметров с установленным замком.

Политики одного и того же приложения действуют друг на друга по иерархии групп администрирования: параметры с установленным замком из вышележащей политики переписывают одноименные параметры из нижележащей политики.

Существует особый вид политики – политика для автономных пользователей. Эта политика вступает в силу на устройстве, когда устройство переходит в автономный режим. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.

Политика для автономных пользователей не будет поддерживаться в будущих версиях Kaspersky Security Center. Вместо политик для автономных пользователей следует использовать профили политик.

Профили политик

Применение политик к устройствам, исходя только из иерархии групп администрирования, во многих случаях неудобно. Может возникнуть необходимость создать несколько копий политики для разных групп администрирования и в дальнейшем вручную синхронизировать содержимое этих политик.

Чтобы помочь избежать подобных проблем, Kaspersky Security Center поддерживает *профили политик*. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на клиентском устройстве (компьютере, мобильном устройстве). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политик сейчас имеют следующие ограничения:

- в политике может быть не более 100 профилей;
- профиль политики не может содержать другие профили;
- профиль политики не может содержать параметры уведомлений.

Состав профиля

Профиль политики содержит следующие составные части:

- Имя. Профили с одинаковыми именами действуют друг на друга по иерархии групп администрирования с общим правилами.
- Подмножество параметров политики. В отличие от политики, где содержатся все параметры, в профиле присутствуют лишь те параметры, которые действительно нужны (на которых установлен замок).
- Условие активации – логическое выражение над свойствами устройства. Профиль активен (дополняет политику), только когда условие активации профиля становится истинным. В остальных случаях профиль неактивен и игнорируется. В логическом выражении могут участвовать следующие свойства устройства:
 - состояние автономного режима;
 - свойства сетевого окружения – имя активного правила подключения Агента администрирования (см. раздел "О профилях соединения для автономных пользователей" на стр. [303](#));
 - наличие или отсутствие у устройства указанных тегов;
 - местоположение устройства в подразделении Active Directory: явное (устройство находится непосредственно в указанном подразделении) или неявное (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности);
 - членство устройства в группе безопасности Active Directory (явное или неявное);

- членство владельца устройства в группе безопасности Active Directory (явное или неявное).
- Флажок отключения профиля. Отключенные профили всегда игнорируются, условия их активации не проверяются на истинность.
- Приоритет профиля. Условия активации профилей независимы, поэтому одновременно могут активироваться сразу несколько профилей. Если активные профили содержат непересекающиеся наборы параметров, то никаких проблем не возникает. Но если два активных профиля содержат разные значения одного и того же параметра, возникает неоднозначность. значение неоднозначной переменной будет взято из профиля с большим приоритетом (из того профиля, который располагается выше в списке профилей).

Поведение профилей при действии политик друг на друга по иерархии

Одноименные профили объединяются согласно правилам объединения политик. Профили верхней политики приоритетнее профилей нижней политики. Если в "верхней" политике запрещено изменение параметров (кнопка замок нажата), в "нижней" политике используются условия активации профиля из "верхней" политики. Если в "верхней" политике разрешено изменение параметров, то используются условия активации профиля из "нижней" политики.

Поскольку профиль политики может в условии активации содержать свойство **Устройство в автономном режиме**, профили полностью заменяют функциональность политик для автономных пользователей, которая в дальнейшем не будет поддерживаться.

Политика для автономных пользователей может содержать профили, но активация ее профилей может произойти не ранее, чем устройство перейдет в автономный режим.

Наследование параметров политики

Политика задается для группы администрирования. Параметры политики могут *наследоваться*, то есть передаваться в подгруппы (дочерние группы) групп администрирования, для которых она создана. Политика, созданная для родительской группы, также называется *родительской политикой*.

Можно включить или выключить два параметра наследования: **Наследовать параметры родительской политики** и **Форсировать наследование параметров дочерними политиками**.

- Если вы включили **Наследовать параметры родительской политики** для дочерней политики и заблокировали некоторые параметры в родительской политике, тогда вы не можете изменить эти параметры для дочерней группы. Однако вы можете изменить параметры, которые не заблокированы в родительской политике.
- Если вы выключили **Наследовать параметры родительской политики** для дочерней политики, тогда вы можете изменить все параметры в дочерней группе, даже если некоторые параметры заблокированы в родительской политике.
- Если в родительской группе включен параметр **Обеспечить принудительное наследование параметров для дочерних политик**, это включит параметр **Наследовать параметры родительской политики** для каждой дочерней политики. В этом случае вы не можете выключить этот параметр для дочерних политик. Все параметры, которые заблокированы в родительской политике, принудительно наследуются в дочерних группах, и вы не можете изменить эти параметры в дочерних группах.
- В политиках для группы **Управляемые устройства** параметр **Наследовать параметры родительской политики** не влияет ни на какие параметры, так как группа **Управляемые устройства** не имеет вышестоящих групп и, следовательно, не наследует никакие политики.

По умолчанию параметр **Наследовать параметры родительской политики** включен для новой политики.

Если у политики имеются профили, все дочерние политики наследуют эти профили.

Управление политиками

Централизованная настройка параметров приложений, установленных на клиентских устройствах, осуществляется через определение политик.

Политики, сформированные для приложений в группе администрирования, отображаются в рабочей области на вкладке **Политики**. Перед именем каждой политики отображается значок, характеризующий ее статус (см. раздел "Статусы устройств, задач и политик" на стр. [935](#)).

После удаления политики или прекращения ее действия приложение продолжает работу с параметрами, заданными в политике. В дальнейшем эти параметры можно изменить вручную.

Применение политики производится следующим образом: если на устройстве выполняются резидентные задачи (задачи постоянной защиты), их выполнение продолжается с новыми значениями параметров. Запущенные периодические задачи (проверка по требованию, обновление баз приложений) выполняются с неизменными значениями. Новый запуск периодических задач производится с измененными значениями параметров.

Политики для приложений с поддержкой мультитенантности наследуются для групп администрирования более низкого уровня, а также для групп администрирования верхнего уровня: политика распространяется на все клиентские устройства, на которых установлено приложение.

В случае использования иерархической структуры Серверов администрирования подчиненные Серверы получают политики с главного Сервера администрирования и распространяют их на клиентские устройства. При включенном механизме наследования параметры политики можно изменять на главном Сервере администрирования. После этого изменения, внесенные в параметры политики, распространяются на унаследованные политики на подчиненных Серверах администрирования.

При разрыве соединения между главным и подчиненным Серверами администрирования политика на подчиненном Сервере продолжает действовать с прежними параметрами. Параметры политики, измененные на главном Сервере администрирования, распространяются на подчиненный Сервер после восстановления соединения.

При отключенном механизме наследования параметры политики можно изменять на подчиненном Сервере независимо от главного Сервера.

Если происходит разрыв соединения между Сервером администрирования и клиентским устройством, на устройстве вступает в силу политика для автономного пользователя (если она определена), или политика продолжает действовать с прежними параметрами до восстановления соединения.

Результаты распространения политики на подчиненные Серверы администрирования отображаются в окне свойств политики на главном Сервере администрирования.

Результаты распространения политики на клиентские устройства отображаются в окне свойств политики Сервера администрирования, к которому они подключены.

Не используйте в параметрах политик конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

В этом разделе

Создание политики	435
Отображение унаследованной политики во вложенной группе	436
Активация политики	437
Автоматическая активация политики по событию "Вирусная атака"	437
Применение политики для автономных пользователей	437
Изменение политики. Откат изменений	438
Сравнение политик	438
Просмотр диаграммы состояния применения политики	439
Удаление политики	439
Копирование политики	439
Экспорт политики	440
Импорт политики	440
Конвертация политик	440

Создание политики

В Консоли администрирования можно создавать политики непосредственно в папке группы администрирования, для которой создается политика, и в рабочей области папки **Политики**.

► Чтобы создать политику в папке группы администрирования:

1. В дереве консоли выберите группу администрирования, для которой нужно создать политику.
2. В рабочей области группы выберите вкладку **Политики**.
3. Запустите мастер создания политики по кнопке **Новая политика**.

В результате запускается мастер создания политики. Следуйте далее указаниям мастера.

► Чтобы создать политику в рабочей области папки **Политики**:

1. В дереве консоли выберите папку **Политики**.
2. Запустите мастер создания политики по кнопке **Новая политика**.

В результате запускается мастер создания политики. Следуйте далее указаниям мастера.

Для одного приложения в группе можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика становится неактивной.

При создании политики можно настроить минимальный набор параметров, без которых приложение не будет работать. Остальные значения параметров устанавливаются по умолчанию и соответствуют значениям по умолчанию при локальной установке приложения. Вы можете изменять политику после ее создания.

Не используйте в параметрах политик конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Параметры приложений "Лаборатории Касперского", которые изменяются после применения политик, подробно описаны в руководствах к каждой из них.

После создания политики параметры, на изменение которых наложен запрет (установлен "замок" ) , начинают действовать на клиентских устройствах независимо от того, какие параметры были определены для приложения ранее.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства[405](#)

Отображение унаследованной политики во вложенной группе

► Чтобы включить отображение унаследованных политик для вложенной группы администрирования:

1. В дереве консоли выберите группу администрирования, для которой нужно отображать унаследованные политики.
2. В рабочей области выбранной группы выберите вкладку **Политики**.
3. В контекстном меню списка политик выберите пункт **Вид** → **Унаследованные политики**.

В результате унаследованные политики отображаются в списке политик со значком:

-  – если они были унаследованы от группы, созданной на главном Сервере администрирования;
-  – если они были унаследованы от группы верхнего уровня.

При включенном режиме наследования параметров изменение унаследованных политик доступно только в той группе, в которой они были созданы. Изменение унаследованных политик недоступно в той группе, которая наследует политики.

Активация политики

► *Чтобы сделать политику активной для выбранной группы:*

1. В рабочей области группы на вкладке **Политики** выберите политику, которую нужно сделать активной.
2. Для активации политики выполните одно из следующих действий:
 - В контекстном меню политики выберите пункт **Активная политика**.
 - В окне свойств политики откройте раздел **Общие** и в блоке параметров **Состояние политики** выберите вариант **Активная политика**.

В результате политика становится активной для выбранной группы администрирования.

При применении политики на большом количестве клиентских устройств на некоторое время существенно возрастают нагрузка на Сервер администрирования и объем сетевого трафика.

Автоматическая активация политики по событию "Вирусная атака"

► *Чтобы политика активировалась автоматически при наступлении события "Вирусная атака":*

1. В окне свойств Сервера администрирования откройте раздел **Вирусная атака**.
2. Откройте окно **Активация политик** по ссылке **Настроить активацию политик по возникновению события "Вирусная атака"** и добавьте политику в выбранный список политик, активируемых при обнаружении вирусной атаки.

В случае активации политики по событию *Вирусная атака* вернуться к предыдущей политике можно только вручную.

Применение политики для автономных пользователей

Политика для автономных пользователей вступает в силу на устройстве в случае его отключения от сети организации.

► *Чтобы применить политику для автономных пользователей:*

в окне свойств политики откройте раздел **Общие** и в блоке параметров **Состояние политики** выберите вариант **Политика для автономных пользователей**.

В результате политика для автономных пользователей начинает действовать на устройствах в случае их отключения от сети организации.

Изменение политики. Откат изменений

► Чтобы изменить политику:

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
3. Внесите необходимые изменения.
4. Нажмите на кнопку **Применить**.

Изменения политики будут сохранены в свойствах политики, в разделе **История ревизий**.

В случае необходимости вы можете откатить изменения политики.

► Чтобы откатить изменения политики:

1. В дереве консоли выберите папку **Политики**.
2. Выберите политику, изменения которой нужно откатить и с помощью контекстного меню перейдите в окно свойств политики.
3. В окне свойств политики выберите раздел **История ревизий**.
4. В списке ревизий политики выберите номер ревизии, к которой нужно откатить изменения.
5. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Сравнение политик

Вы можете сравнивать две политики для одного управляемого приложения. В результате сравнения политик вы получаете отчет, показывающий, какие параметры политик совпадают, а какие различаются. Сравнивать политики бывает нужно, например, если разные администраторы в своих локальных офисах создали несколько политик для одного управляемого приложения или если одна политика верхнего уровня была унаследована и изменена для каждого локального офиса. Вы можете сравнивать политики одним из следующих способов: путем выбора одной политики и сравнения ее с другой или путем сравнения любых двух политик из списка политик.

► Чтобы сравнить политику с другой политикой:

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику, которую нужно сравнить с другой политикой.
3. В контекстном меню политики выберите пункт **Сравнить политику с другой политикой**.
4. В окне **Выбор политики** выберите политику, с которой нужно провести сравнение.
5. Нажмите на кнопку **ОК**.

Отобразится отчет сравнения двух политик для приложения в формате HTML.

► Чтобы сравнить две политики из списка политик:

1. В папке **Политики** в списке политик с помощью клавиши **SHIFT** или **CTRL** выберите две политики для одного управляемого приложения.
2. В контекстном меню выберите пункт **Сравнить**.

Отобразится отчет сравнения двух политик для приложения в формате HTML.

В отчете сравнения параметров политик для приложения Kaspersky Endpoint Security для Windows выполняется также сравнение профилей политики. Результаты сравнения параметров профилей политик можно свернуть. Чтобы свернуть блок, нажмите на значок стрелки (▲) рядом с названием блока.

Просмотр диаграммы состояния применения политики

В Kaspersky Security Center вы можете просмотреть результаты применения политик на каждом устройстве.

► *Чтобы просмотреть статус применения политики на каждом устройстве:*

1. В рабочей области группы на вкладке **Политики** выберите политику, статус распространения которой вы хотите просмотреть.

Диаграмма на правой панели отображает состояние применения политики.

2. Нажмите на кнопку **Подробнее**.

Откроется окно **Результаты применения политики**.

Вы можете экспортировать результаты применения политики в файлы форматов CSV или TXT.

Удаление политики

► *Чтобы удалить политику:*

1. В рабочей области группы администрирования на вкладке **Политики** выберите политику, которую нужно удалить.
2. Удалите политику одним из следующих способов:
 - В контекстном меню политики выберите пункт **Удалить**.
 - Перейдите по ссылке **Удалить политику** в информационном окне выбранной политики.

Копирование политики

► *Чтобы скопировать политику:*

1. В рабочей области нужной вам группы на вкладке **Политики** выберите политику.
2. В контекстном меню политики выберите пункт **Копировать**.
3. Выберите в дереве консоли группу, в которую требуется добавить политику.
Политику можно добавить в ту же группу, из которой она скопирована.
4. В контекстном меню списка политик для выбранной группы на вкладке **Политики** выберите пункт **Вставить**.

В результате политика копируется с сохранением всех параметров и распространяется на устройства группы, в которую она перенесена. Если вы вставляете политику в ту же группу, из которой она была скопирована, индекс (**<следующий порядковый номер>**) автоматически добавляется к имени политики, например: **(1)**, **(2)**.

Активная политика при копировании становится неактивной. В случае необходимости вы можете сделать ее активной.

Экспорт политики

► Чтобы экспортировать политику:

1. Экспортируйте политику одним из следующих способов:
 - В контекстном меню политики выберите пункт **Все задачи** → **Экспортировать**.
 - Перейдите по ссылке **Экспортировать политику в файл** в информационном окне выбранной политики.
2. В открывшемся окне **Сохранить как** укажите имя файла политики и путь. Нажмите на кнопку **Сохранить**.

Импорт политики

► Чтобы импортировать политику:

1. В рабочей области нужной вам группы на вкладке **Политики** выберите один из следующих способов импорта политики:
 - В контекстном меню списка политик выберите пункт **Все задачи** → **Импортировать**.
 - По кнопке **Импортировать политику из файла** в блоке управления списком политик.
2. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать политику. Нажмите на кнопку **Открыть**.

Импортированная политика отображается в списке политик. Также импортируются параметры и профили политики. Независимо от статуса политики, выбранной при экспорте, импортируемая политика неактивна. Вы можете изменить статус политики в свойствах политики.

Если имя новой импортированной политики идентично имени существующей политики, имя импортированной политики расширяется с помощью окончания вида (**<порядковый номер>**), например: **(1)**, **(2)**.

Конвертация политик

Kaspersky Security Center может конвертировать политики предыдущих версий управляемых приложений "Лаборатории Касперского" в политики текущих версий этих приложений. Преобразованные политики сохраняют текущие параметры администратора, заданные до обновления, а также включают новые параметры из актуальных версий приложений. Плагины управления приложениями "Лаборатории Касперского" определяют, доступна ли конвертация политик этих приложений. Информацию о преобразовании политик для каждого поддерживаемого приложения "Лаборатории Касперского" см. в соответствующей справке из следующего списка:

- Приложения "Лаборатории Касперского" для рабочих станций:

- Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/KESWin/12.6/en-US/134238.htm>
- Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/233554.htm>
- Kaspersky Endpoint Security для Linux Elbrus Edition <https://support.kaspersky.com/help/KES4LinuxElbrus/10.1.2/en-US/180528.htm>
- Kaspersky Endpoint Security для Mac https://support.kaspersky.com/KESMac/11.2.1_adminguide/en-US/180604.htm
- Kaspersky Endpoint Agent <https://support.kaspersky.com/KEA/3.13/en-US/232801.htm>
- Kaspersky Embedded Systems Security для Windows <https://support.kaspersky.com/KESS/3.0/en-us/146617.htm>
- **Kaspersky Industrial CyberSecurity:**
 - Kaspersky Industrial CyberSecurity for Nodes <https://support.kaspersky.com/KICS4Nodes/3.1/en-US/146617.htm>
 - Kaspersky Industrial CyberSecurity for Linux Nodes <https://support.kaspersky.com/help/KICS4Linux/1.3/en-US/233542.htm>
 - Kaspersky Industrial CyberSecurity for Networks (централизованное развертывание не поддерживается) <https://support.kaspersky.com/help/KICSforNetworks/3.1/en-US/140030.htm>
- **Kaspersky applications formobile devices:**
 - Kaspersky Endpoint Security для Android <https://support.kaspersky.com/KESMob/10SP4MR3/en-US/99183.htm>
 - Kaspersky Security для iOS <https://support.kaspersky.com/KESMob/10SP4MR3/en-US/99183.htm>
- **Kaspersky applications forfile servers:**
 - Kaspersky Security для Windows Server <https://support.kaspersky.com/KSWS/11.0.1/en-US/146617.htm>
 - Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/KESWin/12.6/en-US/134238.htm>
 - Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/233554.htm>
- **Приложения "Лаборатории Касперского" для виртуальных машин:**
 - Kaspersky Security для виртуальных сред Легкий агент <https://support.kaspersky.com/KSVLA/5.2/en-US/62771.htm>
 - Kaspersky Security для виртуальных сред Защита без агента <https://support.kaspersky.com/KSV/6.0/en-US/84556.htm>
- **Приложения "Лаборатории Касперского" для почтовых систем и серверов SharePoint / серверов совместной работы:**
 - Kaspersky Security для Linux Mail Server <https://support.kaspersky.com/KLMS/8.2/en-US/100512.htm>
 - Kaspersky Security для Microsoft Exchange Servers <https://support.kaspersky.com/KS4Exchange/9.6/en-US/131648.htm>
- **Приложения "Лаборатории Касперского" для обнаружения целевых атак:**

- Kaspersky Sandbox <https://support.kaspersky.com/KSB/2.0/en-US/189564.htm>
- Kaspersky Endpoint Detection and Response Optimum https://support.kaspersky.com/KEDR_Optimum/2.3/en-US/220194.htm
- Kaspersky Managed Detection and Response <https://support.kaspersky.com/MDR/en-US/196544.htm>
- **Kaspersky applications for KasperskyOS devices:**
 - Kaspersky IoT Secure Gateway <https://support.kaspersky.com/IoTSecureGateway/2.1/en-US/188039.htm>
 - Kaspersky Security Management Suite (плагин для Kaspersky Thin Client) <https://support.kaspersky.com/help/KTC/2.0/en-US/231960.htm>

► Чтобы конвертировать политики:

1. В дереве консоли выберите Сервер администрирования, для которого вы хотите выполнить конвертацию политик.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи → Мастер массовой конвертации политик и задач**.

В результате запускается мастер массовой конвертации политик и задач. Следуйте далее указаниям мастера.

После завершения работы мастера создаются политики, использующие текущие параметры политик администратора и новые параметры из актуальных версий приложений "Лаборатории Касперского".

Управление профилями политик

В этом разделе описывается управление профилями политики и предоставляется информация о просмотре профилей политики, изменении приоритета профиля политики, создании профиля политики, изменении профиля политики, копировании профиля политики, создании правила активации профиля политики и удалении профиля политики.

В этом разделе

О профиле политики.....	442
Создание профиля политики	445
Изменение профиля политики.....	446
Удаление профиля политики	447
Создание правила активации профиля политики.....	447

О профиле политики

Профиль политики – это именованный набор параметров политики, который активируется на клиентском устройстве (компьютере, мобильном устройстве), если устройство удовлетворяет заданным правилам активации (см. раздел "Создание правила активации профиля политики" на стр. [447](#)). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики. Например, возможна ситуация, когда в группе администрирования для некоторых устройств параметры политики должны быть изменены. В этом случае для такой политики можно настроить профили политики, использование которых позволяет изменять параметры политики не для всех устройств группы администрирования. Например, политика запрещает запуск приложений городской навигации для всех устройств группы администрирования "Пользователи". Приложения городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". На этом устройстве можно установить тег "Курьер" и настроить профиль политики таким образом, чтобы был разрешен запуск приложений городской навигации только на устройстве с тегом "Курьер", с сохранением всех остальных параметров политики. В этом случае если в группе администрирования "Пользователи" появляется устройство с тегом "Курьер", на нем будет разрешен запуск приложений городской навигации. Запуск приложений городской навигации на других устройствах в группе администрирования "Пользователи", у которых тег "Курьер" отсутствует, будет запрещен.

Профили поддерживаются только для следующих политик:

- политики Kaspersky Endpoint Security для Windows;
- политики Kaspersky Endpoint Security для Mac;
- политики плагина Kaspersky Mobile Device Management версий от 10 Service Pack 1 до 10 Service Pack 3 Maintenance Release 1;
- политики плагина Kaspersky Device Management для iOS;
- политики Kaspersky Security для виртуальных сред 5.1 Легкий агент для Windows;
- политики Kaspersky Security для виртуальных сред 5.1 Легкий агент для Linux.

Профили политик облегчают управление клиентскими устройствами, на которых применены политики:

- Параметры профиля политики могут отличаться от параметров самой политики.
- Не требуется поддерживать и применять вручную несколько копий одной политики, которые различаются только небольшим количеством параметров.
- Не требуется отдельная политика для автономных пользователей.
- Вы можете экспортировать и импортировать профили политики, а также создавать новые профили на основе существующих.
- Для одной политики несколько профилей политики могут быть активными. К устройству будут применены те из профилей, которые удовлетворяют правилам активации на этом устройстве.
- Профили подчиняются иерархии политик. Унаследованная политика содержит все профили политики верхнего уровня.

Приоритеты профилей

Профили, созданные для политики, упорядочены в порядке убывания приоритета. Например, если профиль X находится выше профиля Y в списке профилей, то профиль X имеет более высокий приоритет, чем Y. К одному устройству одновременно могут быть применены несколько профилей. Если значение какого-то параметра различается в профилях, на устройстве применится значение параметра из того профиля, который имеет более высокий приоритет.

Правила активации профиля

Профиль политики активируется на клиентском устройстве при выполнении правила активации. *Правила активации* – набор условий, при выполнении которых профиль политики начинает работать на устройстве.

Правило активации может содержать следующие условия:

- Агент администрирования на клиентском устройстве подключается к Серверу с определенным набором параметров подключения, например, адрес Сервера, номер порта и так далее.
- Клиентское устройство находится в автономном режиме.
- Клиентскому устройству назначены определенные теги.
- Клиентское устройство явно (устройство находится непосредственно в указанном подразделении) или неявно (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности) размещено в определенном подразделении Active Directory, устройство или его владелец находятся в группе безопасности Active Directory.
- Клиентское устройство принадлежит определенному владельцу или владелец устройства находится во внутренней группе безопасности Kaspersky Security Center.
- Владелец клиентского устройства была назначена определенная роль.

Политики в иерархии групп администрирования

Если вы создаете политику в группе администрирования нижнего уровня, то новая политика наследует профили активной политики для группы верхнего уровня. Профили с одинаковыми именами объединяются. Профили политики для группы более высокого уровня имеют более высокий приоритет. Например, в группе администрирования *A* политика *P(A)* имеет профили *X1*, *X2*, и *X3*, в порядке убывания приоритета. В группе администрирования *B*, которая является подгруппой группы *A*, создана политика *P(B)*, с профилями *X2*, *X4*, *X5*. Тогда политика *P(B)* будет изменена политикой *P(A)*, так, что в политике *P(B)* список профилей в порядке убывания приоритета будет *X1*, *X2*, *X3*, *X4*, *X5*. Приоритет профиля *X2* будет зависеть от начального состояния *X2* политики *P(B)* и *X2* политики *P(A)*. После создания политики *P(B)* политика *P(A)* не будет отображаться в подгруппе *B*.

Активная политика вычисляется каждый раз заново при запуске Агента администрирования, при включении и выключении автономного режима, а также при изменении списка тегов, назначенных клиентскому устройству. Например, устройству увеличили объем оперативной памяти, в результате активировался профиль политики, который применяется для устройств с большим объемом оперативной памяти.

Свойства и ограничения профиля политики

Профили имеют следующие свойства:

- Профили неактивной политики не влияют на клиентские устройства.
- Если для политики установлено состояние **Политика для автономных пользователей**, профили политики также будут применяться при отключении устройства от корпоративной сети.
- Профили не поддерживают статический анализ доступа к исполняемым файлам (см. раздел "Просмотр результатов статического анализа правил запуска исполняемых файлов" на стр. [584](#)).
- Профиль политики не может содержать параметры оповещений о событиях.
- Если используется UDP-порт 15000 для подключения устройства к Серверу администрирования, то при назначении тега устройству соответствующий профиль политики активируется в течение одной минуты.
- Вы можете использовать правила подключения Агента администрирования к Серверу администрирования (см. раздел "Создание правила переключения Агента администрирования по сетевому местоположению" на стр. [308](#)), когда вы создаете правила активации профиля политики.

Создание профиля политики

Создание профиля доступно только для политик следующих приложений:

- Kaspersky Endpoint Security 10 Service Pack 1 для Windows и выше;
- Kaspersky Endpoint Security 10 Service Pack 1 для Mac;
- плагина Kaspersky Mobile Device Management до версий 10 Service Pack 3 Maintenance Release 1;
- плагина Kaspersky Device Management для iOS;
- Kaspersky Security для виртуальных сред 5.1 Легкий агент для Windows и Linux.

► Чтобы создать профиль политики:

1. В дереве консоли выберите группу администрирования, для политики которой нужно создать профиль политики.
2. В рабочей области группы администрирования выберите вкладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Выберите раздел **Профили политики** в окне свойств политики и нажмите на кнопку **Добавить**. Запустится мастер создания профиля политики.
5. В окне мастера **Имя профиля политики** укажите:
 - a. Имя профиля политики.
Имя профиля не может превышать 100 символов.
 - b. Состояние профиля политики (*Включен* или *Выключен*).
Рекомендуется создавать неактивные профили политики и включать их только после полного завершения настройки параметров и условий активации профилей политики.
6. Установите флажок **После закрытия мастера создания профиля политики перейти к настройке правила активации профиля политики**, чтобы запустить мастер создания правила активации профиля политики (см. раздел "Создание правила активации профиля политики" на стр. [447](#)). Следуйте инструкциям мастера.
7. Измените параметры профиля политики в окне свойств профиля политики (см. раздел "Изменение профиля политики" на стр. [446](#)), как вам необходимо.
8. Сохраните изменения, нажав на кнопку **ОК**.
Профиль будет сохранен. Профиль будет активирован на устройствах, удовлетворяющих правилам активации.

Для одной политики можно создать несколько профилей политики. Профили, созданные для политики, отображаются в свойствах политики в разделе **Профили политики**. Вы можете изменить профиль политики и приоритет профиля (см. раздел "Изменение профиля политики" на стр. [446](#)), а также удалить профиль (см. раздел "Удаление профиля политики" на стр. [447](#)).

См. также:

Настройка и распространение политик: подход, ориентированный на устройства[405](#)

Изменение профиля политики

Изменение параметров профиля политики

Изменение профиля доступно только для политик Kaspersky Endpoint Security для Windows.

► Чтобы изменить профиль политики:

1. В дереве консоли выберите группу администрирования, для которой нужно изменить профиль политики.
2. В рабочей области группы выберите вкладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Откройте раздел **Профили политики** в свойствах политики.
В разделе содержится список профилей, созданных для политики. Профили в списке отображаются в соответствии с их приоритетом.
5. Выберите профиль политики и нажмите на кнопку **Свойства**.
6. В окне свойств настройте параметры профиля:
 - Если необходимо, в разделе **Общие** измените имя профиля и включите или выключите профиль с помощью флажка **Включить профиль**.
 - В разделе **Правила активации** измените правила активации профиля.
 - Измените параметры политики в соответствующих разделах.
7. Нажмите на кнопку **ОК**.

Измененные параметры начнут действовать после синхронизации устройства с Сервером администрирования (если профиль политики активен) либо после выполнения правила активации (если профиль политики неактивен).

Изменение приоритета профиля политики

Приоритет профилей политик определяет порядок активации профилей на клиентском устройстве. Приоритет используется, если для разных профилей политики заданы одинаковые правила активации.

Например, созданы два профиля политики: *Профиль 1* и *Профиль 2*, отличающиеся друг от друга значениями одного параметра (*Значение 1* и *Значение 2*). Приоритет *Профиля 1* выше, чем приоритет *Профиля 2*. Кроме того, существуют профили с более низким приоритетом, чем *Профиль 2*. Правила активации профилей совпадают.

При выполнении правила активации будет активирован *Профиль 1*. Параметр на устройстве примет *Значение 1*. Если удалить *Профиль 1*, то *Профиль 2*, будет иметь самый высокий приоритет, и параметр примет *Значение 2*.

В списке профилей политики профили отображаются в соответствии с их приоритетом. На первом месте в списке стоит профиль с самым высоким приоритетом. Приоритет профиля можно изменять с помощью

кнопок со стрелкой вверх  и со стрелкой вниз .

Удаление профиля политики

► Чтобы удалить профиль политики:

1. Выберите в дереве консоли группу администрирования, для которой нужно удалить профиль политики.
2. В рабочей области группы администрирования выберите вкладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Откройте раздел **Профили политики** в свойствах политики Kaspersky Endpoint Security.
5. Выберите профиль политики, который нужно удалить, и нажмите на кнопку **Удалить**.

В результате профиль политики будет удален. Активным станет либо другой профиль политики, правила активации которого выполняются на устройстве, либо политика.

Создание правила активации профиля политики

► Чтобы создать правило активации профиля политики:

1. В дереве консоли выберите группу администрирования, для которой нужно создать правило активации профиля политики.
2. В рабочей области группы выберите вкладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Выберите раздел **Профили политики** в окне свойств политики.
5. Выберите профиль политики, для которого нужно создать правило активации, и нажмите на кнопку **Свойства**.

В результате откроется окно свойств профиля политики.

Если список профилей политики пуст, вы можете создать профиль политики (см. раздел "Создание профиля политики" на стр. [445](#)).

6. Выберите раздел **Правила активации** и нажмите на кнопку **Добавить**.
В результате запустится мастер создания правила активации профиля политики.
7. В окне **Правила активации профиля политики** установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

- **Общие правила активации профиля политики**

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

- **Правила для использования Active Directory**

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от размещения устройства в подразделении Active Directory или же от членства устройства или его владельца в группе безопасности Active Directory.

- **Правила для определенного владельца устройства**

Установите флажок, чтобы настроить правила активации профиля политики на

устройстве в зависимости от того, кто является владельцем устройства, и от членства устройства во внутренней группе безопасности Kaspersky Security Center.

- **Правило для характеристик оборудования**

Установите флажок, чтобы настроить условие активации на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.

8. В разделе **Общие условия** укажите следующие параметры:

- В поле **Устройство в автономном режиме** в раскрывающемся списке укажите условие нахождения устройства в сети:

- **Да**

Устройство находится во внешней сети, то есть Сервер администрирования недоступен.

- **Нет**

Устройство находится в сети, Сервер администрирования доступен.

- **Значение не выбрано**

Критерий не применяется.

- В поле **Устройство находится в указанном сетевом местоположении** с помощью раскрывающихся списков настройте активацию профиля политики при выполнении/невыполнении на устройстве правила подключения к Серверу администрирования:

- **Выполняется/Не выполняется**

Условие активации профиля политики (правило выполняется или не выполняется).

- **Имя правила**

Описание сетевого местоположения устройства для подключения к Серверу администрирования, при выполнении или невыполнении условий которого профиль политики будет активирован.

Описание сетевого местоположения устройств для подключения к Серверу администрирования можно создать или настроить в правиле переключения Агента администрирования.

Окно **Общие условия** отображается, если был установлен флажок **Общие правила активации профиля политики**.

9. В разделе **Условия с использованием тегов** укажите следующие параметры:

- **Список тегов**

В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тега.

Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

- **Применить к устройствам без выбранных тегов**

Установите флажок, если необходимо инвертировать выбор тегов.

Если флажок установлен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если флажок снят, критерий не применяется. По умолчанию флажок снят.

Окно **Условия с использованием тегов** отображается, если установлен флажок **Общие правила активации профиля политики**.

10. В разделе **Условия с использованием Active Directory** укажите следующие параметры:

- **Членство владельца устройства в группе безопасности Active Directory**

Если флажок установлен, профиль политики активируется на устройстве, владелец которого является членом указанной группы безопасности или членом групп безопасности, входящих в указанную группу. Вы можете указать группу безопасности Active Directory, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Членство устройства в группе безопасности Active Directory**

Если флажок установлен, профиль политики активируется на устройстве, которое является членом указанной группы безопасности или членом групп безопасности, входящих в указанную группу. Вы можете указать группу безопасности Active Directory, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Размещение устройства в подразделении Active Directory**

Если флажок установлен, профиль политики активируется на устройстве, которое явно или неявно входит в указанное подразделение Active Directory. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

Окно **Условия с использованием Active Directory** отображается, если установлен флажок **Правила для использования Active Directory**.

1. В разделе **Условия с использованием владельца устройства** укажите следующие параметры:

- **Владелец устройства**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- устройство принадлежит указанному владельцу (знак "=");
- устройство не принадлежит указанному владельцу (знак "≠").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Владелец устройства входит во внутреннюю группу безопасности**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky Security Center. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- владелец устройства является членом указанной группы безопасности (знак "=");
- владелец устройства не является членом указанной группы безопасности (знак "≠").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky Security Center, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Активировать профиль политики по наличию роли у владельца устройства**

Включите этот параметр, чтобы настроить и включить правило активации профиля политики на устройстве в зависимости от наличия определенной роли (см. раздел "Настройка прав. Пользовательские роли" на стр. [809](#)) у его владельца. Добавить роль вручную из списка существующих ролей.

Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием.

Окно **Условия с использованием владельца устройства** отображается, если установлен флажок **Правила для определенного владельца устройства**.

1. В разделе **Условия с использованием характеристик оборудования** укажите следующие параметры:

- **Объем оперативной памяти (МБ)**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- объем оперативной памяти устройства меньше указанного значения (знак "<");
- объем оперативной памяти устройства больше указанного значения (знак ">").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной памяти устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Количество логических процессоров**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- количество логических процессоров устройства меньше или равно указанному значению (знак "<=");
- количество логических процессоров устройства больше или равно указанному значению (знак ">=").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

Окно **Условия с использованием характеристик оборудования** отображается, если установлен флажок **Правило для характеристик оборудования**.

2. В окне **Имя правила активации профиля политики** в поле **Имя правила** укажите название правила.

В результате профиль будет сохранен. Профиль будет активирован на устройстве, когда будут выполнены правила активации.

Правила активации профиля политики, созданные для профиля, отображаются в свойствах профиля политики в разделе **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства 405

Правила перемещения устройств

Рекомендуется автоматизировать процесс размещения устройств в группах администрирования при помощи *правил перемещения устройств*. Правило перемещения состоит из трех основных частей: имени, условия выполнения (логического выражения над атрибутами устройства) и целевой группы администрирования. Правило перемещает устройство в целевую группу администрирования, если атрибуты устройства удовлетворяют условию выполнения правила.

Правила перемещения устройств имеют приоритеты. Сервер администрирования проверяет атрибуты устройства на соответствие условию выполнения каждого правила, в порядке убывания приоритета правил. Если атрибуты устройства удовлетворяют условию выполнения правила, то устройство перемещается в целевую группу, и на этом обработка правил для этого устройства прекращается. Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Правила перемещения устройств могут создаваться неявно. Например, в свойствах пакета или задачи удаленной установки может быть указана группа администрирования, в которую должно попасть устройство после установки на нем Агента администрирования. Также правила перемещения могут быть созданы администратором Kaspersky Security Center в явном виде, в списке правил перемещения. Список расположен в Консоли администрирования в свойствах группы **Нераспределенные устройства**.

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает только один раз устройства, находящиеся в группе **Нераспределенные устройства**. Если устройство однажды было перемещено этим правилом, правило не переместит его повторно, даже если вернуть устройство вручную в группу **Нераспределенные устройства**. Это рекомендуемый способ использования правил перемещения.

Можно перемещать устройства, уже размещенные в группах администрирования. Для этого в свойствах правила снимите флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования. Флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования** заблокирован в свойствах автоматически созданных правил перемещения. Такие правила создаются при добавлении задачи *Удаленная установка приложения* или создании автономного инсталляционного пакета.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенной точки распространения.

Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и на сетевой трафик. Также эти сценарии противоречат модели работы Kaspersky Security Center (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик (на стр. [432](#)), задачи для выборок устройств (см. раздел "Задачи" на стр. [48](#)), назначать Агенты администрирования согласно методике (см. раздел "Настройка точек распространения и шлюзов соединений" на стр. [685](#)).

См. также:

Сценарий: обнаружение сетевых устройств	322
Основной сценарий установки.....	56
Создание правил автоматического перемещения устройств в группы администрирования	335

Копирование правил перемещения устройств

Если вам нужно создать несколько правил перемещения устройств с аналогичными параметрами, вы можете скопировать существующее правило, а затем изменить параметры скопированного правила. Например, это удобно, когда вам нужно иметь несколько одинаковых правил перемещения устройств с разными IP-диапазонами и целевыми группами.

► Чтобы скопировать правило перемещения устройств:

1. Откройте главное окно приложения.
2. В папке **Нераспределенные устройства** нажмите на кнопку **Настроить правила**.
Откроется окно **Свойства: Нераспределенные устройства**.
3. В разделе **Перемещение устройств** выберите правило перемещения устройств, которое вы хотите скопировать.
4. Нажмите на кнопку **Клонировать правило**.
Копия выбранного правила будет добавлена в конец списка.

Новое правило будет создано выключенным. Вы можете выключить или изменить правило в любое время.

Категоризация программного обеспечения

Основным средством контроля запуска приложений являются *категории "Лаборатории Касперского"* (далее также *KL-категории*). KL-категории облегчают администратору Kaspersky Security Center работу по поддержанию категоризации ПО и минимизируют объем трафика, передаваемого на управляемые устройства.

Пользовательские категории следует создавать только для приложений, не подпадающих ни под одну KL-категорию (например, для приложений, разработанных на заказ). Пользовательские категории создаются на основе дистрибутива приложения (MSI) или на основе папки с дистрибутивами.

В случае если имеется большая пополняемая коллекция программного обеспечения, не категоризированного при помощи KL-категорий, может быть целесообразным создать автоматически обновляемую категорию. Такая категория будет автоматически пополняться контрольными суммами исполняемых файлов при изменении папки с дистрибутивами.

Не создавайте автоматически обновляемые категории программного обеспечения для папок Мои документы, %windir%, %ProgramFiles% и %ProgramFiles(x86)%. Файлы в этих папках часто меняются, что приводит к увеличению нагрузки на Сервер администрирования и к увеличению трафика в сети. Следует создать отдельную папку с коллекцией программного обеспечения и время от времени пополнять ее.

Необходимые условия для установки приложений на устройства организации-клиента

Процесс удаленной установки приложений на устройства организации-клиента совпадает с процессом удаленной установки приложений внутри организации (см. раздел "Приложения "Лаборатории Касперского". Централизованное развертывание" на стр. [357](#)).

Для установки приложений на устройства организации-клиента необходимо выполнение следующих условий:

- Перед первой установкой приложений на устройства организации-клиента требуется установить на них Агент администрирования.

При настройке инсталляционного пакета Агента администрирования поставщиком услуг в приложении Kaspersky Security Center в окне свойств инсталляционного пакета требуется настроить следующие параметры:

- В разделе **Подключение** в строке **Сервер администрирования** требуется указать тот же адрес виртуального Сервера администрирования, что и при локальной установке Агента администрирования на точку распространения.
- В разделе **Дополнительно** установите флажок **Подключаться к Серверу администрирования через шлюз соединения**. В строке **Адрес шлюза соединения** нужно указать адрес точки распространения. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.
- В качестве способа загрузки инсталляционного пакета Агента администрирования необходимо выбрать **Средствами операционной системы с помощью точек распространения**. Выбор способа загрузки осуществляется следующим образом:
 - При установке приложений с помощью задач удаленной установки способ загрузки можно выбрать двумя способами:
 - при создании задачи удаленной установки в окне **Параметры**;
 - в окне свойств задачи удаленной установки в разделе **Параметры**.

- При установке приложений с помощью мастера удаленной установки способ загрузки можно выбрать в окне мастера **Параметры**.
- Учетная запись, под которой работает точка распространения, должна иметь доступ к ресурсу Admin\$ на клиентских устройствах.

Просмотр и изменение локальных параметров приложения

Система администрирования Kaspersky Security Center позволяет удаленно управлять локальными параметрами приложений на устройствах через Консоль администрирования.

Локальные параметры приложения – это параметры приложения, индивидуальные для устройства. С помощью Kaspersky Security Center вы можете устанавливать локальные параметры приложений для устройств, входящих в группы администрирования.

Подробные описания параметров приложений "Лаборатории Касперского" приводятся в руководствах для этих приложений.

► *Чтобы просмотреть или изменить локальные параметры приложения:*

1. В рабочей области группы, в которую входит нужное вам устройство, выберите вкладку **Устройства**.
2. В окне свойств в разделе **Приложения** выберите соответствующее приложение.
3. Откройте окно свойств приложения двойным щелчком мыши по названию приложения или нажатием на кнопку **Свойства**.

В результате откроется окно локальных параметров выбранного приложения, которые можно просмотреть и изменить.

Вы можете изменять значения тех параметров, изменение которых не запрещено групповой политикой (параметр не закрыт замком (🔒) в политике).

Обновление Kaspersky Security Center и управляемых приложений

В этом разделе описаны шаги, которые необходимо выполнить для обновления Kaspersky Security Center и управляемых приложений.

В этом разделе

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455
Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"	460
Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"	467
Включение функции загрузки файлов различий	468
Создание задачи для загрузки обновлений в хранилище Сервера администрирования	469
Создание задачи загрузки обновлений в хранилища точек распространения	474
Настройка параметров задачи загрузки обновлений в хранилище Сервера администрирования ..	479
Проверка полученных обновлений	479
Настройка проверочных политик и вспомогательных задач	481
Просмотр полученных обновлений	482
Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства	482
Офлайн-модель получения обновлений	484
Включение и выключение офлайн-модели получения обновлений	485
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center	487
Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center	487
Автоматическое распространение обновлений	488
Удаление обновлений программного обеспечения из хранилища	497
Установка патча для приложения "Лаборатории Касперского" в кластерной модели	497

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, модулей приложений и приложений "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации (см. раздел "Сценарий: настройка защиты сети" см. стр. [403](#)), вам нужно поддерживать надежность системы защиты, чтобы обеспечить защиту Серверов администрирования и управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Защита сети поддерживается обновленной с помощью регулярных обновлений следующего:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложений безопасности.

Когда вы завершите этот сценарий, вы можете быть уверены, что:

- Ваша сеть защищена самым последним программным обеспечением "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложения безопасности.
- Антивирусные базы и другие базы данных "Лаборатории Касперского", критически важные для безопасности сети, всегда актуальны.

Предварительные требования

Управляемые устройства должны иметь соединение с Сервером администрирования. Если у устройств нет соединения, рассмотрите возможность обновления баз, программных модулей и программ «Лаборатории Касперского» вручную или напрямую с серверов обновлений «Лаборатории Касперского».

Сервер администрирования должен иметь подключение к интернету.

Прежде чем приступить, убедитесь, что вы выполнили следующее:

1. Развернуты приложения безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console.
2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети (см. раздел "Сценарий: настройка защиты сети" см. стр. [403](#)).
3. Назначено соответствующее количество точек распространения (см. раздел "Расчет количества и конфигурации точек распространения" на стр. [149](#)) в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и приложений «Лаборатории Касперского» состоит из следующих этапов:

а. Выбор схемы обновления

Существует несколько схем (см. раздел "Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"" см. стр. [460](#)), которые вы можете использовать для установки обновлений компонентов Kaspersky Security Center и приложений безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

б. Создание задачи для загрузки обновлений в хранилище Сервера администрирования

Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, создайте задачу сейчас.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования, а также обновления баз и модулей приложений для Kaspersky Security Center. После загрузки обновлений их можно распространять на управляемые устройства.

Если в вашей сети назначены точки распространения, обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. В этом случае управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.

Инструкции:

- Консоль администрирования: Создание задачи для загрузки обновлений в хранилище Сервера администрирования (на стр. [469](#)).

- Kaspersky Security Center Web Console: Создание задачи для загрузки обновлений в хранилище Сервера администрирования

с. Создание задачи загрузки обновлений в хранилища точек распространения (если требуется)

По умолчанию обновления загружаются в хранилища точек распространения из хранилища Сервера администрирования. Вы можете настроить Kaspersky Security Center так, чтобы точки распространения загружали обновления непосредственно с серверов обновлений "Лаборатории Касперского". Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Когда вашей сети назначены точки распространения и создана задача *Загрузка обновлений в хранилища точек распространения*, точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Инструкции:

- Консоль администрирования: Создание задачи загрузки обновлений в хранилища точек распространения (на стр. [474](#)).
- Kaspersky Security Center Web Console: Создание задачи загрузки обновлений в хранилища точек распространения.

d. Настройка точек распространения

Если в вашей сети назначены точки распространения (см. раздел "Назначение устройства точкой распространения вручную" на стр. [491](#)), убедитесь, что параметр **Распространять обновления** включен в свойствах всех требуемых точек распространения. Если этот параметр выключен для точки распространения, устройства, включенные в область действия точки распространения, загружают обновления из хранилища Сервера администрирования.

Если вы хотите, чтобы управляемые устройства получали обновления только от точек распространения, включите параметр **Распространять файлы только через точки распространения** в политике Агента администрирования (см. раздел "Параметры политики Агента администрирования" см. стр. [789](#)).

e. Оптимизация процесса обновления с использованием офлайн-модели получения обновлений или загрузки файлов различий (если требуется)

Вы можете оптимизировать процесс обновления, используя офлайн-модель загрузки обновлений (см. раздел "Офлайн-модель получения обновлений" на стр. [484](#)) (включена по умолчанию), или используя файлы различий (см. раздел "Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"" см. стр. [467](#)). Для каждого сегмента сети вам нужно выбрать, какую из этих двух функций включить, так как они не могут работать одновременно.

Когда офлайн-модель получения обновлений включена, Агент администрирования загружает необходимые обновления на управляемое устройство после загрузки обновлений в хранилище Сервера администрирования, прежде чем приложение безопасности запросит обновления. Это повышает надежность процесса обновления. Чтобы использовать эту функцию, включите параметр **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)** в свойствах задачи Политика Агента администрирования (см. раздел "Параметры политики Агента администрирования" см. стр. [789](#)).

Если вы не используете офлайн-модель загрузки обновлений, вы можете оптимизировать трафик между Сервером администрирования и управляемыми устройствами, используя файлы различий. Когда эта функция включена, Сервер администрирования или точка распространения загружает файлы различий вместо целых файлов баз данных или модулей приложений "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или

модулями приложения. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Загрузить файлы различий** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

Инструкции:

- Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского" (см. раздел "Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"" см. стр. [467](#)).
- Консоль администрирования: Включение и выключение офлайн-модели получения обновлений (на стр. [485](#)).
- Kaspersky Security Center Web Console: Консоль администрирования: Включение и выключение офлайн-модели получения обновлений.

f. Проверка полученных обновлений (если требуется)

Перед установкой загруженных обновлений вы можете проверить обновления с помощью задачи *Проверка обновлений*. Эта задача последовательно запускает задачи обновления устройства и задачи поиска вредоносного ПО, настроенные с помощью параметров для указанного набора тестовых устройств. После получения результатов задачи Сервер администрирования запустит или заблокирует распространение обновлений на оставшиеся устройства.

Задача *Проверка обновлений* может быть выполнена как часть задачи *Загрузка обновлений в хранилище Сервера администрирования*. В свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* включите параметр **Выполнять проверку обновлений перед распространением** в Консоли администрирования или параметр **Выполнить проверку обновлений** в Kaspersky Security Center Web Console.

Инструкции:

- Консоль администрирования: Проверка полученных обновлений (на стр. [479](#)).
- Kaspersky Security Center Web Console: Проверка полученных обновлений.

g. Одобрение и отклонение обновлений программного обеспечения

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус обновления на *Одобрено* или *Отклонено*. Одобренные обновления всегда устанавливаются. Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Неопределенные обновления могут быть установлены только на Агента администрирования и других компонентах Kaspersky Security Center (см. раздел "Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center" на стр. [487](#)) в соответствии с параметрами политики Агента администрирования. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для приложения безопасности было установлено, Kaspersky Security Center попытается удалить обновления со всех устройств. Обновления для компонентов Kaspersky Security Center не могут быть удалены.

Инструкции:

- Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения (на стр. [505](#)).
- Kaspersky Security Center Web Console: Одобрение и отклонение обновлений программного обеспечения.

h. Настройка автоматической установки обновлений и патчей для компонентов Kaspersky Security Center

Загруженные обновления и патчи для Агента администрирования и других компонентов Kaspersky Security Center (см. раздел "Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center" на стр. [487](#)) устанавливаются автоматически. Если вы оставили включенным параметр **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** в свойствах Агента администрирования, тогда все обновления будут установлены автоматически после их загрузки в хранилище (или несколько хранилищ). Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобен*.

Инструкции:

- Консоль администрирования: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center (см. стр. [487](#)).
- Kaspersky Security Center Web Console: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center.

i. Установка обновлений для Сервера администрирования

Обновления программного обеспечения для Сервера администрирования не зависят от статусов обновлений. Они не устанавливаются автоматически и должны быть предварительно одобрены администратором на вкладке **Мониторинг** в Консоли администрирования (**Сервер администрирования** <имя Сервера> → **Мониторинг**) или в разделе **Уведомления** в Kaspersky Security Center Web Console (**Мониторинг и отчеты** → **Уведомления**). После этого администратор должен явно запустить установку обновлений.

j. Настройка автоматической установки обновлений для приложений безопасности

Создайте задачу *Обновление* для управляемых приложений, чтобы обеспечить своевременное обновление приложений, модулей приложений и баз данных "Лаборатории Касперского", в том числе антивирусных баз. Рекомендуется выбрать параметр **При загрузке обновлений в хранилище** при настройке расписания задач для своевременного обновления.

Если в вашей сети есть устройства, поддерживающие только IPv6, и вы хотите регулярно обновлять приложения безопасности, установленные на этих устройствах, убедитесь, что на управляемых устройствах установлены Сервер администрирования (версии 13.2 или выше) и Агент администрирования (версии 13.2 или выше).

По умолчанию обновления для Kaspersky Endpoint Security для Windows и для Kaspersky Endpoint Security для Linux устанавливаются только после изменения статуса обновления на *Одобрено*. Вы можете изменить параметры обновления в задаче *Обновление*.

Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства.

Инструкции:

- Консоль администрирования: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства (на стр. [482](#)).
- Kaspersky Security Center Web Console: Консоль администрирования: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства.

Результаты

По завершении сценария Kaspersky Security Center настроен для обновления баз "Лаборатории Касперского" и установленных приложений "Лаборатории Касперского" после загрузки обновлений в

хранилище Сервера администрирования или в хранилища точек распространения. Теперь вы можете приступить к мониторингу состояния сети.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вам нужно своевременно предоставлять обновления следующего:

- Баз и модулей приложений "Лаборатории Касперского".

Kaspersky Security Center проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и модулей приложений "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы (см. раздел "Доступ к общедоступным DNS-серверам" на стр. [919](#)). Это необходимо для обновления антивирусных баз и поддержания уровня безопасности управляемых устройств.

- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложений безопасности.

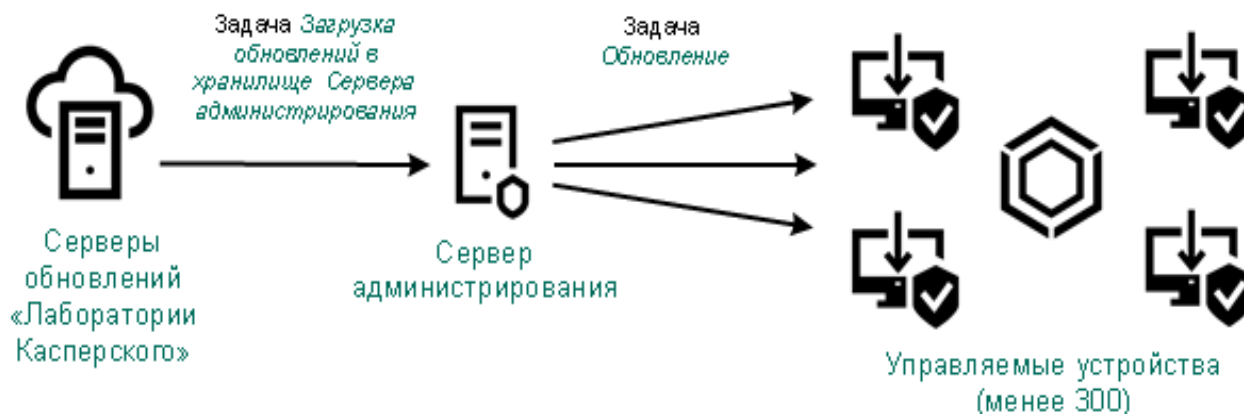
В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- С помощью одной задачи: *Загрузка обновлений в хранилище Сервера администрирования*
- С помощью двух задач:
 - *Задача Загрузка обновлений в хранилище Сервера администрирования.*
 - *Задача Загрузка обновлений в хранилища точек распространения.*
- Вручную через локальную папку, общую папку или FTP-сервер
- Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах
- Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

Использование задачи *Загрузка обновлений в хранилище Сервера администрирования*

В этой схеме Kaspersky Security Center загружает обновления с помощью задачи *Загрузка обновлений в хранилище Сервера администрирования*. В небольших сетях, которые содержат менее 300 управляемых устройств в одном сегменте сети или менее десяти управляемых устройств в каждом сегменте, обновления

распространяются на управляемые устройства непосредственно из хранилища Сервера администрирования (см. рисунок ниже).

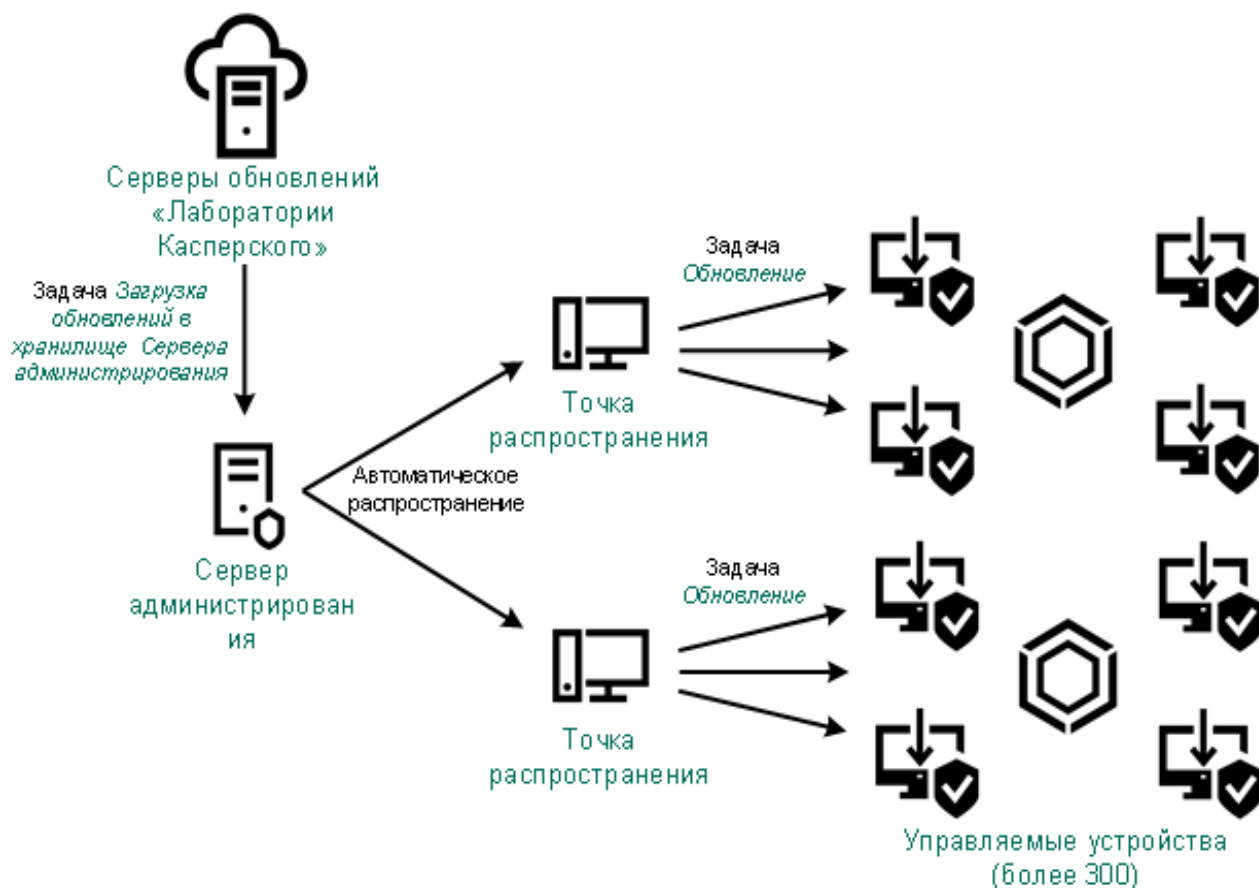


По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

Если ваша сеть содержит более 300 управляемых устройств в одном сегменте сети или ваша сеть содержит несколько сегментов, в которых больше девяти управляемых устройств, мы рекомендуем использовать точки распространения (см. раздел "О точках распространения" на стр. [147](#)) для распространения обновлений на управляемые устройства (см. рисунок ниже). Точки распространения уменьшают загрузку Сервера администрирования и оптимизируют трафик между Сервером администрирования и управляемыми устройствами. Вы можете рассчитать (см. раздел "Расчет количества и конфигурации точек распространения" на стр. [149](#)) количество точек распространения и их конфигурацию, необходимые для вашей сети.

В этой схеме обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. Управляемые устройства, входящие в область действия точки

распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.



После завершения задачи *Загрузка обновлений в хранилище Сервера администрирования* следующие обновления загружаются в хранилище Сервера администрирования:

- Базы и модули приложений "Лаборатории Касперского" для Kaspersky Security Center.
Эти обновления устанавливаются автоматически.
- Базы и модули приложений "Лаборатории Касперского" для приложений безопасности на управляемых устройствах.
Эти обновления устанавливаются с помощью задачи Обновление Kaspersky Endpoint Security для Windows.
- Обновления для Сервера администрирования.
Эти обновления не устанавливаются автоматически. Администратор должен явно одобрить обновления и запустить установку обновлений.

Для установки патчей на Сервере администрирования требуются права локального администратора.

- Обновления для компонентов Kaspersky Security Center.

По умолчанию эти обновления устанавливаются автоматически. Вы можете изменить параметры политики Агента администрирования.

- Обновления для приложений безопасности.

По умолчанию приложение Kaspersky Endpoint Security для Windows устанавливает только те обновления, которые вы одобрили. (Вы можете одобрить обновления с помощью Консоли администрирования (см. раздел "Одобрение и отклонение обновлений программного обеспечения" на стр. [505](#)) или Kaspersky Security Center Web Console). Обновления устанавливаются с помощью задачи *Обновление* и могут быть настроены в свойствах этой задачи.

*Задача **Загрузка обновлений в хранилище Сервера администрирования** недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.*

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

Каждое управляемое приложение "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются приложениями. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и модулей приложений "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

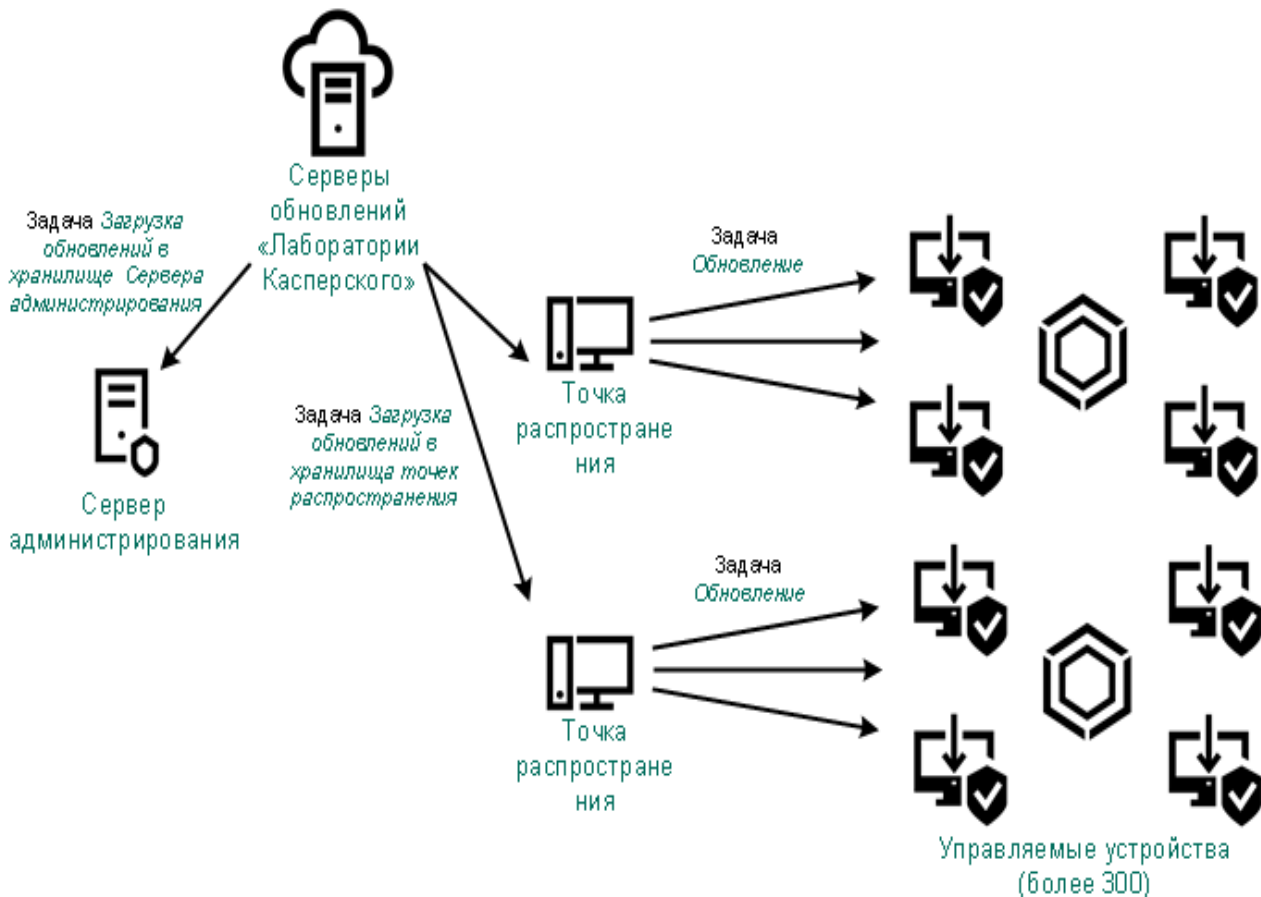
- идентификатор и версия приложения;
- идентификатор установки приложений;
- идентификатор активного ключа;
- идентификатор запуска задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

Использование двух задач: *Загрузка обновлений в хранилище Сервера администрирования* и *Загрузка обновлений в хранилища точек распространения*

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами

обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.



По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и/или точки распространения на использование протокола HTTP вместо HTTPS.

Для реализации этой схемы создайте задачу *Загрузка обновлений в хранилища точек распространения* в дополнение к задаче *Загрузка обновлений в хранилище Сервера администрирования*. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

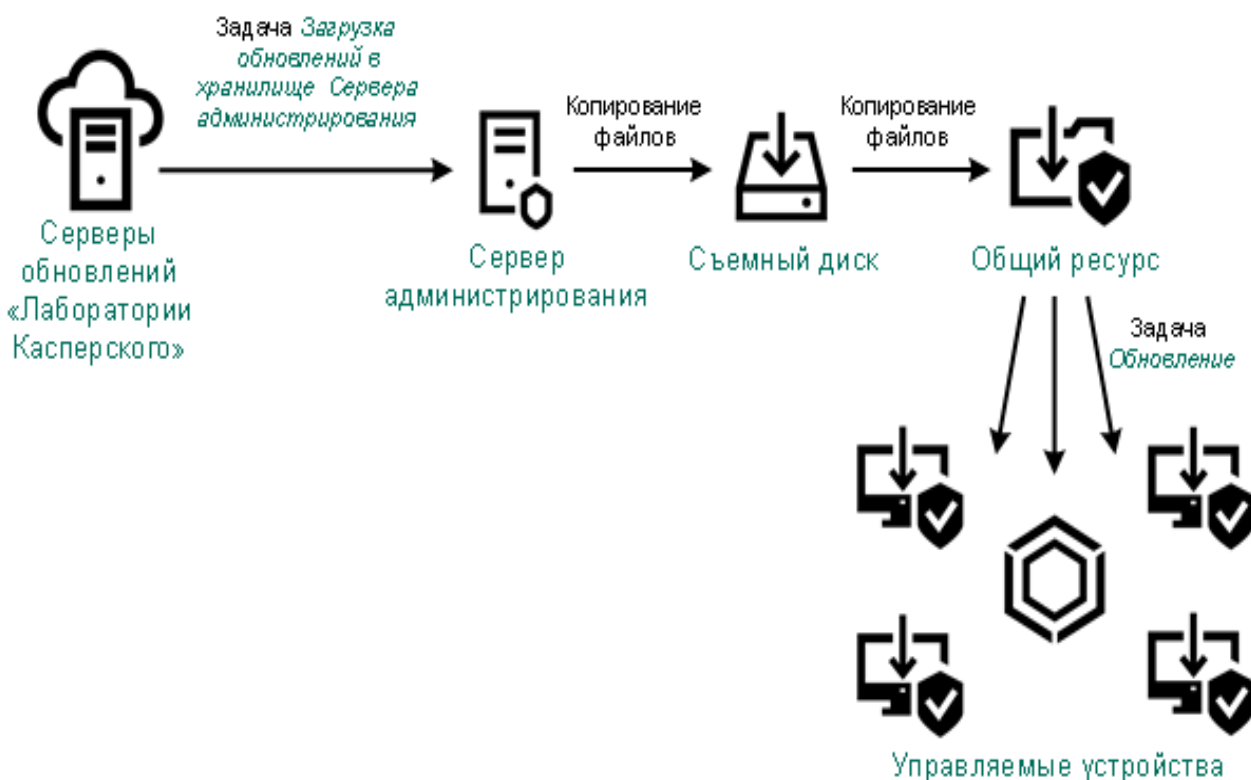
Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Для этой схемы также требуется задача *Загрузка обновлений в хранилище Сервера администрирования*, так как эта задача используется для загрузки баз и модулей приложений "Лаборатории Касперского" для Kaspersky Security Center.

Вручную через локальную папку, общую папку или FTP-сервер

Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать локальную папку или общий ресурс в качестве источника обновления баз, модулей приложений и приложений "Лаборатории Касперского". В этой схеме вам нужно скопировать необходимые обновления из хранилища Сервера администрирования на съемный диск, а затем скопировать обновления в локальную папку или общий ресурс, указанный в качестве источника обновлений в параметрах Kaspersky Endpoint Security (см. рисунок ниже).

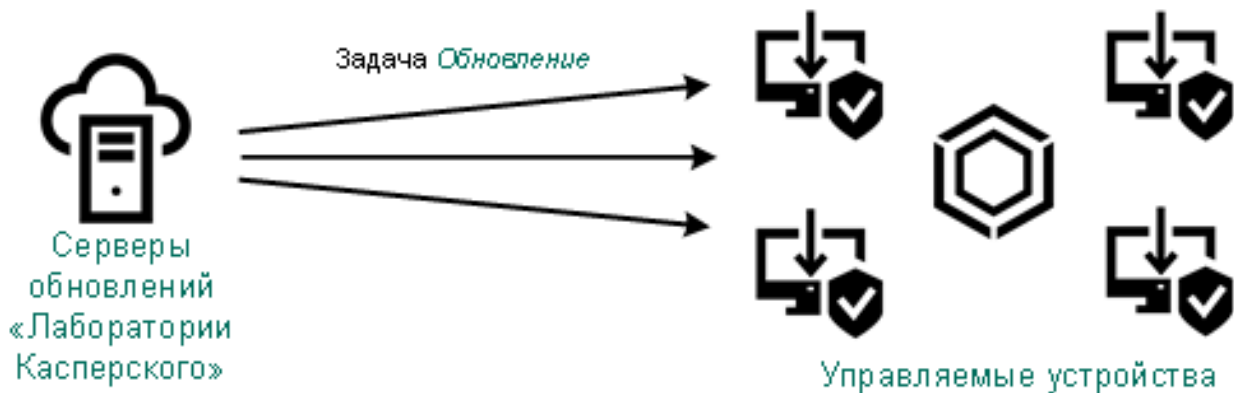


Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих справках:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



В этой схеме приложения безопасности не используют хранилища, предоставленные Kaspersky Security Center. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в интерфейсе приложения безопасности. Дополнительные сведения об этих параметрах см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

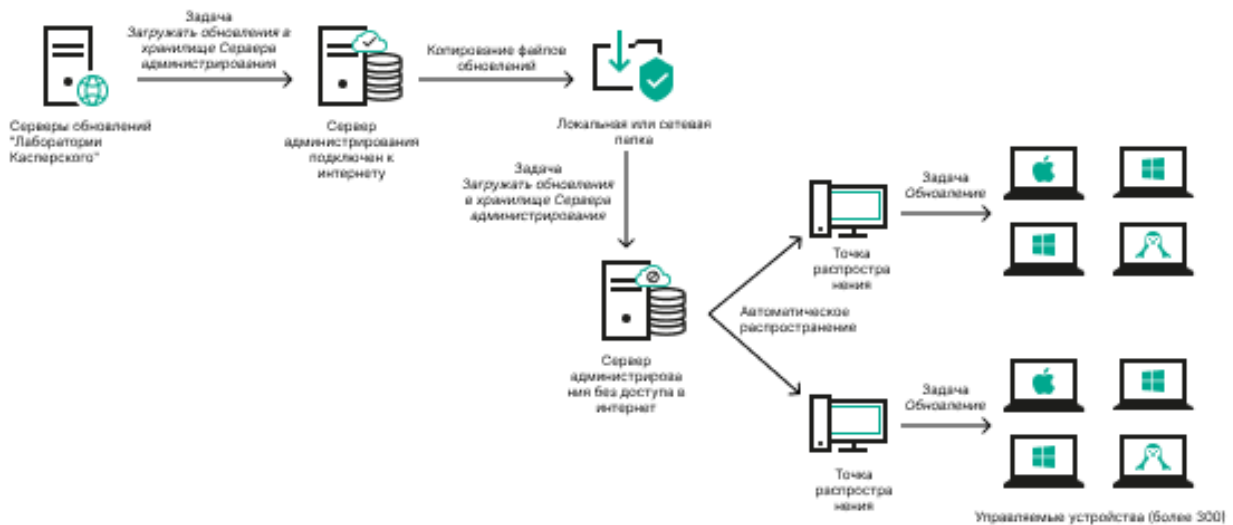
Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузка обновлений в хранилище Сервера администрирования* для загрузки обновлений из локальной или сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. Например, вы можете скопировать необходимые файлы обновления из одного из следующих источников:

- Сервер администрирования, имеющий выход в интернет (см. рис. ниже).

Так как Сервер администрирования загружает только те обновления, которые запрашиваются приложениями безопасности, наборы приложений безопасности, которыми управляют Серверы администрирования (подключенные и не подключенные к интернету) должны совпадать.

Если Сервер администрирования, который вы используете для загрузки обновлений, имеет версию 13.2 или более раннюю, откройте свойства задачи *Загрузка обновлений в хранилище Сервера*

администрирования, а затем включите параметр **Загружать обновления, используя старую схему**.



- Kaspersky Update Utility <https://support.kaspersky.com/updater4>

Так как утилита использует старую схему для загрузки обновлений, откройте свойства задачи **Загрузка обновлений в хранилище Сервера администрирования**, а затем включите параметр **Загружать обновления, используя старую схему**.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"

Когда Kaspersky Security Center загружает обновления с серверов обновлений "Лаборатории Касперского", он оптимизирует трафик с помощью файлов различий. Вы также можете включить использование файлов различий устройствами (Серверов администрирования, точек распространения и клиентских устройств), которые принимают обновления с других устройств в вашей сети.

О функции загрузки файлов различий

Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и модулей приложений. Если функция **Загрузить файлы различий** включена для Сервера администрирования или точки распространения, файлы различий сохраняются на этом Сервере администрирования или точке распространения. В результате устройства, которые получают обновления от этого Сервера администрирования или точки распространения, могут использовать сохраненные файлы различий для обновления своих баз и модулей приложений.

Для оптимизации использования файлов различий рекомендуется синхронизировать расписание обновления устройств с расписанием обновлений Сервера администрирования или точки распространения, с которых это устройство получает обновления. Однако трафик может быть сохранен, даже если

устройства обновляются в несколько раз реже, чем Сервер администрирования или точки распространения, с которых устройство получает обновления.

Функция загрузки файлов различий может быть включена только на Серверах администрирования и точках распространения версии 11 и выше. Чтобы сохранить файлы различий на Серверах администрирования и точках распространения предыдущих версий, их необходимо обновить до версии 11 или выше.

Функция загрузки файлов различий несовместима с офлайн-моделью получения обновлений (см. раздел "Офлайн-модель получения обновлений" на стр. 484). Это означает, что Агенты администрирования, использующие офлайн-модель загрузки обновлений, не загружают файлы различий, даже если функция загрузки файлов различий включена на Сервере администрирования или точке распространения, которые предоставляют обновления этим Агентам администрирования. Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Включение функции загрузки файлов различий[468](#)

Включение функции загрузки файлов различий

Предварительные требования

Необходимые предварительные условия для сценария:

- Сервер администрирования и точки распространения обновлены до версии 11 или выше.
- Офлайн модель получения обновлений выключена в свойствах политики Агента администрирования.

Этапы

а. Включение функции на Сервере администрирования

Включите функцию в свойствах задачи Загрузка обновлений в хранилище Сервера администрирования (см. раздел "Параметры задачи загрузки обновлений в хранилище Сервера администрирования" см. стр. [959](#)).

б. Включение функции для точки распространения

Включить функцию для точки распространения, которая получает обновления с помощью задачи Загрузка обновлений в хранилища точек распространения

Включите функцию для точки распространения, которая получает обновления с Сервера администрирования.

Эта функция включается в свойствах политики Агента администрирования (см. раздел "Параметры политики Агента администрирования" см. стр. [789](#)) и (если точки распространения назначены вручную и если вы хотите переопределить параметры политики) в свойствах Сервера

администрирования в разделе **Точки распространения** (см. раздел "**Загрузка обновлений точками распространения**" см. стр. [496](#)).

Чтобы проверить, что функция загрузки файлов различий успешно включена, вы можете измерить внутренний трафик до и после выполнения сценария.

См. также:

Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"	467
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455
Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"	460

Создание задачи для загрузки обновлений в хранилище Сервера администрирования

Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Задача *Загрузка обновлений в хранилище Сервера администрирования* может быть создана в одном экземпляре. Поэтому вы можете создать задачу *Загрузка обновлений в хранилище Сервера администрирования* только в случае, если она была удалена из списка задач Сервера администрирования.

► Чтобы создать задачу загрузки обновлений в хранилище Сервера администрирования:

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:
 - В контекстном меню **Задачи** в дереве консоли выберите пункт **Новый** → **Задачу**.
 - Нажмите на кнопку **Создать задачу** в рабочей области папки **Задачи**.
 Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне мастера **Выбор типа задачи** выберите **Загрузка обновлений в хранилище Сервера администрирования**.
4. В окне мастера **Параметры**, укажите следующие параметры задачи:
 - **Источники обновлений**
 - **Прочие параметры:**
 - **Принудительно обновить подчиненные Серверы**
 Если параметр включен, после получения обновлений Сервер администрирования будет запускать задачи получения обновлений подчиненными Серверами администрирования. В противном случае задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.
 По умолчанию параметр выключен.
 - **Копировать полученные обновления в дополнительные папки**

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

По умолчанию параметр выключен.

- **Не обновлять устройства и подчиненные Серверы администрирования принудительно до окончания копирования**

Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

1. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время

начала каждого запуска.

- **Каждые N минут**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрываемым списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрываемым списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрываемом списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемым списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемом списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** — только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

1. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?!\:|).
2. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера созданная задача **Загрузка обновлений в хранилище Сервера администрирования** появится в рабочей области списка задач Сервера администрирования.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и модулей приложений копируются с источника обновлений и размещаются в папке общего доступа. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Из папки общего доступа обновления распространяются на клиентские устройства и подчиненные Серверы администрирования.

См. также:

Проверка полученных обновлений	479
Параметры задачи загрузки обновлений в хранилище Сервера администрирования	959
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455

Создание задачи загрузки обновлений в хранилища точек распространения

Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

► Чтобы создать задачу загрузки обновлений в хранилища точек распространения для выбранной группы администрирования:

1. В дереве консоли выберите папку **Задачи**.
2. По кнопке **Новая задача** в рабочей области папки запустите мастер создания задачи.
Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне **Выбор типа задачи** мастера создания задачи выберите узел **Сервер администрирования Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Загрузка обновлений в хранилища точек распространения**.
4. В окне мастера **Параметры**, укажите следующие параметры задачи:
 - **Источники обновлений**

В качестве источника обновлений для точек распространения могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского"
HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.
По умолчанию этот вариант выбран.
- Главный Сервер администрирования
Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
- Локальная или сетевая папка
Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует проверки

подлинности, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

- **Папка для хранения обновлений**

Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

- **Загружать обновления, используя старую схему**

1. В окне мастера **Выберите группу администрирования** нажмите на кнопку **Обзор** и выберите группу администрирования, для которой задача будет применена.
2. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим

Ежедневно, под раскрывающимся списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение **Воскресенье**, а в поле **Время запуска** – **15:00:00**, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение **20**, а в поле **Время запуска** – **15:00:00**, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение **1**, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события **Вирусная атака**. Под раскрывающимся списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;

- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрывающимся списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрывающемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.
- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

1. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\":|).
2. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера созданная задача **Загрузка обновлений в хранилища точек распространения** появится в списке задач Агента администрирования в соответствующей группе администрирования и в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи *Загрузка обновлений в хранилища точек распространения* обновления баз и модулей приложений копируются с источника обновлений и размещаются в папке общего доступа. Загруженные обновления будут использоваться только теми точками распространения, которые входят в указанную группу администрирования и для которых нет явно заданной задачи получения обновлений.

В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Точки распространения**. В свойствах каждой точки распространения в разделе **Источник обновлений** можно указать источник обновлений (**Получать с Сервера администрирования** или **Использовать задачу принудительной загрузки обновлений**). Для точки распространения, назначенной вручную или автоматически, по умолчанию выбран вариант **Получать с Сервера администрирования**. Такие точки распространения будут использовать результаты задачи *Загрузка обновлений в хранилища точек распространения*.

В свойствах каждой точки распространения указана сетевая папка, настроенная индивидуально для этой точки распространения. Названия папок могут быть разными для разных точек распространения. Поэтому не рекомендуется изменять сетевую папку обновлений в свойствах задачи, если задача создается для группы устройств.

Вы можете изменить сетевую папку обновлений в свойствах задачи *Загрузка обновлений в хранилища точек распространения*, если вы создаете локальную задачу для устройства.

См. также:

- Параметры задачи загрузки обновлений в хранилища точек распространения[960](#)
- Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Настройка параметров задачи загрузки обновлений в хранилище Сервера администрирования

► Чтобы настроить параметры задачи загрузки обновлений в хранилище Сервера администрирования:

1. В рабочей области папки дерева консоли **Задачи** выберите задачу **Загрузка обновлений в хранилище Сервера администрирования** в списке задач.
2. Откройте окно свойств задачи одним из следующих способов:
 - В контекстном меню файла выберите пункт **Свойства**.
 - По ссылке **Настроить параметры задачи** в блоке работы с выбранной задачей.

Откроется окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*. В нем вы можете настроить параметры загрузки обновлений в хранилище Сервера администрирования.

См. также:

Параметры задачи загрузки обновлений в хранилище Сервера администрирования.....	959
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....	455

Проверка полученных обновлений

Перед установкой обновлений на управляемые устройства вы можете сначала проверить их на работоспособность и ошибки с помощью задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется автоматически в рамках задачи *Загрузка обновлений в хранилище Сервера администрирования*. Сервер администрирования загружает обновления с источника, сохраняет их во временном хранилище и запускает задачу *Проверка обновлений*. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования (<Папка установки Kaspersky Security Center>\Share\Updates). Обновления распространяются на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи *Проверка обновлений* размещенные во временном хранилище обновления признаны некорректными или задача *Проверка обновлений* завершается с ошибкой, копирование обновлений в папку общего доступа не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции выполняются при следующем запуске задачи *Загрузка обновлений в хранилище Сервера администрирования*, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты приложения безопасности;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования приложения "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача *Проверка обновлений* считается успешно выполненной.

Прежде чем приступить к созданию задачи *Проверка обновлений*, выполните предварительные условия:

1. Создайте группу администрирования (см. раздел "Создание групп администрирования" на стр. [743](#)) с несколькими тестовыми устройствами. Эта группа понадобится вам для проверки обновлений.

В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Такой подход повышает качество и вероятность обнаружения вирусов при проверке, а также минимизирует риск ложных срабатываний. При нахождении вирусов на тестовых устройствах задача *Проверка обновлений* считается завершившейся неудачно.

2. Создайте задачи *Обновление* и *Поиск вредоносного ПО* для приложения, поддерживаемого Kaspersky Security Center, например, Kaspersky Endpoint Security для Windows или Kaspersky Security для Windows Server. При создании задач *Обновление* и *Поиск вредоносного ПО* укажите группу администрирования с тестовыми устройствами.

Задача *Проверка обновлений* последовательно запускает задачи *Обновление* и *Поиск вредоносного ПО* на тестовых устройствах и так проверяет, что все обновления актуальны. Также при создании задачи *Проверка обновлений* необходимо указать задачи *Обновление* и *Поиск вредоносного ПО*.

3. Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования* (см. раздел "Создание задачи для загрузки обновлений в хранилище Сервера администрирования" на стр. [469](#)).

► Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские устройства:

1. В рабочей области папки **Задачи** дерева консоли выберите задачу *Загрузка обновлений в хранилище Сервера администрирования* в списке задач.
2. Откройте окно свойств задачи одним из следующих способов:
 - В контекстном меню файла выберите пункт **Свойства**.
 - По ссылке **Настроить параметры задачи** в блоке работы с выбранной задачей.
3. Если задача *Проверка обновлений* существует, нажмите на кнопку **Обзор**. В открывшемся окне выберите задачу *Проверка обновлений* в группе администрирования с тестовыми устройствами.
4. Если вы не создали задачу *Проверка обновлений* ранее, нажмите на кнопку **Создать**. Запустится мастер создания задачи *Проверка обновлений*. Следуйте далее указаниям мастера.
5. Закройте окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*, нажав на кнопку **ОК**.

Автоматическая проверка обновлений включена. Теперь вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования*, и она начнется с проверки обновлений.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского" [455](#)

Настройка проверочных политик и вспомогательных задач

При создании задачи *Проверка обновлений* (см. раздел "*Проверка полученных обновлений*" на стр. [479](#)) Сервер администрирования формирует проверочные политики, а также вспомогательные групповые задачи обновления и проверки по требованию.

На выполнение вспомогательных групповых задач обновления и проверки по требованию требуется некоторое время. Эти задачи выполняются в рамках выполнения задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется в рамках выполнения задачи *Загрузка обновлений в хранилище*. Время выполнения задачи *Загрузки обновлений в хранилище* включает в себя время выполнения вспомогательных групповых задач обновления и проверки по требованию.

Параметры проверочных политик и вспомогательных задач можно изменять.

► *Чтобы изменить параметры проверочной политики или вспомогательной задачи:*

1. В дереве консоли выберите группу, для которой сформирована задача *Проверка обновлений*.
2. В рабочей области группы выберите одну из следующих вкладок:
 - **Политики**, если вы хотите изменить параметры проверочной политики.
 - **Задачи**, если вы хотите изменить параметры вспомогательной задачи.
3. В рабочей области вкладки выберите политику или задачу, параметры которой вы хотите изменить.
4. Откройте окно свойств этой политики (задачи) одним из следующих способов:
 - В контекстном меню политики (задачи) выберите пункт **Свойства**.
 - По ссылке **Настроить параметры политики (Настроить параметры задачи)** в блоке работы с выбранной политикой (задачей).

Чтобы проверка обновлений выполнялась правильно, необходимо соблюдать следующие ограничения на изменение параметров проверочных политик и вспомогательных задач:

- В параметрах вспомогательных задач:
 - Сохранять на Сервере администрирования все события с уровнями важности **Критическое событие** и **Отказ функционирования**. На основе событий этих типов Сервер администрирования проводит анализ работы приложений.
 - Использовать в качестве источника обновлений Сервер администрирования.
 - Указывать тип расписания задач: **Вручную**.
- В параметрах проверочных политик:
 - Отключить технологии проверки iChecker и iSwift (**Базовая защита** → **Защита от файловых угроз** → **Параметры** → **Дополнительно** → **Технологии проверки**).
 - Выбрать действия над зараженными объектами: **Лечить; удалять, если лечение невозможно / Лечить; блокировать, если лечение невозможно / Блокировать**. (**Базовая защита** → **Защита от файловых угроз** → **Действие при обнаружении угрозы**).
- В параметрах проверочных политик и вспомогательных задач:

Если после установки обновлений модулей приложений потребуется перезагрузка устройства, ее следует выполнить незамедлительно. Если устройство не будет перезагружено, то проверить этот

тип обновлений будет невозможно. Для некоторых приложений установка обновлений, требующих перезагрузки, может быть запрещена или выполняться только после подтверждения от пользователя. Эти ограничения должны быть отключены в параметрах проверочных политик и вспомогательных задач.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Просмотр полученных обновлений

► Чтобы просмотреть список полученных обновлений,

В дереве консоли в папке **Хранилища** выберите вложенную папку **Обновления баз и модулей приложений "Лаборатории Касперского"**.

В рабочей области папки **Обновления баз и модулей приложений "Лаборатории Касперского"** представлен список обновлений, сохраненных на Сервере администрирования.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства

Вы можете настроить автоматическое обновление баз и модулей приложения Kaspersky Endpoint Security на клиентских устройствах.

► Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security на устройства:

1. В дереве консоли выберите папку **Задачи**.
2. Создайте задачу с типом **Обновление** одним из следующих способов:
 - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Новый** → **Задачу**.
 - В рабочей области папки **Новая задача** нажмите на кнопку **Задачи**.
 Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Обновление**.
4. Следуйте дальнейшим шагам мастера.
 В результате работы мастера создается задача обновления для Kaspersky Endpoint Security. Созданная задача отображается в списке задач в рабочей области папки **Задачи**.
5. В рабочей области папки **Задачи** выберите созданную задачу обновления.

6. В контекстном меню задачи выберите пункт **Свойства**.

7. В открывшемся окне свойств задачи в панели **Разделы** выберите раздел **Свойства**.

В разделе **Свойства** можно настроить параметры задачи обновления в локальном и мобильном режимах:

- **Параметры обновления в локальном режиме:** между устройством и Сервером администрирования установлена связь.
- **Обновите параметры для автономного режима:** между устройством и Kaspersky Security Center не установлена связь (например, если устройство не подключено к интернету).

8. По кнопке **Параметры** выберите источник обновлений.

9. Выберите параметр **Загружать обновления модулей приложения**, чтобы одновременно с базами приложения загружать и устанавливать обновления модулей приложения.

Если флажок установлен, то Kaspersky Endpoint Security уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления включает обновления модулей приложения в пакет обновлений. Настройте применение модулей обновлений:

- **Устанавливать критические и одобренные обновления.** При наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей приложения – после одобрения их установки администратором.
- **Устанавливать только утвержденные обновления.** При наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс приложения или с помощью Kaspersky Security Center.

Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то приложение устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.

10. Выберите параметр **Копировать обновления в папку**, чтобы приложение сохраняло загруженные обновления в папку, указанную по кнопке **Обзор**.

11. Нажмите на кнопку **ОК**.

При выполнении задачи **Обновление** приложение отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых приложений.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского" [455](#)

Офлайн-модель получения обновлений

Агент администрирования на управляемых устройствах не всегда может подключиться к Серверу администрирования для получения обновлений. Например, Агент администрирования может быть установлен на ноутбук, который иногда не подключен к интернету и локальной сети. Также администратор может ограничить время подключения устройств к сети. В таких случаях устройства с установленным Агентом администрирования не смогут получить обновления от Сервера администрирования в соответствии с расписанием. Если настроено обновление управляемых приложений (например, Kaspersky Endpoint Security) с помощью Агента администрирования, для обновления требуется соединение с Сервером администрирования. Когда соединение между Агентом администрирования и Сервером администрирования отсутствует, обновление невозможно. Соединение Агента администрирования с Сервером может быть настроено так, чтобы Агент подключался к Серверу только в определенные периоды времени. В худшем случае, если настроенные периоды подключения "пересекаются" с периодами, когда связь отсутствует, базы никогда не будут обновлены. Также возможны ситуации, когда много управляемых приложений одновременно обращаются к Серверу администрирования за обновлениями. В этом случае Сервер администрирования может перестать отвечать на запросы (как во время DDoS-атаки).

Во избежание описанных проблем в Kaspersky Security Center реализована офлайн-модель получения обновления баз и модулей управляемых приложений. Эта модель обеспечивает надежность механизма распространения обновлений вне зависимости от временных проблем недоступности каналов связи сервера администрирования, а также снижает нагрузку на Сервер администрирования. Эта модель также снижает нагрузку на Сервер администрирования.

Как работает офлайн-модель получения обновлений

Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые потребуются для управляемых приложений. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для приложений на устройстве.

Когда управляемое приложение на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемого приложения, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемому приложению обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для приложений на клиентских устройствах, но подключение не требуется для обновления.

Чтобы распределить нагрузку на Сервер администрирования, Агент администрирования на устройстве подключается к Серверу и загружает обновления случайным образом в течение интервала времени, определенного Сервером. Интервал времени зависит от количества устройств с установленным Агентом администрирования, которые загружают обновления, и от размера обновлений. Для снижения нагрузки на Сервер администрирования вы можете использовать Агент администрирования в качестве точки распространения.

Если офлайн-модель получения обновлений отключена, обновления распространяются в соответствии с расписанием задачи загрузки обновлений в хранилище.

По умолчанию офлайн-модель получения обновлений включена.

Офлайн-модель получения обновлений используется только для тех управляемых устройств, на которых задача получения обновлений управляемыми приложениями имеет расписание **При загрузке обновлений в хранилище**. Для остальных управляемых устройств используется традиционная система получения обновлений с Сервера администрирования в реальном времени.

Рекомендуется выключить офлайн-модель получения обновлений через настройки политик Агента администрирования соответствующих групп администрирования, если в управляемых приложениях настроено получение обновлений не с Сервера администрирования, а с серверов "Лаборатории Касперского" либо из сетевой папки и при этом задача получения обновлений имеет расписание **При загрузке обновлений в хранилище**.

См. также:

Включение и выключение офлайн-модели получения обновлений	485
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455

Включение и выключение офлайн-модели получения обновлений

Не рекомендуется выключать офлайн-модель получения обновлений. Выключение может привести к сбоям в доставке обновлений на устройства. В некоторых случаях специалисты Службы технической поддержки "Лаборатории Касперского" могут рекомендовать вам снять флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее**. Тогда вам нужно будет убедиться, что задача загрузки обновлений в хранилище для приложений "Лаборатории Касперского" настроена.

► Чтобы включить или выключить офлайн-модель получения обновлений для группы администрирования:

1. В дереве консоли выберите группу администрирования, для которой требуется включить офлайн-модель получения обновлений.
2. В рабочей области группы откройте вкладку **Политики**.
3. На вкладке **Политики** выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.
Откроется окно свойств политики Агента администрирования.
5. В окне свойств политики выберите раздел **Управление патчами и обновлениями**.
6. Установите или снимите флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**, чтобы включить или выключить офлайн-модель получения обновлений соответственно.

По умолчанию офлайн-модель получения обновлений включена.

В результате офлайн-модель получения обновлений будет включена или выключена.

См. также:

Офлайн-модель получения обновлений	484
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center

По умолчанию автоматически устанавливаются загруженные обновления и патчи для следующих компонентов приложения:

- Агент администрирования для Windows
- Консоль администрирования.
- Сервер iOS MDM

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center доступна только для устройств под управлением Windows. Вы можете выключить автоматическую установку обновлений и патчей для этих компонентов. В этом случае загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобрено*. Обновления и патчи со статусом *Не определено* не будут установлены.

См. также:

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center	487
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center

Автоматическая установка обновлений для компонентов Kaspersky Security Center включена по умолчанию при установке Агента администрирования на устройство. Вы можете выключить ее при установке Агента администрирования или же выключить позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center при локальной установке Агента администрирования на устройство:*

1. Запустите локальную установку Агента администрирования на устройство (см. раздел "Локальная установка Агента администрирования" на стр. [193](#)).
2. На шаге **Дополнительные параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**.
3. Следуйте далее указаниям мастера.

На устройстве будет установлен Агент администрирования с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

- *Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center при установке Агента администрирования на устройство с помощью инсталляционного пакета:*

1. В дереве консоли выберите папку **Удаленная установка** → **Инсталляционные пакеты**.
2. В контекстном меню пакета **Агент администрирования Kaspersky Security Center <номер версии>** выберите пункт **Свойства**.
3. В свойствах инсталляционного пакета, в разделе **Параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**.

Агент администрирования будет устанавливаться из этого пакета с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

Если при установке Агента администрирования на устройство флажок был установлен (снят), впоследствии вы можете выключить (включить) автоматическую установку с помощью политики Агента администрирования.

- *Чтобы включить или выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center с помощью политики Агента администрирования:*

1. В дереве консоли выберите группу администрирования, для которой требуется включить или выключить автоматическую установку обновлений и патчей.
2. В рабочей области группы откройте вкладку **Политики**.
3. На вкладке **Политики** выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.
Откроется окно свойств политики Агента администрирования.
5. В окне свойств политики выберите раздел **Управление патчами и обновлениями**.
6. Установите или снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**, чтобы включить или выключить автоматическую установку обновлений и патчей.
7. Установите замок при этом флажке.

Политика применится к выбранным устройствам, и автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center будет включена (выключена) на этих устройствах.

См. также:

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center	487
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455

Автоматическое распространение обновлений

Kaspersky Security Center позволяет автоматически распространять и устанавливать обновления на клиентские устройства и подчиненные Серверы администрирования.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

В этом разделе

Автоматическое распространение обновлений на клиентские устройства[489](#)

Автоматическое распространение обновлений на подчиненные Серверы администрирования[490](#)

Автоматическое назначение точек распространения[490](#)

Назначение устройства точкой распространения вручную[491](#)

Удаление устройства из списка точек распространения[495](#)

Загрузка обновлений точками распространения[496](#)

Автоматическое распространение обновлений на клиентские устройства

- Чтобы обновления выбранного вами приложения автоматически распространялись на клиентские устройства сразу после загрузки обновлений в хранилище Сервера администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся клиентские устройства.
2. Создайте задачу распространения обновлений этого приложения для выбранных клиентских устройств одним из следующих способов:
 - Если требуется распространять обновления на клиентские устройства, входящие в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание задачи" на стр. [416](#)).
 - Если требуется распространять обновления на клиентские устройства, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. [418](#)).

Запустится мастер создания задачи. Следуйте его указаниям, выполнив следующие условия:

- a. В окне мастера **Тип задачи** в узле нужного вам приложения выберите задачу распространения обновлений.

Название задачи распространения обновлений, которое отображается в окне **Тип задачи**, зависит от приложения, для которого создается задача. Подробнее о названиях задач обновления для выбранных приложений "Лаборатории Касперского" см. в руководствах к этим приложениям.

- b. В окне мастера **Расписание** в поле **Запуск по расписанию** выберите вариант запуска **При загрузке обновлений в хранилище**.

В результате созданная задача распространения обновлений будет запускаться для выбранных устройств каждый раз при загрузке обновлений в хранилище Сервера администрирования.

Если задача распространения обновлений нужного вам приложения уже создана для выбранных устройств, для автоматического распространения обновлений на клиентские устройства в окне свойств задачи в разделе **Расписание** нужно выбрать вариант запуска **При загрузке обновлений в хранилище** в поле **Запуск по расписанию**.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Автоматическое распространение обновлений на подчиненные Серверы администрирования

► Чтобы обновления выбранного вами приложения автоматически распространялись на подчиненные Серверы администрирования сразу после загрузки обновлений в хранилище главного Сервера администрирования:

1. В дереве консоли в узле главного Сервера администрирования выберите папку **Задачи**.
2. В списке задач в рабочей области выберите задачу загрузки обновлений в хранилище Сервера администрирования.
3. Откройте раздел **Параметры** окна свойств выбранной задачи одним из следующих способов:
 - В контекстном меню файла выберите пункт **Свойства**.
 - По ссылке **Изменить параметры** в блоке работы с выбранной задачей.
4. В разделе **Параметры** окна свойств задачи откройте окно **Прочие параметры** по ссылке **Настроить** в подразделе Прочие параметры.
5. В открывшемся окне **Прочие параметры** установите флажок **Принудительно обновить подчиненные Серверы**.

В параметрах задачи получения обновлений Сервером администрирования на вкладке **Параметры** окна свойств задачи установите флажок **Принудительно обновить подчиненные Серверы**.

В результате сразу после получения обновлений главным Сервером администрирования будут автоматически запускаться задачи загрузки обновлений подчиненными Серверами администрирования, независимо от расписания, установленного в параметрах этих задач.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения.

► Чтобы назначить точки распространения автоматически:

1. Откройте главное окно приложения.

2. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется автоматически назначать точки распространения.
3. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
4. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Точки распространения**.
5. В правой части окна выберите параметр **Автоматически назначать точки распространения**.

Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

6. Нажмите на кнопку **ОК**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Назначение устройства точкой распространения вручную

Kaspersky Security Center позволяет назначать устройства точками распространения.

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения. Однако если вы по какой-то причине хотите отказаться от автоматического назначения точек распространения (например, если вы хотите использовать специально выделенные серверы), вы можете назначать точки распространения вручную, предварительно рассчитав их количество и конфигурацию (см. раздел "Расчет количества и конфигурации точек распространения" на стр. [149](#)).

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

► Чтобы вручную назначить устройство точкой распространения:

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** нажмите на кнопку **Добавить**. Кнопка доступна, если выбран вариант **Вручную назначать точки распространения**.
Откроется окно **Добавление точки распространения**.
4. В окне **Добавление точки распространения** выполните следующие действия:
 - а. Выберите устройство, которое будет выполнять роль точки распространения (в группе администрирования или укажите IP-адрес устройства). При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения (см. раздел "Точка распространения" на стр. [51](#)).

- b. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.

5. Нажмите на кнопку **ОК**.

Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

6. Выберите в списке добавленную точку распространения и по кнопке **Свойства** откройте окно ее свойств.
7. В окне свойств настройте параметры точки распространения:
- В разделе **Общие** укажите параметры взаимодействия точки распространения с клиентскими устройствами.
 - **SSL-порт**

Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к агенту обновлений с использованием протокола SSL.

По умолчанию номер порта – 13000.
 - **Использовать многоадресную IP-рассылку**

Если флажок установлен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.
 - **Адрес IP-рассылки**

IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

По умолчанию указан IP-адрес 225.6.7.8.
 - **Номер порта IP-рассылки**

Номер порта многоадресной рассылки.

Номер порта по умолчанию – 15001. Если в качестве агента обновлений указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.
 - **Распространять обновления**

Если флажок установлен, обновления распространяются на клиентские устройства с помощью этого агента обновлений.

По умолчанию флажок установлен.
 - **Распространять инсталляционные пакеты**

Если флажок установлен, инсталляционные пакеты обновления распространяются на клиентские устройства с помощью этого агента обновлений.

По умолчанию флажок установлен.
 - Использовать точку распространения в качестве извещающего сервера
 - Порт push-сервера
 - В разделе **Область действия** укажите область, на которую точка распространения распространяет обновления (группы администрирования и/или сетевое местоположение).

- В разделе **Прокси-сервер KSN** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.
- **Включить прокси-сервер KSN на стороне точки распространения**

Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены (см. раздел "Настройка доступа к KPSN" на стр. [874](#)) в окне свойств Сервера администрирования.

Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.
- **Переслать KSN запрос Серверу администрирования**

Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

По умолчанию параметр включен.
- **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к KPSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения.

Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к KPSN.
- **Игнорировать параметры прокси-сервера для подключения к KPSN**

Установите этот флажок, если параметры прокси-сервера настроены в свойствах точки распространения или политики Агента администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

Это параметр доступен, если вы выбрали параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.
- **TCP-порт**

Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.
- **UDP-порт**

Чтобы управляемое устройство подключалось к прокси-серверу KSN через UDP-

порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **HTTPS-порт**

Если вам нужно, чтобы управляемые устройства подключались к прокси-серверу KSN через порт HTTPS, включите параметр **Использовать HTTPS** и укажите номер порта в поле **Через HTTPS-порт**. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

- В разделе **Обнаружение устройств** настройте опрос доменов Windows, Active Directory и IP-диапазонов точкой распространения.

- **Windows-домены**

Вы можете включить обнаружение устройств для Windows-доменов и задать его расписание.

- **Active Directory**

Вы можете включить опрос Active Directory и задать расписание опроса.

Если вы используете точку распространения с операционной системой Windows, можно выбрать один из следующих вариантов:

- **Опросить текущий домен Active Directory.**
- **Опросить лес доменов Active Directory.**
- **Опросить указанные домены Active Directory.** Если вы выбрали этот вариант, добавьте один или несколько доменов Active Directory в список.

Если вы используете точку распространения с операционной системой Linux с установленным Агентом администрирования версии 15, вы можете опрашивать только те домены Active Directory, для которых вы указываете адрес и учетные данные пользователя. Опрос текущего домена Active Directory и леса доменов Active Directory недоступен.

- **IP-диапазоны**

Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов (см. раздел "Добавление IP-диапазонов в список диапазонов, опрашиваемых точкой распространения" на стр. [696](#)).

Если включить параметр **Использовать Zeroconf для опроса IPv6-сетей**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией <http://www.zeroconf.org/> (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вам нужно установить утилиту avahi-browse на точке распространения.

- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных.

- **Использовать папку по умолчанию**

При выборе этого варианта для сохранения данных будет использоваться папка, в которую на агенте обновлений установлен Агент администрирования.

- **Использовать указанную папку**

При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на агенте обновлений, так и удаленно, на любом из устройств, входящих в состав сети организации.

Учетная запись, под которой на агенте обновлений запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

В результате выбранные устройства будут выполнять роль точек распространения.

Только устройства под управлением операционной системы Windows могут определять свое сетевое местоположение. Определение сетевого местоположения недоступно для устройств под управлением других операционных систем.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Удаление устройства из списка точек распространения

► *Чтобы удалить устройство из списка точек распространения:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** выберите устройство, выполняющее функции точки распространения, и нажмите на кнопку **Удалить**.

В результате устройство будет удалено из списка точек распространения и перестанет выполнять функции точки распространения.

Невозможно удалить устройство из списка точек распространения, если оно было назначено Сервером администрирования автоматически (см. раздел "Назначение устройства точкой распространения вручную" на стр. [491](#)).

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Загрузка обновлений точками распространения

Kaspersky Security Center позволяет точкам распространения получать обновления от Сервера администрирования, серверов "Лаборатории Касперского", из локальной или сетевой папки.

► *Чтобы настроить получение обновлений для точки распространения, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** выберите точку распространения, через которую обновления будут доставляться на клиентские устройства группы.
4. По кнопке **Свойства** откройте окно свойств выбранной точки распространения.
5. В окне свойств точки распространения выберите раздел **Источники обновлений**.
6. Выберите источник обновлений для точки распространения:
 - Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получать с Сервера администрирования**:
 - **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий (см. раздел "Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"" см. стр. [467](#)).

По умолчанию параметр включен.

- Чтобы точка распространения получала обновления с помощью задачи, выберите вариант **Использовать задачу принудительной загрузки обновлений**:
 - Нажмите на кнопку **Выбрать**, если такая задача уже есть на устройстве, и выберите задачу в появившемся списке.
 - Нажмите на кнопку **Новая задача**, чтобы создать задачу, если такой задачи еще нет на устройстве. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Задача загрузки обновлений в хранилища точек распространения является локальной. Для каждого устройства, выполняющего роль точки распространения, задачу требуется создавать отдельно.

В результате точка распространения будет получать обновления из указанного источника.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского" [455](#)

Удаление обновлений программного обеспечения из хранилища

► Чтобы удалить обновления программного обеспечения из хранилища Сервера администрирования:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области папки **Обновления программного обеспечения** выберите обновление, которое нужно удалить.
3. В контекстном меню обновления выберите **Удалить файлы обновлений**.

Обновления программного обеспечения будут удалены из хранилища Сервера администрирования.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Установка патча для приложения "Лаборатории Касперского" в кластерной модели

Kaspersky Security Center поддерживает только ручную установку патчей для приложений "Лаборатории Касперского" в кластерной модели.

► Чтобы установить патч для приложения "Лаборатории Касперского":

1. Загрузите на каждый узел кластера патч.
2. Запустите установку патча на активном узле.
3. Дождитесь успешной установки патча.
4. Последовательно запустите патч на всех подчиненных узлах кластера.

При запуске патча из командной строки используйте ключ `"-CLUSTER_SECONDARY_NODE"`.

В результате этих действий патч будет установлен на каждом узле кластера.

5. Запустите вручную кластерные службы "Лаборатории Касперского".

Каждый узел кластера будет отображаться в Консоли администрирования как устройство с установленным Агентом администрирования.

Информацию об установленных патчах можно просмотреть в папке **Обновления программного обеспечения** или в отчете о версиях обновлений модулей приложений "Лаборатории Касперского".

См. также:

Настройка общих параметров Сервера администрирования[716](#)

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Управление приложениями сторонних производителей на клиентских устройствах

Kaspersky Security Center позволяет управлять приложениями "Лаборатории Касперского" и других производителей, установленными на клиентских устройствах.

Администратор может выполнять следующие действия:

- создавать категории приложений на основании заданных критериев;
- управлять категориями приложений с помощью специально созданных правил;
- управлять запуском приложений на устройствах;
- выполнять инвентаризацию и вести реестр программного обеспечения, установленного на устройствах;
- закрывать уязвимости программного обеспечения, установленного на устройствах;
- устанавливать обновления Windows Update и других производителей программного обеспечения на устройствах;
- отслеживать использование лицензионных ключей для групп лицензионных приложений.

В этом разделе

Установка обновлений приложений сторонних производителей	498
Уязвимости в приложениях	528
Группы приложений	571

Установка обновлений приложений сторонних производителей

Kaspersky Security Center позволяет управлять обновлениями программного обеспечения, установленного на клиентских устройствах, и закрывать уязвимости в приложениях Microsoft и других производителей программного обеспечения с помощью установки необходимых обновлений.

Kaspersky Security Center выполняет поиск обновлений с помощью задачи поиска обновлений и загружает обновления в хранилище обновлений. После завершения поиска обновлений приложение предоставляет администратору информацию о доступных обновлениях и об уязвимостях в приложениях, которые можно закрыть с помощью этих обновлений.

Информация о доступных обновлениях Microsoft Windows передается из центра обновлений Windows. Сервер администрирования может использоваться в роли сервера Windows Update (WSUS). Для использования Сервера администрирования в роли сервера Windows Update необходимо настроить синхронизацию обновлений с центром обновлений Windows. После настройки синхронизации данных с центром обновлений Windows Сервер администрирования с заданной периодичностью централизованно предоставляет обновления службам Windows Update на устройствах.

Управлять обновлениями программного обеспечения можно также с помощью политики Агента администрирования. Для этого необходимо создать политику Агента администрирования и настроить параметры обновлений программного обеспечения в соответствующих окнах мастера создания политики.

Администратор может просматривать список доступных обновлений в папке **Обновления программного обеспечения**, входящей в состав папки **Управление приложениями**. Эта папка содержит список

полученных Сервером администрирования обновлений приложений Microsoft и других производителей программного обеспечения, которые могут быть распространены на устройства. После просмотра информации о доступных обновлениях администратор может выполнить установку обновлений на устройства.

Обновление некоторых приложений Kaspersky Security Center выполняется путем удаления предыдущей версии приложения и установки новой версии приложения.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Убедитесь, что параметры **Отображать Системное администрирование** включены в окне **Настройка интерфейса** (см. раздел "**Настройка интерфейса**" на стр. 320) для главного и подчиненного Сервера администрирования. Иначе задача поиска обновлений обрабатывает только обновления WSUS.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Специалисты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также специалисты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Перед установкой обновлений на все устройства можно выполнить проверочную установку, чтобы убедиться, что установленные обновления не вызовут сбоев в работе приложений на устройствах.

Вы можете получить сведения о программном обеспечении сторонних производителей, которое можно обновлять с помощью Kaspersky Security Center на веб-сайте Службы технической поддержки на странице Kaspersky Security Center, в разделе Управление Сервером (<http://support.kaspersky.ru/9327>).

В этом разделе

Сценарий: обновление приложений сторонних производителей	499
Просмотр информации о доступных обновлениях для приложений сторонних производителей	503
Одобрение и отклонение обновлений программного обеспечения	505
Синхронизация обновлений Windows Update с Сервером администрирования	506
Установка обновлений на устройства вручную	513
Настройка обновлений Windows в политике Агента администрирования	526

Сценарий: обновление приложений сторонних производителей

В этом разделе представлен сценарий обновления приложений сторонних производителей, установленных на клиентских устройствах. Приложения сторонних производителей включают в себя приложения от

Microsoft и других поставщиков программного обеспечения. Обновления для приложений Microsoft предоставляются службой Центра обновления Windows.

Предварительные требования

Сервер администрирования должен иметь подключение к интернету для установки обновлений приложений сторонних производителей, отличных от приложений Microsoft.

По умолчанию Сервер администрирования не требует подключения к интернету для установки обновлений приложений Microsoft на управляемые устройства. Например, управляемые устройства могут загружать обновления приложений Microsoft непосредственно с серверов обновлений Microsoft или с Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации. Если вы используете Сервер администрирования в качестве сервера WSUS, Сервер администрирования должен быть подключен к интернету.

Этапы

Обновление производителей состоит из следующих этапов:

а. Поиск требуемых обновлений

Чтобы найти обновления приложений сторонних производителей, необходимые для управляемых устройств, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky Security Center Сервера администрирования. Если вы не запустили мастер, создайте задачу или запустите мастер первоначальной настройки.

Инструкции:

- Консоль администрирования: Поиск уязвимостей в приложениях (на стр. [535](#)), Задание расписания для задачи поиска уязвимостей и требуемых обновлений (см. раздел "Настройка расписания задачи Поиск уязвимостей и требуемых обновлений." на стр. [412](#)).
- Kaspersky Security Center Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений, Параметры задачи поиска уязвимостей и требуемых обновлений.

б. Анализ списка найденных обновлений

Просмотрите список **Обновления программного обеспечения** и решите, какие обновления следует установить. Чтобы просмотреть подробную информацию о каждом обновлении, нажмите на имя обновления в списке. Для каждого обновления в списке также можно просмотреть статистику установки обновлений на клиентских устройствах.

Инструкции:

- Консоль администрирования: Просмотр информации о доступных обновлениях (см. раздел "Просмотр информации о доступных обновлениях для приложений сторонних производителей" см. стр. [503](#)).
- Kaspersky Security Center Web Console: Просмотр информации о доступных обновлениях приложений сторонних производителей.

с. Настройка установки обновлений

После того как Kaspersky Security Center получает список обновлений приложений сторонних производителей, вы можете установить их на клиентские устройства, используя задачу *Установка требуемых обновлений и закрытия уязвимостей* или задачу *Установка обновлений Центра*

обновления Windows. Создайте одну из этих задач. Вы можете создать эти задачи на вкладке **Задачи** или с помощью списка **Обновления программного обеспечения**.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для установки обновлений для приложений Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления приложений других поставщиков. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование.

Задача *Установка обновлений Центра обновления Windows* не требует лицензии, но ее можно использовать только для установки обновлений Центра обновления Windows.

Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

Вы можете запустить задачу установки обновления по расписанию. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Инструкции:

- Консоль администрирования: Закрытие уязвимостей в приложениях (на стр. [541](#)), Просмотр информации о доступных обновлениях (см. раздел "Просмотр информации о доступных обновлениях для приложений сторонних производителей" см. стр. [503](#)).
- Kaspersky Security Center Web Console: Создание задачи Установка требуемых обновлений и закрытие уязвимостей, Создание задачи Установка обновлений Центра обновления Windows, Просмотр информации о доступных обновлениях приложений сторонних производителей.

d. Задание расписания задачи

Чтобы убедиться, что список обновлений всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. По умолчанию задача *Поиск уязвимостей и требуемых обновлений* запускается в 18:00:00 вручную.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. При планировании задачи *Установка обновлений Центра обновления Windows* обратите внимание, что для этой задачи вам нужно определять список обновлений каждый раз перед запуском этой задачи.

При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

e. Одобрение и отклонение обновлений программного обеспечения (если требуется)

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете указать правила установки обновлений в свойствах задачи. Если вы создали задачу *Установка обновлений Центра обновления Windows*, пропустите этот шаг.

Для каждого правила вы можете выбрать устанавливаемые обновления в зависимости от их статуса: *Не определено*, *Одобрено* или *Отклонено*. Например, вы можете создать определенную задачу для серверов и установить правило для этой задачи, чтобы разрешить установку только обновлений Центра обновления Windows и только тех, которые имеют статус *Одобрено*. После этого вы вручную устанавливаете статус *Одобрено* для тех обновлений, которые вы хотите установить. В этом случае обновления Центра обновления Windows со статусом *Не определено* или *Отклонено* не будут установлены на серверы, указанные в задаче.

При управлении установкой обновлений использовать статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие*

уязвимостей. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. При ручном одобрении большого количества обновлений производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус на *Одобрено* или *Отклонено* в списке **Обновления программного обеспечения (Операции → Управление патчами → Обновления программного обеспечения)**.

Инструкции:

- Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения (на стр. [505](#)).
- Kaspersky Security Center Web Console: Одобрение и отклонение обновлений приложений сторонних производителей.

f. Настройка Сервера администрирования для работы в качестве службы Windows Server Update Services (WSUS) (если требуется)

По умолчанию обновления Центра обновления Windows загружаются на управляемые устройства с серверов Microsoft. Вы можете изменить этот параметр, чтобы использовать Сервер администрирования в роли WSUS-сервера. В этом случае Сервер администрирования синхронизирует данные обновления с Центром обновления Windows с заданной периодичностью и предоставляет обновления централизованно службам Центра обновления Windows на сетевых устройствах.

Чтобы использовать Сервер администрирования в качестве сервера WSUS, создайте задачу Синхронизация обновлений Windows Update и установите флажок **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования.

Инструкции:

- Консоль администрирования: Синхронизация обновлений Windows Update с Сервером администрирования (на стр. [506](#)), Настройка обновлений Windows в политике Агента администрирования (на стр. [526](#)).
- Kaspersky Security Center Web Console: Создание задачи Синхронизация обновлений Windows Update.

g. Запуск задачи установки обновлений

Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. После запуска этих задач, обновления загружаются и устанавливаются на управляемые устройства. После завершения задачи убедитесь, что в списке задач она имеет статус *Завершена успешно*.

h. Создание отчета о результатах установки обновлений приложений сторонних производителей (если требуется)

Чтобы просмотреть статистику установки обновления, сформируйте **Отчет о результатах установки обновлений стороннего ПО**.

Инструкции:

- Консоль администрирования: Создание и просмотр отчета (на стр. [607](#)).
- Kaspersky Security Center Web Console: Генерация и просмотр отчета.

Результаты

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытия уязвимостей*, обновления будут автоматически установлены на управляемые устройства. При загрузке новых обновлений

в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли они критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут установлены автоматически при следующем запуске задачи.

Если вы создали задачу *Установка обновлений Центра обновления Windows*, будут установлены только те обновления, которые указаны в свойствах задачи *Установка обновлений Центра обновления Windows*. Позже, если вы захотите установить новые обновления, загруженные в хранилище Сервера администрирования, вам будет необходимо добавить требуемые обновления в список обновлений существующей задачи или создать задачу *Установка обновлений Центра обновления Windows*.

См. также

Просмотр информации о доступных обновлениях для приложений сторонних производителей	503
Одобрение и отклонение обновлений программного обеспечения	505
Синхронизация обновлений Windows Update с Сервером администрирования	506
Установка обновлений на устройства вручную.....	513
Настройка обновлений Windows в политике Агента администрирования	526

Просмотр информации о доступных обновлениях для приложений сторонних производителей

- *Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на клиентских устройствах,*

В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.

В рабочей области папки вы можете просматривать список имеющихся обновлений для приложений, установленных на устройствах.

- *Чтобы просмотреть свойства обновления,*

в рабочей области папки **Обновления программного обеспечения** в контекстном меню обновления выберите пункт **Свойства**.

В окне свойств обновления для просмотра доступна следующая информация:

- В разделе **Общие** вы можете просмотреть **Статус одобрения обновления**:
 - **Не определено** – обновление доступно в списке обновлений, но не одобрено для установки.
 - **Одобрено** – обновление доступно в списке обновлений и одобрено к установке.
 - **Отклонено** – обновление отклонено для установки.
- В разделе **Атрибуты** вы можете просмотреть значения поля **Устанавливаемый автоматически**:
 - Значение **Автоматически** отображается, если задача *Установка требуемых обновлений и закрытие уязвимостей* может устанавливать обновления для приложения. Задача автоматически устанавливает новые обновления с веб-адреса, предоставленного поставщиком приложений сторонних производителей.

- Значение **Вручную** отображается, если Kaspersky Security Center не может установить обновления для приложения автоматически. Вы можете установить обновления вручную.

Поле **Устанавливаемый автоматически** не отображается для обновлений приложений Windows.

- Список клиентских устройств, для которых применимо обновление.
- Список системных компонентов (предварительных требований), которые должны быть установлены перед обновлением (любым).
- Уязвимости в приложениях, которые закрывают это обновление.

См. также:

Сценарий: обновление приложений сторонних производителей	499

Одобрение и отклонение обновлений программного обеспечения

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

Для управления установкой обновлений приложений сторонних производителей использование статуса **Одобрено** целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений приложений сторонних производителей, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус **Одобрено** только для тех обновлений, которые не соответствуют критериям, указанным в правилах. При ручном одобрении большого количества обновлений производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

► *Чтобы подтвердить или отменить одно или несколько обновлений:*

1. В дереве консоли выберите узел **Дополнительно** → **Управление приложениями** → **Обновления программного обеспечения**.
2. В рабочей области папки **Обновления программного обеспечения** перейдите по ссылке **Обновить** вверху справа и дождитесь загрузки списка обновлений. Отобразится список обновлений.
3. Выберите обновления, которые требуется подтвердить или отклонить.
Блок работы с выбранным объектом отображается в правой части рабочей области.
4. В раскрывающемся списке **Статус одобрения обновления** выберите **Одобрено**, чтобы подтвердить выбранные обновления, или **Отклонено**, чтобы отменить выбранные обновления.

По умолчанию указано значение **Не определено**.

Обновления, для которых установлен статус **Одобрено**, помещаются в очередь на установку.

Обновления, для которых установлен статус **Отклонено**, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для приложений "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус **Отклонено**, Kaspersky Security Center не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем. Если обновления для приложений "Лаборатории Касперского" не могут быть удалены, это свойство отображается в окне свойств обновления. В панели **Разделы** выберите **Общие**, и свойство отобразится в разделе **Требования к установке** рабочей области. Если вы устанавливаете статус **Отклонено** для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить их, вы можете сделать это вручную локально.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....	455
Сценарий: обновление приложений сторонних производителей	499

Синхронизация обновлений Windows Update с Сервером администрирования

Если в окне **Параметры управления обновлениями** мастера первоначальной настройки вы выбрали вариант **Использовать Сервер администрирования в роли WSUS-сервера**, задача синхронизации с Центром обновления Windows создается автоматически. Запустить задачу можно в папке **Задачи**. Функция обновления программного обеспечения Microsoft доступна только после успешного завершения задачи **Синхронизация обновлений Windows Update**.

Обновления программного обеспечения Microsoft могут превышать 10 ГБ. Убедитесь, что база данных Сервера администрирования способна вместить такие тома, иначе задача **Синхронизация обновлений Windows Update** не будет выполнена. База данных Microsoft SQL Express не поддерживается для задачи **Синхронизация обновлений Windows Update**.

Задача **Синхронизация обновлений Windows Update** загружает с серверов Microsoft только метаданные. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

► Чтобы создать задачу синхронизации обновлений Windows Update с Сервером администрирования:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите значение **Настроить синхронизацию обновлений Windows Update**.

В мастере создается задача **Синхронизация обновлений Windows Update**, отображаемая в папке **Задачи**.

Запустится мастер создания задачи получения данных из центра обновлений Windows. Следуйте далее указаниям мастера.

Задачу синхронизации обновлений Windows Update также можно создать в папке **Задачи** по кнопке **Создать задачу**.

Microsoft периодически удаляет со своих серверов устаревшие обновления, так что число актуальных обновлений составляет от 200 000 до 300 000. Для уменьшения используемого дискового пространства и размера базы данных Kaspersky Security Center удаляет устаревшие обновления, которые отсутствуют на серверах обновления Microsoft.

Во время выполнения задачи **Синхронизация обновлений Windows Update**, приложение получает список актуальных обновлений с сервера обновлений Microsoft. После чего Kaspersky Security Center определяет

список устаревших обновлений. При следующем запуске задачи **Поиск уязвимостей и требуемых обновлений** Kaspersky Security Center отмечает устаревшие обновления и устанавливает время на удаление. При следующем запуске задачи **Синхронизация обновлений Windows Update** удаляются обновления, которые были отмечены на удаление 30 дней назад. Kaspersky Security Center также выполняет дополнительную проверку для удаления устаревших обновлений, которые были отмечены на удаление более 180 дней назад.

После завершения работы задачи **Синхронизация обновлений Windows Update** и удаления устаревших обновлений в базе данных могут оставаться хеш-коды файлов удаленных обновлений, а также соответствующие им файлы в папке %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\working\wusfiles, в случае если они были загружены ранее. С помощью задачи **Обслуживание Сервера администрирования** (см. раздел "**обслуживание Сервера администрирования**"; на стр. [918](#)) можно удалить такие устаревшие записи из базы данных и соответствующие им файлы.

См. также:

Сценарий: обновление приложений сторонних производителей	499
В этом разделе	
Шаг 1. Определение необходимости уменьшения трафика	507
Шаг 2. Приложения	508
Шаг 3. Категории обновлений	508
Шаг 4. Языки локализации обновлений	508
Шаг 5. Выбор учетной записи для запуска задачи	509
Шаг 6. Настройка расписания запуска задачи	509
Шаг 7. Определение названия задачи	512
Шаг 8. Завершение создания задачи	513

Шаг 1. Определение необходимости уменьшения трафика

Когда Kaspersky Security Center синхронизирует обновления с серверами Microsoft Windows Update Servers, информация обо всех файлах сохраняется в базе данных Сервера администрирования. Также на диск загружаются все файлы, необходимые для обновления, при взаимодействии с Агентом обновления Windows. В частности, Kaspersky Security Center сохраняет информацию о файлах экспресс-установки в базу данных и загружает их по мере необходимости. Загрузка файлов экспресс-установки приводит к сокращению свободного места на диске.

Чтобы уменьшить сокращение объема дискового пространства и снизить трафик, вы можете выключить параметр **Загружать файлы экспресс-установки**.

Если параметр выбран, в процессе выполнения задачи загружаются файлы экспресс-установки. По умолчанию вариант не выбран.

См. также:

Синхронизация обновлений Windows Update с Сервером администрирования	506
Сценарий: обновление приложений сторонних производителей	499

Шаг 2. Приложения

В этом разделе можно выбрать приложения, для которых будут загружаться обновления.

Если установлен флажок **Все приложения**, то обновления будут загружаться для всех имеющихся приложений, а также для тех приложений, которые могут быть выпущены в будущем.

По умолчанию флажок **Все приложения** установлен.

См. также:

Синхронизация обновлений Windows Update с Сервером администрирования	506
Сценарий: обновление приложений сторонних производителей	499

Шаг 3. Категории обновлений

В этом разделе можно выбрать категории обновлений, которые будут загружаться на Сервер администрирования.

Если установлен флажок **Все категории**, то обновления будут загружаться для всех имеющихся категорий обновлений, а также для тех категорий, которые могут появиться в будущем.

По умолчанию флажок **Все категории** установлен.

См. также:

Синхронизация обновлений Windows Update с Сервером администрирования	506
Сценарий: обновление приложений сторонних производителей	499

Шаг 4. Языки локализации обновлений

В этом окне можно выбрать языки локализации обновлений, которые будут загружаться на Сервер администрирования. Выберите один из следующих вариантов загрузки языков локализации обновлений:

- **Загружать все языки, включая новые**

Если выбран этот вариант, на Сервер администрирования будут загружаться все доступные языки локализации обновлений. По умолчанию выбран этот вариант.

- **Загружать выбранные языки**

Если выбран этот вариант, в списке можно выбрать языки локализации обновлений, которые должны загружаться на Сервер администрирования.

См. также:

Синхронизация обновлений Windows Update с Сервером администрирования	506
Сценарий: обновление приложений сторонних производителей	499

Шаг 5. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** можно указать, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **Учетная запись по умолчанию**

Задача будет запускаться под той же учетной записью, под которой была установлено и запущено приложение, выполняющее эту задачу.

По умолчанию выбран этот вариант.

- **Задать учетную запись**

Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

- **Учетная запись**

Учетная запись, от имени которой будет запускаться задача.

- **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

См. также:

Синхронизация обновлений Windows Update с Сервером администрирования	506
Сценарий: обновление приложений сторонних производителей	499

Шаг 6. Настройка расписания запуска задачи

В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15

часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрывающимся списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security

Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- Один раз
- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрываемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрываемся списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемым списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемся списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.
- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи**

случайным образом в интервале (мин). По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

См. также:

Синхронизация обновлений Windows Update с Сервером администрирования	506
Сценарий: обновление приложений сторонних производителей	499

Шаг 7. Определение названия задачи

В окне **Определение названия задачи** укажите название создаваемого правила. Имя задачи не может превышать 100 символов и не может содержать специальные символы (" * < > ? \ : |). По умолчанию значение равно *Синхронизация обновлений Windows Update*.

См. также:

Синхронизация обновлений Windows Update с Сервером администрирования	506
Сценарий: обновление приложений сторонних производителей	499

Шаг 8. Завершение создания задачи

В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Созданная задача синхронизации обновлений Windows Update отобразится в списке задач в папке **Задачи** дерева консоли.

См. также:

Синхронизация обновлений Windows Update с Сервером администрирования	506
Сценарий: обновление приложений сторонних производителей	499

Установка обновлений на устройства вручную

Если в окне **Параметры управления обновлениями** мастера первоначальной настройки вы выбрали вариант **Искать и устанавливать требуемые обновления**, задача *Установка требуемых обновлений и закрытие уязвимостей* создается автоматически. Остановить или запустить задачу можно в папке **Управляемые устройства** на вкладке **Задачи**.

Если в мастере первоначальной настройки вы выбрали вариант **Искать требуемые обновления**, вы можете установить обновления программного обеспечения на клиентские устройства с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*.

Вы можете выполнить одно из следующих действий:

- Создайте задачу для установки обновлений.
- Добавьте правило для установки обновления в существующую задачу установки обновлений.
- В параметрах существующей задачи установки обновлений настройте тестовую установку обновлений.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Установка обновлений с помощью создания задачи установки обновлений

Вы можете выполнить одно из следующих действий:

- Создайте задачу для установки требуемых обновлений.
- Выберите обновление и создайте задачу для его установки и для установки аналогичных обновлений.

► *Чтобы установить требуемые обновления:*

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области папки выберите обновление, которое вы хотите установить.
3. Выполните одно из следующих действий:
 - В контекстном меню выбранного обновления выберите пункт **Установить обновление** → **Новая задача**.
 - По ссылке **Установить обновление (создать задачу)** в блоке работы с выбранными файлами.
4. Откроется окно установки всех предыдущих версий приложения. Нажмите **Да**, если вы согласны на последовательную установку версий приложения, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить приложение, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Следуйте далее указаниям мастера.
5. В окне мастера **Выбор действия при необходимости перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

- **Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрываемым списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрываемым списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрываемом списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**,

приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемым списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемом списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

1. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>? \:|).
2. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Вы можете включить автоматическую установку общесистемных компонентов (пререквизитов), перед установкой обновления в свойствах задачи *Установка требуемых обновлений и закрытие уязвимостей*. Когда параметр включен, все требуемые общесистемные компоненты устанавливаются перед обновлением. Список этих компонентов можно посмотреть в свойствах обновления.

В свойствах задачи *Установка требуемых обновлений и закрытие уязвимостей* вы можете разрешить установку обновлений, которые обновляют приложение до новой версии.

Если в параметрах задачи настроены правила установки обновлений сторонних производителей, Сервер администрирования загружает с сайта производителей требуемые обновления. Обновления сохраняются в хранилище Сервера администрирования и далее распространяются и устанавливаются на устройства, где они применимы.

Если в параметрах задачи настроены правила установки обновлений Microsoft и Сервер администрирования используется в качестве WSUS-сервера, Сервер администрирования загружает необходимые обновления в хранилище и далее распространяет на управляемые устройства. Если в сети

не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

► *Чтобы установить требуемое обновление и аналогичные обновления:*

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области выберите обновление, которое вы хотите установить.
3. Нажмите на кнопку **Запустить мастер установки обновления**.

Запустится мастер установки обновления.

Функционал мастера установки обновления доступен при наличии лицензии на Системное администрирование.

Следуйте далее указаниям мастера.

4. На странице **Поиск существующих задач установки обновления** укажите следующие параметры:
 - **Искать задачи, устанавливающие выбранное обновление**

Если этот параметр включен, мастер установки обновления ищет существующую задачу, чтобы установить выбранное обновление.

Если этот параметр выключен или если не было найдено подходящей задачи, мастер установки обновления предлагает создать правило или задачу для установки обновления.

По умолчанию параметр включен.

- **Одобрить установку обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

1. Если вы выбрали поиск существующей задачи для установки обновлений и было найдено несколько подходящих задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

В противном случае нажмите на кнопку **Новая задача установки обновления**.

2. Выберите тип правила установки, чтобы добавить его в новую задачу и нажмите на кнопку **Готово**.
3. Откроется окно установки всех предыдущих версий приложения. Нажмите **Да**, если вы согласны на последовательную установку версий приложения, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить приложение, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Следуйте далее указаниям мастера.

4. В окне мастера **Выбор действия при необходимости перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:
 - **Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. На странице мастера **Выбор устройств, которым будет назначена задача** выберите один из следующих вариантов:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**

В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **Задать адреса устройств вручную или импортировать из списка**

Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

2. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрываемым списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрываемым списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную (выбрано по умолчанию)**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрываемом списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемым списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемом списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании

задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

1. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\\:|).
2. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

После установки новой версии приложения может быть нарушена работа других приложений, установленных на устройствах и зависящих от работы обновляемого приложения.

Установка обновления с помощью добавления правила в существующую задачу

► Чтобы установить обновление с помощью добавления правила в существующую задачу:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области выберите обновление, которое вы хотите установить.
3. Нажмите на кнопку **Запустить мастер установки обновления**.

Запустится мастер установки обновления.

Функционал мастера установки обновления доступен при наличии лицензии на Системное администрирование.

Следуйте далее указаниям мастера.

4. На странице **Поиск существующих задач установки обновления** укажите следующие параметры:
 - **Искать задачи, устанавливающие выбранное обновление**

Если этот параметр включен, мастер установки обновления ищет существующую задачу, чтобы установить выбранное обновление.

Если этот параметр выключен или если не было найдено подходящей задачи, мастер установки обновления предлагает создать правило или задачу для установки обновления.

По умолчанию параметр включен.

- **Одобрить установку обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

1. Если вы выбрали поиск существующей задачи для установки обновлений и было найдено несколько подходящих задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

В противном случае нажмите на кнопку **Добавить правило установки обновления**.

2. Выберите задачу, для которой вы хотите добавить правило и нажмите на кнопку **Добавить правило**.

Также вы можете просмотреть свойства существующих задач, запустить их вручную или создать задачу.

3. Выберите тип правила, которое будет добавлено в выбранную задачу, и нажмите на кнопку **Готово**.
4. Откроется окно установки всех предыдущих версий приложения. Нажмите **Да**, если вы согласны на последовательную установку версий приложения, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить приложение, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Новое правило для установки обновления добавлено в существующую задачу **Установка требуемых обновлений и закрытие уязвимостей**.

Настройка проверочной установки обновлений

► Чтобы настроить проверочную установку обновлений:

1. В дереве консоли в папке **Управляемые устройства** на вкладке **Задачи** выберите задачу **Установка требуемых обновлений и закрытие уязвимостей**.
2. В контекстном меню задачи выберите пункт **Свойства**.
Откроется окно свойств задачи **Установка требуемых обновлений и закрытие уязвимостей**.
3. В окне свойств задачи в разделе **Проверочная установка** выберите один из доступных вариантов проверочной установки:
 - **Не проверять**. Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.
 - **Выполнить проверку на указанных устройствах**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.
 - **Выполнить проверку на устройствах в указанной группе**. Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задайте тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.
 - **Выполнить проверку на указанном проценте устройств**. Выберите этот вариант, если вы хотите выполнить проверку обновлений на части устройств. В поле **Процент тестовых устройств из общего числа устройств** укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.
4. После выбора любого параметра, кроме **Не проверять**, в поле **Среднее время для принятия решения о продолжении установки (ч)** укажите количество часов, которое должно пройти от тестовой установки обновлений, до начала установки обновлений на все устройства.

См. также:

Сценарий: обновление приложений сторонних производителей[499](#)

Настройка обновлений Windows в политике Агента администрирования

► Чтобы настроить обновления Windows в политике Агента администрирования:

1. В дереве консоли выберите **Управляемые устройства**.
2. В рабочей области выберите вкладку **Политики**.
3. Выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.
Откроется окно свойств политики Агента администрирования.
5. В панели **Разделы** выберите **Обновления и уязвимости в приложениях**.
6. Выберите параметр **Использовать Сервер администрирования в роли WSUS-сервера**, чтобы загружать обновления Windows на Сервер администрирования и затем распространять их на клиентские устройства средствами Агента администрирования.

Если этот параметр не выбран, обновления Windows загружаются на Сервер администрирования. В этом случае клиентские устройства получают обновления Windows напрямую с серверов Microsoft.

7. Выберите набор обновлений, которые могут устанавливать пользователи на своих устройствах вручную, используя Центр обновления Windows.

Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, то новый параметр, который вы выбрали под **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

Выберите параметр из раскрывающегося списка:

- **Устанавливать все применимые обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

Выберите этот вариант, если вы не хотите влиять на установку обновлений.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Устанавливать только одобренные обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Запретить устанавливать обновления Центра обновления Windows**

Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

1. Выберите режим поиска обновлений Windows Update:

- **Активный**

Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от агента обновлений Windows.

По умолчанию выбран этот вариант.

- **Пассивный**

Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при последней синхронизации агента обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.

- **Выключен**

Если выбран этот вариант, Сервер администрирования не запрашивает информацию об обновлениях.

2. Выберите параметр **Проверять исполняемые файлы на наличие уязвимостей при запуске**, если требуется выполнять проверку исполняемых файлов на наличие уязвимостей при запуске.
3. Убедитесь, что редактирование заблокировано для всех параметров, которые вы изменили. В противном случае изменения не применяются.
4. Нажмите на кнопку **Применить**.

См. также:

Сценарий: обновление приложений сторонних производителей[499](#)

Уязвимости в приложениях

Папка **Уязвимости в приложениях**, входящая в состав папки **Управление приложениями**, содержит список уязвимостей в приложениях, которые обнаружил на клиентских устройствах установленный на них Агент администрирования. Агент администрирования выполняет поиск известных уязвимостей программного обеспечения на основе признаков из баз данных об известных уязвимостях.

Функциональность анализа информации об уязвимостях в приложениях поддерживается только для операционных систем Microsoft Windows.

Открыв окно свойств выбранного приложения в папке **Уязвимости в приложениях**, вы можете получить общую информацию об уязвимости, о приложении, в котором она обнаружена, просмотреть список устройств, на которых обнаружена уязвимость, а также информацию о закрытии уязвимости.

Вы можете получить сведения об уязвимостях в приложениях на сайте "Лаборатории Касперского" (<https://threats.kaspersky.com/ru/>).

В этом разделе

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....	529
Об обнаружении и закрытии уязвимостей в приложениях	532
Просмотр информации об уязвимостях в приложениях	533
Просмотр статистики уязвимостей на управляемых устройствах.	534
Поиск уязвимостей в приложениях	535
Закрытие уязвимостей в приложениях	541
Закрытие уязвимостей в изолированной сети	555
Игнорирование уязвимостей в приложениях	565
Пользовательские исправления для уязвимостей в приложениях сторонних производителей	566
Правила установки обновлений	567

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей

В этом разделе представлен сценарий обнаружения и закрытия уязвимостей на управляемых устройствах под управлением Windows. Вы можете найти и закрыть уязвимости в приложениях, в операционных системах и в приложениях сторонних производителей, включая программное обеспечение Microsoft.

Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- В сети вашей организации есть управляемые устройства под управлением Windows.
- Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:
 - Составление списка рекомендуемых исправлений уязвимостей в приложениях Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
 - Закрытие уязвимостей в приложениях сторонних производителей, отличных от приложений Microsoft.

Этапы

Обнаружение и закрытие уязвимостей состоит из следующих этапов:

а. Поиск уязвимостей в программном обеспечении, установленном на управляемых устройствах

Чтобы найти уязвимости в приложениях, установленных на управляемых устройствах, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, запустите его сейчас или создайте задачу вручную.

Инструкции:

- Консоль администрирования: Поиск уязвимостей в приложениях (на стр. [535](#)), Задание расписания для задачи поиска уязвимостей и требуемых обновлений (см. раздел "Настройка расписания задачи Поиск уязвимостей и требуемых обновлений." на стр. [412](#)).
- Kaspersky Security Center Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений, Параметры задачи поиска уязвимостей и требуемых обновлений.

b. Анализ списка обнаруженных уязвимостей в приложениях

Просмотрите список **Уязвимости в приложениях** и решите, какие уязвимости требуется закрыть. Чтобы просмотреть подробную информацию о каждой уязвимости, нажмите на имя уязвимости в списке. Для каждой уязвимости в списке вы также можете просмотреть статистику уязвимости на управляемых устройствах.

Инструкции:

- Консоль администрирования: Просмотр информации об уязвимостях в приложениях (на стр. [533](#)), Просмотр статистики уязвимостей на управляемых устройствах (см. раздел "Просмотр статистики уязвимостей на управляемых устройствах." на стр. [534](#)).
- Kaspersky Security Center Web Console: Просмотр информации об уязвимостях в приложениях, Просмотр статистики уязвимостей на управляемых устройствах.

c. Настройка закрытия уязвимостей

Обнаружив уязвимости в приложениях, вы можете закрыть уязвимости в приложениях на управляемых устройствах, используя задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей*.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, в том числе в приложениях Microsoft, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование. Чтобы устранить уязвимости в приложениях, задача *Установка требуемых обновлений и закрытие уязвимостей* использует рекомендованные обновления приложений.

Задача *Закрытие уязвимостей* не требует лицензии для Системного администрирования. Чтобы использовать эту задачу, требуется вручную указать пользовательские исправления для закрытия уязвимостей в приложениях сторонних производителей, которые указаны в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для приложений сторонних производителей.

Вы можете запустить мастер закрытия уязвимостей, который автоматически создаст одну из этих задач, или вы можете создать одну из этих задач вручную.

Инструкции:

- Консоль администрирования: Пользовательские исправления для уязвимостей в приложениях сторонних производителей (на стр. [566](#)), Закрытие уязвимостей в приложениях (на стр. [541](#)).
- Kaspersky Security Center Web Console: Пользовательские исправления для уязвимостей в приложениях сторонних производителей, Закрытие уязвимостей в приложениях сторонних производителей, Создание задачи Установка требуемых обновлений и закрытие уязвимостей.

d. Задание расписания задачи

Чтобы убедиться, что список уязвимостей всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. Рекомендуемый средний период – один раз в неделю.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. При задании расписания задачи *Закрытие уязвимостей*, вам нужно выбрать исправления приложений Microsoft или указать пользовательские исправления для приложений сторонних производителей каждый раз перед запуском задачи.

При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

е. Игнорирование уязвимостей в приложениях (если требуется)

Вы можете игнорировать уязвимости в приложениях, которые должны быть закрыты на всех управляемых устройствах или только на выбранных управляемых устройствах.

Инструкции:

- Консоль администрирования: Игнорирование уязвимостей в приложениях (на стр. [565](#)).
- Kaspersky Security Center Web Console: Игнорирование уязвимостей в приложениях.

ф. Запуск задачи закрытия уязвимости

Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или *Закрытие уязвимостей*. Когда задача будет завершена, убедитесь, что в списке задач она имеет статус *Завершена успешно*.

г. Создание отчета о результатах закрытия уязвимостей в приложениях (если требуется)

Чтобы просмотреть статистику о закрытых уязвимостях, сформируйте отчет об уязвимостях. В отчете отображается информация об уязвимостях в приложениях, которые не закрыты. Таким образом, вы можете иметь представление об обнаружении и закрытии уязвимостей в приложениях сторонних производителей в вашей организации, включая программное обеспечение Microsoft.

Инструкции:

- Консоль администрирования: Создание и просмотр отчета (на стр. [607](#)).
- Kaspersky Security Center Web Console: Генерация и просмотр отчета.

h. Проверка настройки обнаружения и закрытия уязвимостей в приложениях сторонних производителей

Убедитесь, что вы выполнили следующее:

- обнаружили и просмотрели список уязвимостей в приложениях на управляемых устройствах;
- игнорировали уязвимости в приложениях, если хотели;
- настроили задачу закрытия уязвимости;
- запланировали запуск задач для поиска и закрытия уязвимостей в приложениях так, чтобы они запускались последовательно;
- проверили, что задача закрытия уязвимостей была запущена.

Результаты

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытие уязвимостей*, уязвимости будут автоматически закрыты на управляемых устройствах. При запуске задачи, задача выполняет сопоставление списка доступных обновлений программного обеспечения с правилами, указанными в параметрах задачи. Все обновления программного обеспечения, которые соответствуют критериям в правилах, будут загружены в хранилище Сервера администрирования и будут установлены для закрытия уязвимостей в приложениях.

Если вы создали задачу *Закрытие уязвимостей*, закрываются только уязвимости в приложениях Microsoft.

Об обнаружении и закрытии уязвимостей в приложениях

Kaspersky Security Center обнаруживает и закрывает уязвимости в приложениях на управляемых устройствах под управлением операционных систем семейства Microsoft Windows. Уязвимости обнаружены в операционных системах и в приложениях сторонних производителей, включая программное обеспечение Microsoft.

Обнаружение уязвимостей в приложениях

Для обнаружения уязвимостей Kaspersky Security Center выполняет поиск известных уязвимостей программного обеспечения на основе признаков из баз данных об известных уязвимостях. Эта база формируется специалистами "Лаборатории Касперского". Она содержит информацию об уязвимостях, такую как описание уязвимостей, дата обнаружения уязвимостей, уровень критичности уязвимостей. Вы можете получить сведения об уязвимостях в программах на сайте "Лаборатории Касперского" (<https://threats.kaspersky.com/ru/>).

В Kaspersky Security Center для поиска уязвимостей приложений используется задача *Поиск уязвимостей и требуемых обновлений*.

Закрытие уязвимостей в приложениях

Для закрытия уязвимостей в приложениях, Kaspersky Security Center использует обновления программного обеспечения выпущенные поставщиками программного обеспечения. Метаданные обновлений программного обеспечения загружаются в хранилище Сервера администрирования в результате выполнения следующих задач:

- *Загрузка обновлений в хранилище Сервера администрирования.* Эта задача предназначена для загрузки метаданных обновлений для приложений "Лаборатории Касперского" и приложений сторонних производителей. Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Задача загрузки обновлений в хранилище Сервера администрирования может быть создана вручную.
- *Синхронизация обновлений Windows Update.* Эта задача предназначена для загрузки метаданных обновлений программного обеспечения Microsoft.

Обновления программного обеспечения для закрытия уязвимостей могут быть представлены в виде полных дистрибутивов или патчей. Обновления программного обеспечения, которые закрывают уязвимости в приложениях, называются *исправлениями*. *Рекомендуемые исправления* это исправления, которые рекомендуются к установке специалистами "Лаборатории Касперского". *Пользовательские исправления* это исправления, которые вручную указываются для установки пользователями. Чтобы установить пользовательское исправление, необходимо создать инсталляционный пакет, содержащий это исправление.

Если лицензия Kaspersky Security Center предусматривает возможности Системного администрирования, для закрытия уязвимостей используйте задачу *Установка требуемых обновлений и закрытие уязвимостей*. Эта задача автоматически закрывает несколько уязвимостей, устанавливая рекомендуемые исправления. Для этой задачи вы можете вручную настроить определенные правила для закрытия нескольких уязвимостей.

Если лицензия Kaspersky Security Center не предусматривает возможности Системного администрирования, для закрытия уязвимостей используйте задачу *Закрытие уязвимостей*. С помощью этой задачи можно закрыть уязвимости, установив рекомендуемые исправления для приложений Microsoft и пользовательских исправлений для приложений сторонних производителей.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Специалисты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также специалисты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Для закрытия некоторых уязвимостей в приложениях вам нужно принять Лицензионное соглашение для установки приложений, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в приложении не закроется.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Просмотр информации об уязвимостях в приложениях

- Чтобы просмотреть список уязвимостей, обнаруженных на клиентских устройствах,

В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.

Отобразится страница со списком уязвимостей в приложениях, обнаруженных на управляемых устройствах.

- Чтобы получить информацию о выбранной уязвимости,

В контекстном меню уязвимости выберите пункт **Свойства**.

Откроется окно свойств уязвимости, в котором отображается следующая информация:

- приложение, в котором обнаружена уязвимость;
- список устройств, на которых обнаружена уязвимость;
- информация о закрытии уязвимости.

► Чтобы просмотреть отчет обо всех обнаруженных уязвимостях,

В папке **Уязвимости в приложениях** перейдите по ссылке **Просмотреть отчет об уязвимостях в приложениях**.

Будет создан отчет об уязвимостях в приложениях, установленных на устройствах. Отчет можно просмотреть в узле с именем нужного вам Сервера администрирования на вкладке **Отчеты**.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Просмотр статистики уязвимостей на управляемых устройствах.

Вы можете просмотреть статистическую информацию каждой уязвимости в приложениях на управляемых устройствах. Статистика представлена в виде диаграмм. На диаграмме отображается количество устройств со следующими статусами:

- *Игнорируется на:* <количество устройств>. Этот статус присваивается, если в свойствах уязвимости вы вручную установили параметр игнорировать уязвимость.
- *Закрыта на:* <количество устройств>. Этот статус присваивается, если задача закрытия уязвимости успешно завершена.
- *Запланирована к закрытию на:* <количество устройств>. Этот статус присваивается, если вы создали задачу закрытия уязвимостей, но задача пока еще не завершена.
- *Применено исправление на:* <количество устройств>. Этот статус присваивается, если вы вручную выбрали обновление программного обеспечения, чтобы закрыть уязвимость, но это обновление не закрыло уязвимость.
- *Требуется закрытия на:* <количество устройств>. Этот статус присваивается, если уязвимость была закрыта только на некоторых управляемых устройствах, а уязвимость требуется закрыть на других управляемых устройствах.

► Чтобы просмотреть статистику уязвимости на управляемых устройствах:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.

Отобразится страница со списком уязвимостей в приложениях, обнаруженных на управляемых устройствах.

2. Выберите уязвимость для которой вы хотите просмотреть статистику.

В блоке для работы с выбранным объектом отображается диаграмма состояний уязвимости. Нажав на статус, откроется список устройств, на которых уязвимость имеет выбранный статус.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Поиск уязвимостей в приложениях

Если вы выполнили настройку приложения с помощью мастера первоначальной настройки, задача *Поиск уязвимостей* создается автоматически. Просмотреть задачу можно в папке **Управляемые устройства** на вкладке **Задачи**.

► *Чтобы создать задачу поиска уязвимостей в приложениях, установленных на клиентских устройствах:*

1. В дереве консоли выберите **Дополнительно** → **Управление приложениями**, а затем выберите подпапку **Уязвимости в приложениях**.
2. В рабочей области выберите **Дополнительные действия** → **Настроить поиск уязвимостей**.

Если задача для поиска уязвимостей уже существует, она отображается на вкладке **Задачи** в папке **Управляемые устройства**, с существующими выбранными задачами. В противном случае запускается мастер создания задачи поиска уязвимостей и требуемых обновлений. Следуйте далее указаниям мастера.

3. В окне **Выбор типа задачи** выберите **Поиск уязвимостей и требуемых обновлений**.
4. В окне мастера **Параметры**, укажите следующие параметры задачи:

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Соединяться с сервером обновлений для актуализации данных**

Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

- Сервер администрирования Kaspersky Security Center (см. параметры политики Агента администрирования (см. стр. [789](#))).
- Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
- Серверы обновления Microsoft.

Если этот параметр включен, Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее и которая хранится в кеше устройства.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент Центра обновления Windows на управляемом устройстве подключается к серверу обновлений Microsoft, чтобы получить обновления, только если включен параметр **Соединиться с сервером обновлений для актуализации данных** и параметр **Активный** в группе параметров **Режим поиска Центра обновления Windows**.
 - Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, полученную ранее от источника обновлений Microsoft и сохраненную в кеше устройства, если включен параметр **Соединиться с сервером обновлений для актуализации данных** и параметр **Пассивный** в группе параметров **Режим поиска Центра обновления Windows**, или если параметр **Соединиться с сервером обновлений для актуализации данных** выключен, а в группе параметров **Режим поиска Центра обновления Windows** выбран параметр **Активный**.
 - Независимо от параметра **Соединиться с сервером обновлений для актуализации данных** (включен он или выключен), если в группе параметров **Выключен** выбран параметр **Режим поиска Центра обновления Windows**, Kaspersky Security Center не запрашивает информацию об обновлениях.
- **Поиск уязвимостей и сторонних обновлений, перечисленных "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Укажите пути для дополнительного поиска приложений в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке

%WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. раздел "Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center" см. стр. [773](#)), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

1. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрываемым списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрываемом списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При загрузке обновлений в хранилище**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При загрузке обновлений в хранилище**, задача будет запускаться после загрузки обновлений в хранилище.

- **При обнаружении вирусной атаки**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При**

обнаружении вирусной атаки, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрывающимся списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрывающимся списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрывающемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

1. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Поиск уязвимостей и требуемых обновлений**, которая отображается в списке задач, в папке **Управляемые устройства**, на вкладке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

Когда задача *Поиск уязвимостей и требуемых обновлений* завершена, Сервер администрирования отображает список уязвимостей, обнаруженных в приложениях, установленных на устройстве; также Сервер отображает все обновления программного обеспечения, необходимые для исправления обнаруженных уязвимостей.

Если отображается ошибка 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows <https://support.kaspersky.com/15773>.

Сервер администрирования не отображает список необходимых обновлений программного обеспечения при последовательном запуске двух задач: задачи *Синхронизация обновлений Windows Update*, для которой отключен параметр **Загружать файлы экспресс-установки**, и затем задачи *Поиск уязвимостей и требуемых обновлений*. Чтобы просмотреть список необходимых обновлений программного обеспечения, необходимо снова запустить задачу *Поиск уязвимостей и требуемых обновлений*.

Агент администрирования получает информацию о любых доступных обновлениях Windows и других приложений Microsoft от Центра обновления Windows или от Сервера администрирования, если Сервер администрирования выполняет роль WSUS-сервера. Информация передается при запуске приложений (если это предусмотрено политикой) и при каждом запуске задачи *Поиск уязвимостей и требуемых обновлений* на клиентских устройствах.

Вы можете получить сведения о программном обеспечении сторонних производителей, которое можно обновлять с помощью Kaspersky Security Center на веб-сайте Службы технической поддержки на странице Kaspersky Security Center, в разделе **Управление Сервером** (<http://support.kaspersky.ru/9327>).

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....	529
Сценарий: обновление приложений сторонних производителей	499

Заккрытие уязвимостей в приложениях

Если в окне **Параметры управления обновлениями** мастера первоначальной настройки вы выбрали вариант **Искать и устанавливать требующиеся обновления**, задача *Установка требуемых обновлений и закрытие уязвимостей* создается автоматически. Задача отображается в папке **Управляемые устройства** на вкладке **Задачи**.

В противном случае вы можете выполнить одно из следующих действий:

- Создайте задачу для закрытия уязвимостей с помощью установки доступных обновлений.
- Добавьте правило для закрытия уязвимостей в существующую задачу закрытия уязвимостей.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Заккрытие уязвимостей с помощью задачи закрытия уязвимостей

Вы можете выполнить одно из следующих действий:

- Создайте задачу закрытия нескольких уязвимостей, соответствующих определенным правилам.
- Выберите уязвимость и создайте задачу для ее закрытия и для закрытия аналогичных уязвимостей.

► Чтобы закрыть уязвимости, которые соответствуют определенным правилам:

1. В дереве консоли выберите Сервер администрирования, на устройствах которого вы хотите закрыть уязвимости.
2. В меню **Вид** главного окна приложения выберите пункт **Настройка интерфейса**.
3. В открывшемся окне установите флажок **Отображать Системное администрирование** и нажмите на кнопку **ОК**.
4. В окне с сообщением приложения нажмите на кнопку **ОК**.
5. Перезапустите Консоль администрирования, чтобы изменения вступили в силу.
6. В дереве консоли выберите папку **Управляемые устройства**.
7. В рабочей области выберите вкладку **Задачи**.
8. По кнопке **Создать задачу** запустите мастер создания задачи. Следуйте далее указаниям мастера.
9. В окне **Выбор типа задачи** мастера создания задачи выберите **Установка требуемых обновлений и закрытие уязвимостей**.

Если задача не отображается, проверьте, есть ли у вашей учетной записи права (см. раздел "Права доступа к функциям приложения" на стр. [810](#)) **Чтение, Изменение и Выполнение** в функциональной области **Управление системой: Системное администрирование**. Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.

10. В окне мастера **Параметры**, укажите следующие параметры задачи:

- **Задайте правила установки обновлений**

Эти правила применяются при установке обновлений на клиентские устройства. Если правила не указаны, задача не выполняется. Дополнительную информацию о работе с правилами см. в разделе Правила установки обновлений (см. стр. [567](#)).

- **Начинать установку в момент перезагрузки или выключения устройства**

Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

По умолчанию параметр выключен.

- **Устанавливать требуемые общесистемные компоненты**

Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

Если этот параметр выключен, необходимо установить пререквизиты вручную.

По умолчанию параметр выключен.

- **Разрешать установку новой версии приложения при обновлении**

Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии приложения.

Если этот параметр выключен, приложение не обновляется. Можно позднее

установить новые версии приложений вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию приложения или если требуется проверить обновление в тестовой инфраструктуре.

По умолчанию параметр включен.

После установки новой версии приложения может быть нарушена работа других приложений, установленных на клиентских устройствах и зависящих от работы обновляемой приложения.

- **Загружать обновления на устройство, не устанавливая их**

Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Загрузить обновления для**.

Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

По умолчанию параметр выключен.

- **Загрузить обновления для**

Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. раздел "Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center" см. стр. [773](#)), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

1. В окне мастера **Выбор действия при необходимости перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

- **Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

Запущенные приложения могут не позволить перезагрузить клиентское устройство.

Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрывающимся списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим

Еженедельно, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрывающимся списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемом списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

1. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\":|).
2. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

Если результаты задачи содержат ошибку 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

► *Чтобы закрыть требуемую уязвимость и аналогичные ей:*

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.
2. Выберите уязвимость, которую вы хотите закрыть.
3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

Откроется мастер закрытия уязвимости.

Функционал мастера закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

Следуйте далее указаниям мастера.

4. В разделе **Поиск существующих задач закрытия уязвимости** укажите следующие параметры:

- **Показывать только задачи, закрывающие выбранную уязвимость**

Если этот параметр включен, мастер закрытия уязвимости выполняет поиск существующих задач для закрытия выбранной уязвимости.

Если этот параметр выключен или не было найдено применимых задач, мастер закрытия уязвимости предлагает создать правило или задачу для закрытия уязвимости.

По умолчанию параметр включен.

- **Одобрить обновления, закрывающие выбранную уязвимость**

Обновления, которые закрывают уязвимость, будут одобрены к установке.

Включите этот параметр, если некоторые применяемые правила установки обновлений разрешают установку только одобренных обновлений.

По умолчанию параметр выключен.

5. Если для закрытия уязвимости вы выбрали поиск существующих задач и было найдено несколько задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

В противном случае нажмите на кнопку **Новая задача закрытия уязвимости**.

6. Выберите тип правила, закрывающего уязвимость, чтобы добавить его в существующую задачу и нажмите на кнопку **Готово**.
7. Откроется окно установки всех предыдущих версий приложения. Нажмите **Да**, если вы согласны на последовательную установку версий приложения, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить приложение, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Следуйте далее указаниям мастера.

8. В окне мастера **Выбор действия при необходимости перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

- **Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут.

Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. На странице мастера **Выбор устройств, которым будет назначена задача** выберите один из следующих вариантов:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**

В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **Задать адреса устройств вручную или импортировать из списка**

Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

Задача назначается устройствам, входящим в ранее созданную группу

администрирования. Можно указать одну из существующих групп или создать новую группу.

Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

2. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрывающимся списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15

часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрываемом списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемым списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.

- **Результат выполнения.** В раскрывающемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

1. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\\:|).
2. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

Закрытие уязвимости с помощью добавления правила в существующую задачу закрытия уязвимостей

► Чтобы закрыть уязвимость с помощью добавления правила в существующую задачу закрытия уязвимостей:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.
2. Выберите уязвимость, которую вы хотите закрыть.
3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

Откроется мастер закрытия уязвимости.

Функционал мастера закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

Следуйте далее указаниям мастера.

4. В разделе **Поиск существующих задач закрытия уязвимости** укажите следующие параметры:

- **Показывать только задачи, закрывающие выбранную уязвимость**

Если этот параметр включен, мастер закрытия уязвимости выполняет поиск существующих задач для закрытия выбранной уязвимости.

Если этот параметр выключен или не было найдено применимых задач, мастер закрытия уязвимости предлагает создать правило или задачу для закрытия уязвимости.

По умолчанию параметр включен.

- **Одобрить обновления, закрывающие выбранную уязвимость**

Обновления, которые закрывают уязвимость, будут одобрены к установке.

Включите этот параметр, если некоторые применяемые правила установки обновлений разрешают установку только одобренных обновлений.

По умолчанию параметр выключен.

5. Если для закрытия уязвимости вы выбрали поиск существующих задач и было найдено несколько задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

В противном случае нажмите на кнопку **Добавить правило закрытия уязвимости в существующую задачу**.

6. Выберите задачу, для которой вы хотите добавить правило и нажмите на кнопку **Добавить правило**.

Также вы можете просмотреть свойства существующих задач, запустить их вручную или создать задачу.

7. Выберите тип правила, чтобы добавить его в выбранную задачу, и нажмите на кнопку **Готово**.
8. Откроется окно установки всех предыдущих версий приложения. Нажмите **Да**, если вы согласны на последовательную установку версий приложения, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить приложение, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Новое правило для закрытия уязвимости добавлено в существующую задачу **Установка требуемых обновлений и закрытие уязвимостей**.

См. также:

Сценарий: обновление приложений сторонних производителей[499](#)

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Закрытие уязвимостей в изолированной сети

В этом разделе описаны действия, которые вы можете предпринять для закрытия уязвимостей в приложениях сторонних производителей на управляемых устройствах, подключенных к Серверам администрирования и не имеющих доступа в интернет.

Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети

Вы можете устанавливать обновления и закрывать уязвимости приложений сторонних производителей, установленных на управляемых устройствах в изолированной сети. К таким сетям относятся Серверы администрирования и подключенные к ним управляемые устройства, не имеющие доступа в интернет. Для закрытия уязвимостей в такой сети необходим Сервер администрирования, подключенный к интернету. Также вы можете загружать патчи (требуемые обновления) с помощью Сервера администрирования с доступом в интернет и передавать исправления на изолированные Серверы администрирования.

Вы можете загружать обновления приложений сторонних производителей, выпущенные производителями программного обеспечения, но не можете загружать обновления для программного обеспечения Microsoft на изолированных Серверах администрирования с помощью Kaspersky Security Center.

Чтобы узнать, как работает процесс закрытия уязвимостей в изолированной сети, ознакомьтесь с описанием и схемой этого процесса (см. раздел "О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети" см. стр. [557](#)).

Предварительные требования

Перед началом сделайте следующее:

1. Выделите одно устройство для подключения к интернету и загрузки исправлений. Это устройство будет считаться Сервером администрирования с доступом в интернет.
2. Установите Kaspersky Security Center (см. раздел "Основной сценарий установки" на стр. [56](#)) версии не ниже 14 на следующих устройствах:
 - Выделенное устройство, которое будет выступать в роли Сервера администрирования с доступом в интернет.
 - Изолированные устройства, которые будут выступать в роли изолированных от интернета Серверов администрирования (далее – изолированные Серверы администрирования).
3. Убедитесь, что на каждом Сервере администрирования достаточно места на диске для загрузки и хранения обновлений и исправлений.

Этапы

Установка обновлений и закрытие уязвимостей приложений сторонних производителей на управляемых устройствах, относящихся к изолированным Серверам администрирования, состоит из следующих этапов:

а. Настройка Сервера администрирования с доступом в интернет

Подготовьте Сервер администрирования с доступом в интернет (см. раздел "Настройка Сервера администрирования с доступом в интернет для закрытия уязвимостей в изолированной сети" на стр. [558](#)) для обработки запросов на необходимые обновления стороннего программного обеспечения и для загрузки.

б. Настройка изолированных Серверов администрирования

Подготовьте изолированные Серверы администрирования (см. раздел "Настройка изолированных Серверов администрирования для закрытия уязвимостей в изолированной сети" на стр. [559](#)), чтобы они могли регулярно формировать списки необходимых обновлений и обрабатывать патчи, загружаемые Сервером администрирования с доступом в интернет. После настройки изолированные Серверы администрирования больше не пытаются загружать патчи из интернета. Вместо этого они получают обновления через патчи.

с. Передача патчей и установка обновлений на изолированные Серверы администрирования

После завершения настройки Серверов администрирования вы можете передавать необходимые списки обновлений и патчей (см. раздел "Передача исправлений и установка обновлений в изолированной сети" на стр. [561](#)) между Сервером администрирования с доступом в интернет и изолированными Серверами администрирования. Далее обновления из исправлений будут установлены на управляемые устройства с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*.

Результаты

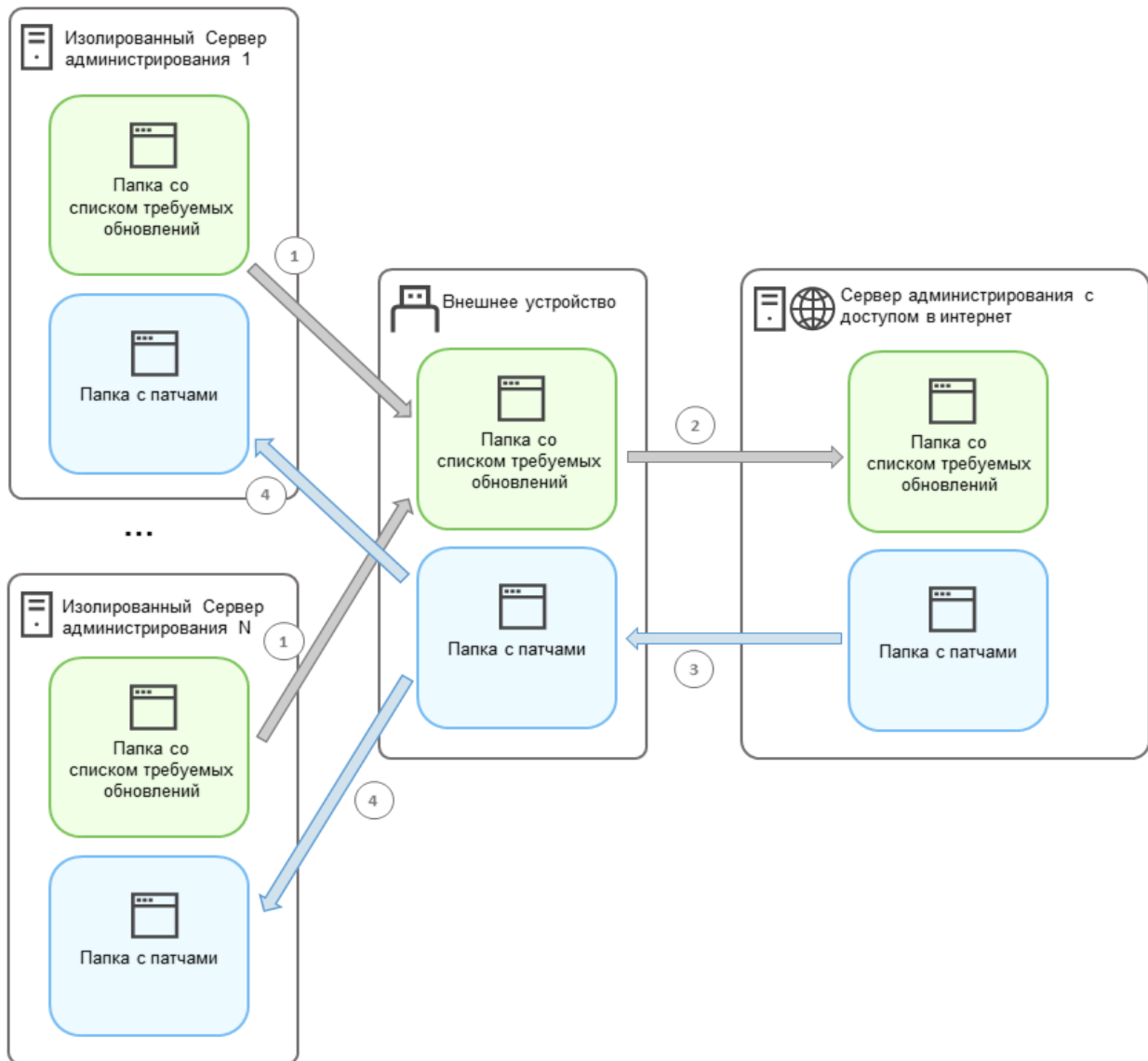
Таким образом обновления приложений сторонних производителей передаются на изолированные Серверы администрирования и устанавливаются на подключенные управляемые устройства с помощью Kaspersky Security Center. Достаточно один раз настроить Серверы администрирования, чтобы получать обновления с нужной вам частотой, например, один или несколько раз в день.

См. также:

Выключение возможности передачи исправлений и установки обновлений в изолированной сети [564](#)

О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети

Процесс закрытия уязвимостей в приложениях сторонних производителей в изолированной сети (см. раздел "Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети" на стр. [555](#)) показан на рисунке и описан ниже. Вы можете периодически повторять этот процесс.



Каждый Сервер администрирования, изолированный от сети интернет (далее — изолированный Сервер администрирования), формирует список обновлений, которые необходимо установить на управляемые устройства, подключенные к данному Серверу администрирования. Список необходимых обновлений хранится в специальной папке и представляет собой набор бинарных файлов. Каждый файл имеет имя, которое содержит идентификатор патча с требуемым обновлением. В результате каждый файл в списке указывает на определенный патч.

С помощью внешнего устройства вы переносите список необходимых обновлений с изолированного Сервера администрирования на выделенный Сервер администрирования с доступом в интернет. После этого выделенный Сервер администрирования загружает патчи из интернета и помещает их в отдельную папку.

Когда все патчи загружены и размещены в специальной для них папке, вы перемещаете патчи на каждый изолированный Сервер администрирования, с которого вы взяли список необходимых обновлений. Вы сохраняете патчи в специально созданную для них папку на изолированном Сервере администрирования. В результате задача *Установка требуемых обновлений и закрытие уязвимостей* запускает патчи и устанавливает обновления на управляемые устройства изолированных Серверов администрирования.

См. также:

Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети [555](#)
 Передача исправлений и установка обновлений в изолированной сети [561](#)

Настройка Сервера администрирования с доступом в интернет для закрытия уязвимостей в изолированной сети

Чтобы подготовиться к закрытию уязвимостей и передаче патчей (см. раздел "Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети" на стр. [555](#)) в изолированной сети, сначала настройте Сервер администрирования с доступом в интернет, а затем настройте изолированные Серверы администрирования (см. раздел "Настройка изолированных Серверов администрирования для закрытия уязвимостей в изолированной сети" на стр. [559](#)).

► Чтобы настроить Сервер администрирования с доступом в интернет:

1. Создайте две папки (см. раздел "О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети" см. стр. [557](#)) на диске, где установлен Сервер администрирования:
 - папку для списка необходимых обновлений;
 - папку для патчей.

Названия папок могут быть любыми.

2. Предоставьте группе KLABins (см. раздел "Права доступа к Серверу администрирования и его объектам" на стр. [706](#)) право Изменение на созданные папки, используя стандартные средства администрирования операционной системы.
3. С помощью утилиты klscflag укажите пути к папкам в свойствах Сервера администрирования.
 Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
4. Введите следующие команды в командной строке Windows:
 - Чтобы указать путь к папке для исправлений:

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<path to the folder>"
```

- Чтобы задать путь к папке для списка необходимых обновлений:

```
klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<path to the folder>"
```

Пример: klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\FolderForPatches"

- При необходимости с помощью утилиты `klscflag` укажите, как часто Сервер администрирования должен проверять наличие новых запросов на исправления:

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v
<значение в секундах>
```

По умолчанию указано значение 120 секунд.

Пример: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

- Создайте задачу *Поиск уязвимостей и требуемых обновлений*, чтобы получить информацию о патчах для приложений сторонних производителей, установленных на управляемых устройствах, и настройте расписание выполнения задачи.
- Создайте задачу *Закрытие уязвимостей*, чтобы указать патчи для приложений сторонних производителей, используемых для закрытия уязвимостей, и настройте расписание задачи.
Запустите задачи вручную, если вы хотите, чтобы они выполнялись раньше, чем указано в расписании задачи. Порядок запуска задач важен. Задачу *Закрытие уязвимостей* необходимо запустить после завершения задачи *Поиск уязвимостей и требуемых обновлений*.
- Перезапустите службу Сервера администрирования.

Теперь Сервер администрирования с доступом в интернет готов к загрузке и передаче обновлений на изолированные Серверы администрирования. Прежде чем приступить к закрытию уязвимостей, настройте изолированные Серверы администрирования (см. раздел "Настройка изолированных Серверов администрирования для закрытия уязвимостей в изолированной сети" на стр. [559](#)).

См. также:

- Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети [555](#)
- О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети.....[557](#)

Настройка изолированных Серверов администрирования для закрытия уязвимостей в изолированной сети

После того, как настройка Сервера администрирования с доступом в интернет (см. раздел "Настройка Сервера администрирования с доступом в интернет для закрытия уязвимостей в изолированной сети" на стр. [558](#)) закончена, подготовьте каждый изолированный Сервер администрирования в вашей сети, чтобы вы могли закрывать уязвимости и устанавливать обновления (см. раздел "Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети" на стр. [555](#)) на управляемых устройствах, подключенных к изолированным Серверам администрирования.

- Чтобы настроить изолированные Серверы администрирования, выполните следующие действия на каждом из них:

- Активируйте лицензионный ключ (см. раздел "Особенности лицензирования Kaspersky Security Center и управляемых приложений" на стр. [355](#)) для Системного администрирования.
- Создайте две папки (см. раздел "О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети" см. стр. [557](#)) на диске, где установлен Сервер администрирования:
 - папку, в которой появится список необходимых обновлений;
 - папку для патчей.

Названия папок могут быть любыми.

3. Предоставьте группе KLAadmins (см. раздел "Права доступа к Серверу администрирования и его объектам" на стр. 706) право *Изменение* на созданные папки, используя стандартные средства администрирования операционной системы.
4. С помощью утилиты klscflag укажите пути к папкам в свойствах Сервера администрирования.
Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

5. Введите следующие команды в командной строке Windows:

- Чтобы указать путь к папке для исправлений:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<путь к папке>"
```

- Чтобы задать путь к папке для списка необходимых обновлений:

```
klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<path to the folder>"
```

Пример: klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\FolderForPatches"

6. При необходимости с помощью утилиты klscflag укажите, как часто изолированный Сервер администрирования должен проверять наличие новых патчей:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <value in seconds>
```

По умолчанию указано значение 120 секунд.

Пример: klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150

7. При необходимости с используйте утилиту klscflag для вычисления хешей SHA256 патчей:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
```

Введя эту команду, вы можете убедиться, что патчи не были изменены при их переносе на изолированный Сервер администрирования и что вы получили корректные патчи, содержащие необходимые обновления.

По умолчанию Kaspersky Security Center не вычисляет хеши SHA256 патчей. Если включить этот параметр, после получения патчей изолированным Сервером администрирования Kaspersky Security Center вычисляет их хеши и сравнивает полученные значения с хешами, хранящимися в базе данных Сервера администрирования. Если вычисленный хеш не совпадает с хешем в базе данных, возникает ошибка и вам необходимо заменить неверные патчи.

8. Создайте задачу *Поиск уязвимостей и требуемых обновлений*, чтобы получить информацию о патчах для приложений сторонних производителей, установленных на управляемых устройствах, и настройте расписание выполнения задачи.
9. Создайте задачу *Закрытие уязвимостей*, чтобы указать патчи для приложений сторонних производителей, используемых для закрытия уязвимостей, и настройте расписание задачи.

Запустите задачи вручную, если вы хотите, чтобы они выполнялись раньше, чем указано в расписании задачи. Порядок запуска задач важен. Задачу *Закрытие уязвимостей* необходимо запустить после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

10. Перезапустите службу Сервера администрирования.

После настройки всех Серверов администрирования вы можете переместить исправления и списки необходимых обновлений (см. раздел "Передача исправлений и установка обновлений в изолированной сети" на стр. [561](#)) и закрыть уязвимости приложений сторонних производителей на управляемых устройствах в изолированной сети.

См. также:

Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети [555](#)

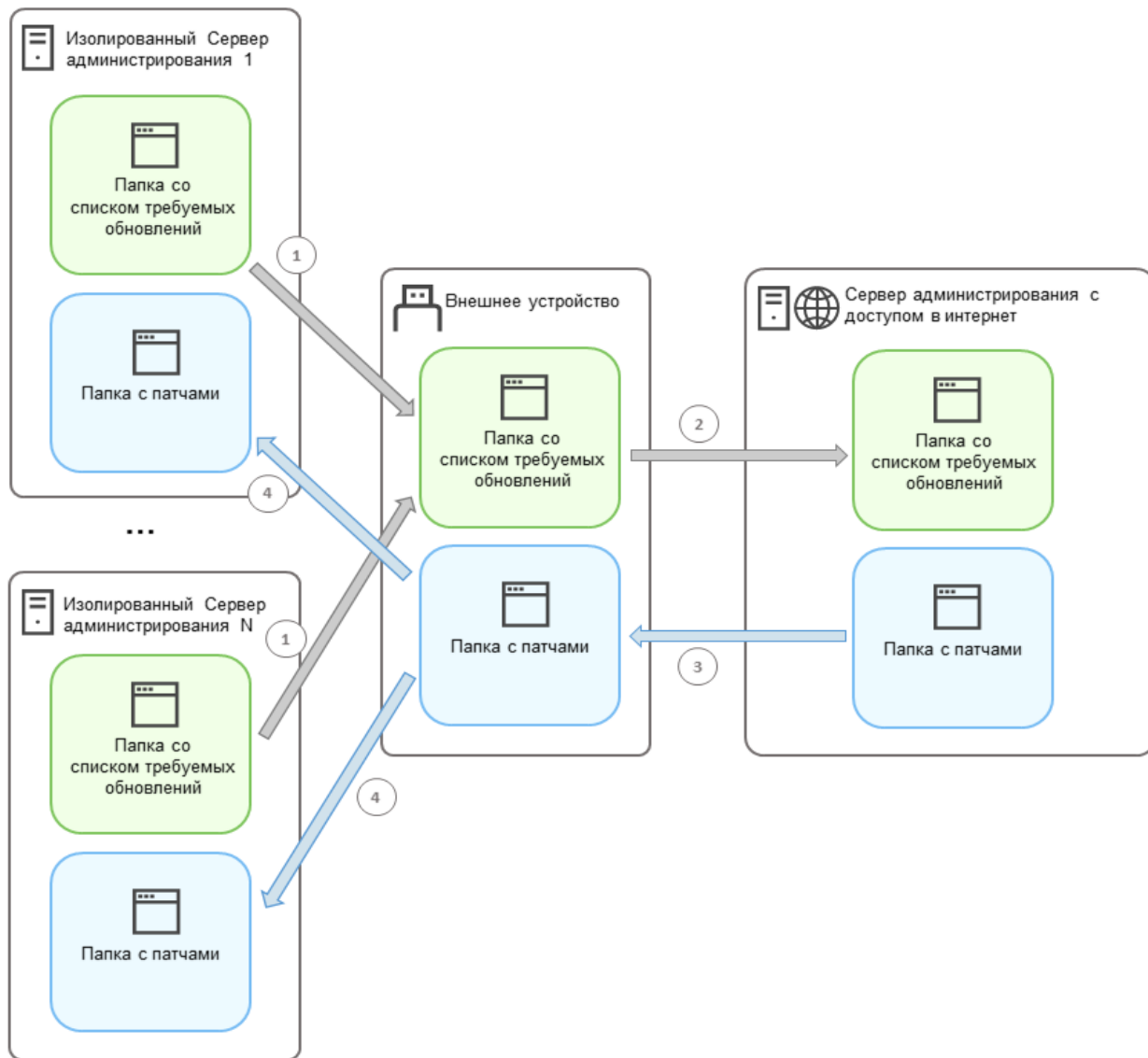
О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети.....[557](#)

Передача исправлений и установка обновлений в изолированной сети

После того, как настройка Серверов администрирования (см. раздел "Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети" на стр. [555](#)) закончена, вы можете переносить патчи с необходимыми обновлениями с Сервера администрирования, имеющего доступ интернет, на изолированные Серверы администрирования. Вы можете передавать и устанавливать обновления с нужной вам частотой, например, один или несколько раз в день.

Съемный диск, например, внешний диск, необходим, для переноса патчей и списка необходимых обновлений между Серверами администрирования. Убедитесь, что внешний диск имеет достаточно места для загрузки и хранения патчей.

Процесс передачи патчей и списка необходимых обновлений показан на рисунке и описан ниже:



► Чтобы установить обновления и закрыть уязвимости на управляемых устройствах, подключенных к изолированным Серверам администрирования:

1. Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей*, если она еще не запущена.
2. Подключите внешний диск к любому изолированному Серверу администрирования.
3. Создайте на внешнем диске две папки: одну для списка необходимых обновлений и одну для патчей. Названия папок могут быть любыми.

Если вы создали эти папки ранее, очистите их.

4. Скопируйте список необходимых обновлений с каждого изолированного Сервера администрирования и вставьте этот список в папку для списка необходимых обновлений на внешнем диске.

В результате вы объединяете все списки, полученные со всех изолированных Серверов администрирования, в одну папку. В этой папке должны находиться бинарные файлы (см. раздел "О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети" см. стр. [557](#)) с идентификаторами патчей, необходимых для всех изолированных Серверов администрирования.

5. Подключите внешний диск к Серверу администрирования с доступом в интернет.
6. Скопируйте список необходимых обновлений с внешнего диска и вставьте этот список в папку для списка необходимых обновлений на Сервере администрирования с доступом в интернет.

Все необходимые патчи автоматически загружаются из интернета в папку патчей на Сервере администрирования. Это может занять несколько часов.
7. Убедитесь, что все необходимые патчи загружены. Для этого можно выполнить одно из следующих действий:
 - Проверьте папку на наличие патчей на Сервере администрирования с доступом в интернет. Все исправления, которые были указаны в списке необходимых обновлений, должны быть загружены в нужную папку. Это удобнее, если требуется небольшое количество исправлений.
 - Подготовьте специальный скрипт, например, shell-скрипт. Если вы получите большое количество патчи, то будет сложно самостоятельно проверить, что все исправления загружены. В таких случаях лучше автоматизировать проверку.
8. Скопируйте патчи с Сервера администрирования с доступом в интернет и вставьте их в соответствующую папку на внешнем диске.
9. Перенесите исправления на каждый изолированный Сервер администрирования. Поместите патчи в специальную папку для них.

В результате каждый изолированный Сервер администрирования формирует актуальный список обновлений, необходимых для управляемых устройств, подключенных к текущему Серверу администрирования. После получения списка необходимых обновлений Сервер администрирования загружает из интернета патчи. При появлении этих патчей на изолированных Серверах администрирования задача *Установка требуемых обновлений и закрытие уязвимостей* обрабатывает патчи. Таким образом, на управляемые устройства устанавливаются обновления и закрываются уязвимости в приложениях сторонних производителей.

При выполнении задачи *Установка требуемых обновлений и закрытие уязвимостей* не перезагружайте устройство Сервера администрирования и не запускайте задачу *Резервное копирование данных Сервера администрирования* (это также вызовет перезагрузку). В результате задача *Установка требуемых обновлений и закрытие уязвимостей* прерывается, а обновления не устанавливаются. В этом случае вам необходимо перезапустить эту задачу вручную или дождаться запуска задачи по настроенному расписанию.

См. также:

- Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети [555](#)
- О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети.....[557](#)

Выключение возможности передачи исправлений и установки обновлений в изолированной сети

Вы можете выключить передачу исправлений (см. раздел "Передача исправлений и установка обновлений в изолированной сети" на стр. [561](#)) на изолированные Сервера администрирования, например, если вы решили вывести один или несколько Серверов администрирования из изолированной сети. Таким образом вы сможете уменьшить количество исправлений и время на их загрузку.

► Чтобы отключить возможность передачи патчей на изолированные Серверы администрирования:

1. Если вы хотите вывести из изоляции все Серверы администрирования, в свойствах Сервера администрирования с доступом в интернет удалите пути к папкам для патчей и список необходимых обновлений. Если вы хотите, чтобы некоторые Серверы администрирования находились в изолированной сети, пропустите этот шаг.

Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Введите следующие команды в командной строке:

- Чтобы удалить путь к папке с патчами:

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
```

- Чтобы удалить путь к папке со списком необходимых обновлений:

```
klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
```

2. Перезапустите службу Сервера администрирования, если вы удалили пути к папкам на этом Сервере администрирования.
3. В свойствах каждого Сервера администрирования, который вы хотите вывести из изоляции, удалите пути к папкам для патчей и список необходимых обновлений.

Введите следующие команды в командной строке Windows с правами администратора:

- Чтобы удалить путь к папке с патчами:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
```

- Чтобы удалить путь к папке со списком необходимых обновлений:

```
klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
```

4. Перезапустите службу каждого Сервера администрирования, на котором вы удалили пути к папкам.

Если вы перенастроили Сервер администрирования с доступом в интернет, вы больше не будете получать патчи через Kaspersky Security Center. Если вы перенастроили только некоторые изолированные Серверы администрирования, например, вынеся некоторые из них из изолированной сети, вы получите патчи только для остальных изолированных Серверов администрирования.

Если вы хотите в будущем приступить к закрытию уязвимостей на отключенных изолированных Серверах администрирования, вам необходимо настроить эти Серверы администрирования и Сервер администрирования с доступом в интернет (см. раздел "Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети" на стр. [555](#)) еще раз.

См. также:

Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети [555](#)

О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети.....[557](#)

Игнорирование уязвимостей в приложениях

Вы можете игнорировать уязвимости в приложениях и не закрывать их. Причины для игнорирования уязвимостей в приложениях могут быть, например, следующими:

- Вы не считаете, что уязвимость в приложении является критической для вашей организации.
- Вы понимаете, что закрытие уязвимости в приложениях может повредить данные приложения, для которого требуется закрыть уязвимость.
- Вы уверены, что уязвимость в приложениях не представляет опасности для сети вашей организации, так как вы используете другие меры для защиты управляемых устройств.

Вы можете игнорировать уязвимость в приложениях на всех управляемых устройствах или только на выбранных управляемых устройствах.

► Чтобы пропустить уязвимость в приложениях на всех управляемых устройствах:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.
В рабочей области папки отображается список уязвимостей в приложениях на устройствах, которые обнаружил Агент администрирования, установленный на них.
 2. Выберите уязвимость, которую вы хотите пропустить.
 3. В контекстном меню уязвимости выберите пункт **Свойства**.
Откроется окно свойств уязвимости.
 4. В разделе **Общие** выберите параметр **Игнорировать уязвимость**.
 5. Нажмите на кнопку **ОК**.
Окно свойств уязвимости в приложениях закроется.
- Уязвимость в приложениях пропускается на всех управляемых устройствах.

► Чтобы пропустить уязвимость в приложениях на выбранных управляемых устройствах:

1. Откройте окно свойств выбранного управляемого устройства (см. раздел "Параметры управляемого устройства" на стр. [782](#)) и выберите раздел **Уязвимости в приложениях**.
 2. Выберите уязвимость в приложениях.
 3. Пропустите выбранную уязвимость.
- Уязвимость в приложениях пропускается на выбранном устройстве.

Пропущенные уязвимости в приложениях не будут закрыты после завершения работы задачи *Закрытие уязвимостей* и задачи *Установка требуемых обновлений и закрытие уязвимостей*. Вы можете исключить пропущенные уязвимости в приложениях из списка уязвимостей с помощью фильтра.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Пользовательские исправления для уязвимостей в приложениях сторонних производителей

Чтобы использовать задачу *Закрытие уязвимостей*, необходимо вручную указать обновления программного обеспечения, чтобы закрыть уязвимости в приложениях сторонних производителей, перечисленные в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для других приложений сторонних производителей. *Пользовательские исправления* это обновления программного обеспечения для закрытия уязвимостей, которые администратор вручную указывает для установки.

► *Чтобы выбрать пользовательские исправления для уязвимостей в приложениях сторонних производителей:*

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.
В рабочей области папки отображается список уязвимостей в приложениях на устройствах, которые обнаружил Агент администрирования, установленный на них.
2. Выберите уязвимость для которой вы хотите указать пользовательское исправление.
3. В контекстном меню уязвимости выберите пункт **Свойства**.
Откроется окно свойств уязвимости.
4. В разделе **Пользовательские и другие исправления** нажмите на кнопку **Добавить**.
Отобразится список доступных инсталляционных пакетов. Список отобразившихся инсталляционных пакетов соответствует списку в папке **Удаленная установка** → **Инсталляционные пакеты**. Если вы не создали инсталляционный пакет, содержащий пользовательское исправление для закрытия выбранной уязвимости, вы можете создать пакет сейчас, запустив мастер создания инсталляционного пакета.
5. Выберите инсталляционный пакет (или пакеты), содержащий пользовательское исправление (или пользовательские исправления) для уязвимости приложениях сторонних производителей.
6. Нажмите на кнопку **ОК**.
Указаны инсталляционные пакеты, содержащие пользовательские исправления для уязвимости в приложениях. После запуска задачи *Закрытие уязвимостей* будет установлен инсталляционный пакет и закрыта уязвимость в приложениях.

См. также:

Об обнаружении и закрытии уязвимостей в приложениях[532](#)

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Правила установки обновлений

Для закрытия уязвимостей в приложениях (см. раздел "Закрытие уязвимостей в приложениях" на стр. [541](#)), необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, создаете ли вы правило для обновлений приложений Microsoft, приложений сторонних производителей (приложений, производимых поставщиками программного обеспечения, кроме "Лаборатории Касперского" и Microsoft) или всех приложений. При создании правила для приложений Microsoft или приложений сторонних производителей вы можете выбрать приложения и версии приложений, для которых вы хотите установить обновления. При создании правила для всех приложений вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые необходимо закрыть с помощью установки обновлений.

► Чтобы создать правило для обновления приложений:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.
Будет запущен мастер создания правила. Следуйте далее указаниям мастера.
2. На странице **Тип правила** выберите **Правило для всех обновлений**.
3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:

- **Набор обновлений для установки**

Выберите обновления, которые должны быть установлены на клиентские устройства:

- **Устанавливать только утвержденные обновления.** В этом случае устанавливаются только одобренные обновления.
- **Устанавливать все обновления, кроме отклоненных.** В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
- **Устанавливать все обновления, включая отклоненные.** В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Обновления** выберите обновления для установки:
 - **Устанавливать все подходящие обновления**

В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

- **Устанавливать только обновления из списка**

В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные приложения или чтобы обновить только требуемые приложения.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

По умолчанию параметр включен.

1. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

- **Закрывать все уязвимости, соответствующие остальным критериям**

В этом случае будут закрыты все уязвимости программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

- **Закрывать только уязвимости из списка**

Закрывать только уязвимости, которые выбраны вручную в списке. Этот список содержит все обнаруженные уязвимости.

Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных приложениях или чтобы закрыть уязвимости только в требуемых приложениях.

1. В окне **Имя** укажите название создаваемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило создастся и отобразится в поле **Задать правила установки обновлений** мастера создания задачи.

► Чтобы создать правило обновления приложений Microsoft:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.

Будет запущен мастер создания правила. Следуйте далее указаниям мастера.

2. На странице **Тип правила** выберите **Правило для обновлений Windows Update**.

3. На странице **Общие критерии** укажите следующие параметры:

- **Набор обновлений для установки**

Выберите обновления, которые должны быть установлены на клиентские устройства:

- **Устанавливать только утвержденные обновления.** В этом случае устанавливаются только одобренные обновления.
- **Устанавливать все обновления, кроме отклоненных.** В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
- **Устанавливать все обновления, включая отклоненные.** В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.
2. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.

3. В окне **Имя** укажите название создаваемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило создается и отображается в поле **Задайте правила установки обновлений** мастера создания задачи.

► Чтобы создать правило для обновления приложений сторонних производителей:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.
Будет запущен мастер создания правила. Следуйте далее указаниям мастера.
2. На странице **Тип правила** выберите **Правило для сторонних обновлений**.
3. На странице **Общие критерии** укажите следующие параметры:

- **Набор обновлений для установки**

Выберите обновления, которые должны быть установлены на клиентские устройства:

- **Устанавливать только утвержденные обновления.** В этом случае устанавливаются только одобренные обновления.
- **Устанавливать все обновления, кроме отклоненных.** В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
- **Устанавливать все обновления, включая отклоненные.** В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.
2. В окне **Имя** укажите название создаваемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило создается и отображается в поле **Задайте правила установки обновлений** мастера создания задачи.

См. также:

Одобрение и отклонение обновлений программного обеспечения	505
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей	529

Группы приложений

В этом разделе описана работа с группами приложений, установленных на устройствах.

Создание категорий приложений

Kaspersky Security Center позволяет создавать категории приложений, установленных на устройствах.

Категории приложений можно создавать следующими способами:

- Администратор указывает папку, исполняемые файлы из которой попадают в выбранную категорию.
- Администратор указывает устройство, исполняемые файлы с которого попадают в выбранную категорию.
- Администратор задает критерии, по которым приложения попадают в выбранную категорию.

Когда категория приложений создана, администратор может задать правила для этой категории приложений. Правила определяют поведение приложений, входящих в указанную категорию. Например, можно запретить или разрешить запуск приложений, входящих в категорию.

Управление запуском приложений на устройствах

Kaspersky Security Center позволяет управлять запуском приложений на устройствах в режиме "Список разрешенных". Подробное описание приведено в онлайн-справке Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>. В режиме "Список разрешенных" на выбранных устройствах разрешен запуск только тех приложений, которые входят в указанные категории. Администратор может просматривать результаты статического анализа правил запуска приложений на устройствах по каждому пользователю.

Инвентаризация программного обеспечения, установленного на устройствах

Kaspersky Security Center позволяет выполнять инвентаризацию программного обеспечения на устройствах под управлением Windows и Linux. Агент администрирования получает информацию обо всех приложениях, установленных на устройствах (см. раздел "Просмотр реестра приложений" на стр. [585](#)). Информация, полученная в результате инвентаризации, отображается в рабочей области папки **Реестр приложений**. Администратор может просматривать подробную информацию о каждом приложении, в том числе версию и производителя.

Количество исполняемых файлов, получаемых от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

Управление группами лицензионных приложений

Kaspersky Security Center позволяет создавать группы лицензионных приложений. В группу лицензионных приложений входят приложения, отвечающие критериям, заданным администратором. Администратор может указывать следующие критерии для групп лицензионных приложений:

- Название приложения.
- Версия приложения.
- Производитель.
- Тег приложения.

Приложения, соответствующие одному или нескольким критериям, автоматически попадают в группу. Для создания группы лицензионных приложений должен быть задан хотя бы один критерий включения приложений в эту группу.

Каждая группа лицензионных приложений имеет свой лицензионный ключ. Лицензионный ключ группы лицензионных приложений определяет допустимое количество установок для приложений, входящих в группу. Если количество установок превысило заданное в лицензионном ключе ограничение, на Сервере администрирования регистрируется информационное событие. Администратор может указать дату окончания действия лицензионного ключа. При наступлении этой даты на Сервере администрирования регистрируется информационное событие.

Просмотр информации об исполняемых файлах

Kaspersky Security Center получает всю информацию об исполняемых файлах, которые запускались на устройствах с момента установки на них операционной системы. Полученная информация об исполняемых файлах отображается в главном окне приложения в рабочей области папки **Исполняемые файлы**.

Использование компонента Контроль приложений для управления исполняемыми файлами

Вы можете использовать компонент Контроль приложений, чтобы разрешить или запретить запуск исполняемых файлов на пользовательских устройствах. Компонент Контроль приложений поддерживает операционные системы Windows и Linux.

Для операционных систем Linux компонент Контроль приложений доступен, начиная с Kaspersky Endpoint Security 11.2 для Linux.

Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux создана и активна.

Этапы

Сценарий использования компонента Контроль приложений состоит из следующих этапов:

а. Формирование и просмотр списка исполняемых файлов на клиентских устройствах

Этот этап помогает вам определить, какие исполняемые файлы обнаружены на управляемых устройствах. Просмотрите список исполняемых файлов и сравните его со списками разрешенных и запрещенных исполняемых файлов. Ограничения использования исполняемых файлов могут быть связаны с политиками информационной безопасности в вашей организации.

Инструкции:

- Консоль администрирования: Инвентаризация исполняемых файлов (на стр. [589](#)).

- Kaspersky Security Center Web Console: Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах.

b. Создание категорий для исполняемых файлов, используемых в вашей организации

Проанализируйте списки исполняемых файлов, хранящихся на управляемых устройствах. На основе анализа сформируйте категории для исполняемых файлов. Рекомендуется создать категорию "Рабочие приложения", которая охватывает стандартный набор исполняемых файлов, используемых в вашей организации. Если разные группы безопасности используют свои наборы исполняемых файлов в своей работе, для каждой группы безопасности можно создать отдельную категорию.

Инструкции:

- Консоль администрирования: Создание пополняемой вручную категории приложений (на стр. [575](#)), Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств (на стр. [577](#)), Создание категории приложений, в которую входят исполняемые файлы из указанных папок (на стр. [579](#)).
- Kaspersky Security Center Web Console: Создание пополняемой вручную категории приложений, Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств, Создание категории приложений, в которую входят исполняемые файлы из указанных папок.

c. Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security

Настройте компонент Контроль приложений в политике Kaspersky Endpoint Security с использованием категорий, которые вы создали на предыдущем этапе.

Инструкции:

- Консоль администрирования: Настройка управления запуском приложений на клиентских устройствах (на стр. [583](#)).
- Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows.

d. Включение компонента Контроль приложений в тестовом режиме

Чтобы правила Контроля приложений не блокировали исполняемые файлы, необходимые для работы пользователей, рекомендуется включить тестирование правил Контроля приложений и проанализировать их работу после создания правил. Когда тестирование включено, Kaspersky Endpoint Security для Windows не будет блокировать исполняемые файлы, запуск которых запрещен правилами Контроля приложений, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

При тестировании правил Контроля приложений рекомендуется выполнить следующие действия:

- Определите период тестирования. Период тестирования может варьироваться от нескольких дней до двух месяцев.
- Изучите события, возникающие в результате тестирования работы компонента Контроль приложений.

Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

e. Изменение параметров категорий компонента Контроль приложений

Если требуется, измените параметры компонента Контроль приложений. На основании результатов тестирования вы можете добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию пополняемую вручную.

Инструкции:

- Консоль администрирования: Добавление исполняемых файлов, связанных с событием, в категорию приложений (на стр. [581](#)).
- Kaspersky Security Center Web Console: Добавление исполняемых файлов, связанных с событием, в категорию приложений.

f. Применение правил Контроля приложений в рабочем режиме

После проверки правил Контроля приложений и завершения настройки категорий вы можете применить правила Контроль приложений в рабочем режиме.

Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

g. Проверка конфигурации Контроля приложений

Убедитесь, что вы выполнили следующее:

- Создали категории для исполняемых файлов.
- Настроили Контроль приложений с использованием категорий.
- Применили правила Контроля приложений в рабочем режиме.

Результаты

После завершения сценария, запуск исполняемых файлов на управляемых устройствах контролируется. Пользователи могут запускать только те исполняемые файлы, которые разрешены в вашей организации, и не могут запускать исполняемые файлы, запрещенные в вашей организации.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>
- Справка Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/>
- Kaspersky Security для виртуальных сред Легкий агент <https://support.kaspersky.com/KSVLA/5.2/en-US/145134.htm>

Создание категорий приложений

► Чтобы создать категорию приложений, выполните следующие действия:

1. В дереве консоли в папке **Управление приложениями** выберите вложенную папку **Категории приложений**.
2. По кнопке **Создать категорию** запустите мастер создания пользовательской категории.
3. В окне мастера выберите тип пользовательской категории:
 - **Пополняемая вручную категория.** Задайте критерии, по которым исполняемые файлы будут попадать в создаваемую категорию.
 - **Автоматически пополняемая категория.** Укажите папку, исполняемые файлы из которой будут автоматически попадать в создаваемую категорию.

При создании автоматически пополняемой категории приложений выполняет инвентаризацию следующих форматов файлов: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, SCR.

- **Категория, в которую входят исполняемые файлы с выбранных устройств.** Укажите устройство, исполняемые файлы которого должны попадать в категорию автоматически.

4. Следуйте указаниям мастера.

В результате работы мастера создается пользовательская категория приложений. Просмотреть созданные категории можно в списке категорий в рабочей области папки **Категории приложений**.

Категории приложений используются компонентом Контроль приложений, который входит в состав приложения защиты Kaspersky Endpoint Security для Windows. Компонент Контроль приложений позволяет администратору установить ограничения на запуск приложений на клиентских устройствах, например, на основании приложений, которые входят в выбранную категорию.

Создание пополняемой вручную категории приложений

Вы можете указать набор критериев в качестве шаблона для исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов, соответствующих критериям, вы можете создать категорию приложений и использовать ее в настройке компонента Контроль приложений.

► Чтобы создать пополняемую вручную категорию приложений:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите подпапку **Категории приложений**.
2. Нажмите на кнопку **Новая категория**.
Запустите мастер **Мастер создания категории**. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На странице мастера **Тип категории** выберите тип пользовательской категории **Пополняемая вручную категория**.
4. На странице мастера **Название категории приложений** введите новое имя категории приложений.
5. На странице **Настройка условий для включения приложений в категории** нажмите на кнопку **Добавить**.
6. В раскрывающемся списке задайте необходимые вам параметры:
 - **Из списка исполняемых файлов**
Если выбран этот вариант, приложения для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.
 - **Из свойств файла**
Если выбран этот вариант, можно вручную указать детальные данные исполняемых файлов, которые будут добавлены в пользовательскую категорию приложений.
 - **Метаданные файлов папки**
Укажите папку на клиентском устройстве, которая содержит исполняемые файлы. Метаданные исполняемых файлов, входящих в указанную папку, будут передаваться на Сервер администрирования. Исполняемые файлы, имеющие

такие же метаданные, будут добавлены в пользовательскую категорию приложений.

- **Хеши файлов папки**

Если выбран этот вариант, можно выбрать или создать папку на клиентском устройстве. Хеш файлов, содержащихся в указанной папке, будет передаваться на Сервер администрирования. Приложения, имеющие такой же хеш, как и файлы в указанной папке, будут добавлены в пользовательскую категорию приложений.

- **Сертификаты файлов из папки**

Если выбран этот вариант, можно указать папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Сертификаты исполняемых файлов считываются и добавляются в условия категории. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Метаданные файлов установщика MSI**

Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика приложения будут передаваться на Сервер администрирования. Приложения, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию приложений.

- **Контрольные суммы файлов msi-инсталлятора приложения**

Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать файл установщика MSI. Хеш файлов установщика приложения будет передаваться на Сервер администрирования. Приложения, у которых хеш файлов установщика MSI совпадает с указанным, будут добавлены в пользовательскую категорию приложения.

- **Из KL-категории**

Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". Приложения, входящие в указанную KL-катеорию, будут добавлены в пользовательскую категорию приложений.

- **Задайте путь к приложению (поддерживаются маски)**

Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию приложений.

- **Выберите сертификат из хранилища сертификатов**

Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Тип носителя**

Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск приложения. Приложения, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию приложений.

7. На странице мастера **Создание категории приложений** нажмите на кнопку **Готово**.

Kaspersky Security Center работает с метаданными только из тех файлов, которые содержат цифровую подпись. Невозможно создать категорию на основе метаданных файлов, не содержащих цифровой подписи.

В результате работы мастера будет создана пользовательская категория приложений, пополняемая вручную. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории приложений**.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств

Вы можете использовать исполняемые файлы с устройства как шаблон исполняемых файлов, запуск которых вы хотите разрешить или запретить. На основе исполняемых файлов с выбранных устройств вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

► Чтобы получить список исполняемых файлов с устройств:

1. Убедитесь, что политика Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux создана и активна. Включите в политике компонент Контроль приложений.
2. Получение списка исполняемых файлов, хранящихся на клиентских устройствах.

► Чтобы создать категорию приложений, в которую входят исполняемые файлы с выбранных устройств:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите подпапку **Категории приложений**.
2. Нажмите на кнопку **Новая категория**.
Запустите мастер **Мастер создания категории**. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На странице мастера **Тип категории** выберите тип пользовательской категории **Категория приложений, в которую входят исполняемые файлы из выбранных устройств**.
4. На странице мастера **Название категории приложений** введите новое имя категории приложений.
5. На странице мастера **Параметры** нажмите на кнопку **Добавить**.
6. Выберите устройство или устройства, чьи исполняемые файлы будут использоваться для создания категории приложений.
7. Задайте следующие параметры:

- **Алгоритм вычисления хеш-функции**

В зависимости от версии приложения защиты, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center для файлов категории:

- Если в вашей сети установлены версии приложений защиты Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою приложения защиты. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.
- Если в вашей сети установлены версии приложений защиты ниже версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows, установите флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**. Добавить категорию, созданную по критерию MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.
- Если на разных устройствах в вашей сети используются новые и ранние версии приложений защиты Kaspersky Endpoint Security 10, установите оба флажка, и **Вычислять SHA-256 для файлов в категории**, и **Вычислять MD5 для файлов в категории**.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Синхронизировать данные с хранилищем Сервера администрирования**

Выберите этот параметр, если вы хотите, чтобы Сервер администрирования периодически выполнял проверку изменений в указанной папке (или папках).

По умолчанию параметр выключен.

Если вы включите этот параметр, укажите период (в часах), чтобы проверять изменения в указанной папке (папках). По умолчанию период проверки равен 24 часам.

1. На странице мастера **Фильтр** укажите следующие параметры:

- **Тип файла**

В этом разделе вы можете указать тип файла, который используется для создания категории приложений.

Все файлы. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.

Только файлы вне категорий приложений. Для создаваемой категории учитываются только файлы вне категорий приложений.

- **Папки**

В этом разделе вы можете указать папки выбранных устройств, содержащие файлы, которые используются для создания категории приложений.

Все папки. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.

Указанная папка. Для создаваемой категории учитывается только указанная папка. Если вы выбирали этот параметр, вам нужно указать путь к папке.

1. На странице мастера **Создание категории приложений** нажмите на кнопку **Готово**.

После завершения мастера создается пользовательская категория приложений. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории приложений**.

Создание категории приложений, в которую входят исполняемые файлы из указанных папок

Вы можете использовать исполняемые файлы выбранных папок как эталонный набор исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов из выбранных папок вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

► Чтобы создать категорию приложений, в которую входят исполняемые файлы из указанных папок:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите подпапку **Категории приложений**.
2. Нажмите на кнопку **Новая категория**.
Запустите мастер **Мастер создания категории**. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На странице мастера **Тип категории** выберите тип пользовательской категории **Категория приложений, в которую входят исполняемые файлы из указанных папок**.
4. На странице мастера **Название категории приложений** введите новое имя категории приложений.
5. На странице мастера **Папка хранилища** нажмите на кнопку **Обзор**.
6. Укажите папку, исполняемые файлы которой будут использоваться для создания категории приложений.
7. Настройте следующие параметры:
 - **Включать в категорию динамически подключаемые библиотеки (DLL)**
В категорию приложений включаются динамически подключаемые библиотеки

(файлы формата DLL), и компонент Контроль приложений регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center.

По умолчанию флажок снят.

- **Включать в категорию данные о скриптах**

В категорию приложений включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center.

По умолчанию флажок снят.

- Алгоритм вычисления хеш-функции: **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше) / Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**

В зависимости от версии приложения защиты, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center для файлов категории:

- Если в вашей сети установлены версии приложений защиты Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою приложения защиты. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.
- Если в вашей сети установлены версии приложений защиты ниже версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows, установите флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**. Добавить категорию, созданную по критерию MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.
- Если на разных устройствах в вашей сети используются новые и ранние версии приложений защиты Kaspersky Endpoint Security 10, установите оба флажка, и **Вычислять SHA-256 для файлов в категории, и Вычислять MD5 для**

файлов в категории.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории** (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше) установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории** (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows) снят.

- **Принудительно проверять папку на наличие изменений**

Если этот параметр включен, приложение периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

По умолчанию параметр выключен.

8. На странице мастера **Создание категории приложений** нажмите на кнопку **Готово**.

После завершения мастера создается пользовательская категория приложений. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории приложений**.

Добавление исполняемых файлов, связанных с событием, в категорию приложений

Вы можете добавить исполняемые файлы, связанные с событиями **Запуск программы запрещен** и **Запуск программы запрещен в тестовом режиме**, в существующую категорию программ, пополняемую вручную, или в новую категорию программ.

► *Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. На вкладке **События** выберите нужное вам событие.
4. В контекстном меню события выберите пункт **Добавить в категорию**.
5. В открывшемся окне **Действие с исполняемым файлом, связанным с событием** задайте требуемые параметры:

Выберите один из следующих вариантов:

- **Добавить в новую категорию приложений**

Выберите этот вариант, если необходимо создать новую категорию приложений.

Нажмите на кнопку **ОК**, чтобы запустить мастер создания пользовательской категории. В результате работы мастера будет создана категория с указанными параметрами.

По умолчанию вариант не выбран.

- **Добавить в существующую категорию**

Выберите этот вариант, если необходимо добавить правила в существующую категорию приложений. Выберите необходимую категорию в списке категорий приложений.

По умолчанию этот вариант выбран.

В блоке **Тип правила** выберите параметры:

- **Добавить в категорию**

Выберите этот вариант, если необходимо добавить правила в условия категории приложений.

По умолчанию этот вариант выбран.

- **Правила для добавления в исключения**

Выберите этот вариант, если необходимо добавить правила в исключения категории приложений.

В блоке **Тип информации о файле** выберите один из параметров:

- **Данные сертификата (или SHA256 для файлов без сертификата)**

Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложений или несколько приложений одного производителя.

Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA-256 для файлов без сертификата.

По умолчанию этот вариант выбран.

- **Данные сертификата (файлы без сертификата пропускаются)**

Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложений или несколько приложений одного производителя.

Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

- **Только SHA256 (файлы без хеша пропускаются)**

Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA-256 исполняемого файла.

- **MD5 (устаревший режим, только для версий Kaspersky Endpoint Security 10 Service Pack 1)**

Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции MD5 исполняемого файла. Вычисление хеш-функции MD5 поддерживается для версий Kaspersky Endpoint Security 10 Service Pack 1 для Windows и ниже.

6. Нажмите на кнопку **ОК**.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Настройка управления запуском приложений на клиентских устройствах

Категоризация приложений позволяет оптимизировать процесс управления запуском приложений на устройствах. Вы можете создать категорию приложений и настроить компонент Контроль приложений политики так, что на устройствах, на которых применена эта политика, будут запускаться только приложения из указанной категории. Например, вы создали категорию, которая содержит приложения *Приложение_1* и *Приложение_2*. После добавления этой категории в политику, на устройствах, к которым применена эта политика, будет разрешен запуск только двух приложений, *Приложение_1* и *Приложение_2*. Если пользователь попытается запустить приложение, которое не входит в категорию, например, *приложение_3*, то запуск такого приложения будет заблокирован. Пользователю будет отображено сообщение о том, что запуск *Приложения_3* запрещен в соответствии с правилом Контроля приложений. Вы можете создать автоматически пополняемую категорию на основе различных критериев, входящих в указанную папку. В этом случае файлы будут автоматически добавляться в категорию из указанной папки. Исполняемые файлы приложений копируются в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию.

► *Чтобы настроить управление запуском приложений на клиентских устройствах:*

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Категории приложений**.
2. В рабочей области папки **Категории приложений** создайте категории приложений (см. раздел "Создание категорий приложений" на стр. [574](#)), запуском которых вы хотите управлять.
3. Чтобы создать политику (см. раздел "Создание политики" см. стр. [435](#)) для приложения Kaspersky Endpoint Security для Windows, в папке **Управляемые устройства** на вкладке **Политики** нажмите на кнопку **Новая политика** и следуйте указаниям мастера.

Если такая политика уже существует, этот шаг можно пропустить. Управление запуском приложений в указанной категории можно настроить в параметрах этой политики. Созданная политика отображается в папке **Управляемые устройства** на вкладке **Политики**.

4. В контекстном меню политики для приложения Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.

Откроется окно свойств политики Kaspersky Endpoint Security для Windows.

5. В окне свойств политики Kaspersky Endpoint Security для Windows, в разделе **Контроль безопасности** → **Контроль приложений** установите флажок **Контроль приложений**.

- Нажмите на кнопку **Добавить**.

Откроется окно **Правило Контроля приложений**.

- В окне **Правило Контроля приложений** в раскрывающемся списке **Категория** выберите категорию приложений, на которую будет распространяться правило запуска. Настройте параметры правила запуска для выбранной категории приложений.

Для приложений версий Kaspersky Endpoint Security для Windows 10 Service Pack 2 и выше категории, созданные по критерию MD5-хеша исполняемого файла, приложения не отображаются.

Не рекомендуется добавлять категорию, созданную по критерию SHA256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2. Это может привести к сбою приложения.

Подробные инструкции по настройке правил контроля приведены в онлайн-справке Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>.

- Нажмите на кнопку **ОК**.

Запуск приложений на устройствах, входящих в указанную категорию, будет выполняться согласно созданному правилу. Созданное правило отображается в окне свойств политики Kaspersky Endpoint Security для Windows в разделе **Контроль приложений**.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Просмотр результатов статического анализа правил запуска исполняемых файлов

- *Чтобы просмотреть информацию о том, запуск каких исполняемых файлов запрещен пользователям:*

- В дереве консоли в папке **Управляемые устройства** выберите вложенную папку **Политики**.
- В контекстном меню политики для приложения Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.

Откроется окно свойств политики приложения.

- В окне свойств политики в панели **Разделы** выберите раздел **Контроль безопасности**, а затем подраздел **Контроль приложений**.
- Нажмите на кнопку **Статический анализ**.

Откроется окно **Анализ списка прав доступа**. В левой части окна отображается список пользователей, основанный на данных Active Directory.

- Выберите в списке пользователя.

В правой части окна отобразятся категории приложений, назначенные этому пользователю.

- Чтобы просмотреть исполняемые файлы, запуск которых запрещен пользователю, в окне **Анализ списка прав доступа** нажмите на кнопку **Просмотреть файлы**.

Откроется окно, в котором отображается список исполняемых файлов, запуск которых запрещен пользователю.

- Чтобы просмотреть список исполняемых файлов, входящих в категорию, выберите категорию приложений и нажмите на кнопку **Просмотреть файлы категории**.

В открывшемся окне отображается список исполняемых файлов, входящих в категорию приложений.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Просмотр реестра приложений

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, которое установлено на управляемых устройствах.

Агент администрирования составляет список приложений, установленных на устройстве с операционной системой Windows или Linux, и передает список Серверу администрирования. Для клиентских устройств с операционной системой Windows Агент администрирования получает большую часть информации об установленных приложениях из реестра Windows. Для клиентских устройств с операционной системой Linux информацию об установленных приложениях Агент администрирования получает от диспетчеров пакетов.

► *Чтобы просмотреть реестр установленных на клиентских устройствах приложений,*

В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Реестр приложений**.

В рабочей области папки **Реестр приложений** отображается список приложений, установленных на клиентских устройствах и Сервере администрирования.

Вы можете просмотреть подробную информацию о любом приложении, выбрав в контекстном меню этого приложения пункт **Свойства**. В окне свойств приложения отображается общая информация о приложении и информация об исполняемых файлах приложения, а также список устройств, на которых установлено приложение.

В контекстном меню любого приложения вы можете:

- добавить это приложение в категорию приложений;
- назначить тег приложению;
- экспортировать список приложений в файлы форматов CSV или TXT;
- просмотреть свойства приложения, например имя производителя, номер версии, список исполняемых файлов, список устройств, на которых установлено приложение, список доступных обновлений программного обеспечения или список обнаруженных уязвимостей программного обеспечения.

Для просмотра приложений, удовлетворяющих определенным критериям, вы можете воспользоваться полями фильтрации в рабочей области папки **Реестр приложений**.

В окне свойств выбранного устройства (см. раздел "Параметры управляемого устройства" на стр. [782](#)) в разделе **Реестр приложений** вы можете просмотреть список приложений, установленных на устройстве.

Генерирование отчета об установленных приложениях

В рабочей области папки **Реестр приложений** вы также можете нажать на кнопку **Просмотреть отчет об установленных приложениях**, чтобы сгенерировать отчет, содержащий информацию об установленных приложениях, включая количество устройств, на которых установлено каждое приложение. Отчет, который открывается на странице **Отчет об установленных приложениях**, содержит информацию о приложениях "Лаборатории Касперского" и о приложениях сторонних производителей. Если вам нужна информация только о приложениях "Лаборатории Касперского", установленных на клиентских устройствах, в списке **Сводная информация** выберите "Лаборатория Касперского".

Информация о приложениях "Лаборатории Касперского" и других производителей на устройствах, подключенных к подчиненным и виртуальным Серверам администрирования, также хранится в реестре приложений главного Сервера администрирования. После добавления данных с подчиненных и виртуальных Серверов нажмите на кнопку **Просмотреть отчет об установленных приложениях**, и на открывшейся странице **Отчет об установленных приложениях** вы можете просмотреть эту информацию.

► *Чтобы добавить информацию с подчиненных и виртуальных Серверов администрирования в отчет об установленных приложениях:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. На вкладке **Отчеты** выберите **Отчет об установленных приложениях**.
4. В контекстном меню отчета выберите пункт **Свойства**.

Откроется окно **Свойства: Отчет об установленных приложениях**.

5. В разделе **Иерархия Серверов администрирования** установите флажок **Включать данные подчиненных и виртуальных Серверов администрирования**.
6. Нажмите на кнопку **ОК**.

В результате информация с подчиненных и виртуальных Серверов администрирования будет включена в **Отчет об установленных приложениях**.

См. также:

Мониторинг установки и удаления приложений	636
Использование компонента Контроль приложений для управления исполняемыми файлами	572
Основной сценарий установки	56

Изменение времени начала инвентаризации программного обеспечения

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Windows.

Агент администрирования составляет список приложений, установленных на устройстве, и передает список Серверу администрирования. Агент администрирования автоматически получает информацию об установленных приложениях из реестра Windows.

Чтобы сохранить ресурсы устройства, по умолчанию Агент администрирования начинает получать информацию об установленных приложениях через 10 минут после запуска службы Агента администрирования.

► *Чтобы изменить время начала инвентаризации программного обеспечения устройства после запуска службы Агента администрирования:*

1. Откройте системный реестр устройства, на котором установлен Агент администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
 - для 32-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
 - для 64-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
3. Для ключа KLINV_INV_COLLECTOR_START_DELAY_SEC установите нужное вам значение в секундах.
По умолчанию указано значение 600 секунд.
4. Перезапустите службу Агента администрирования.

В результате время начала инвентаризации программного обеспечения после запуска службы Агента администрирования изменится.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Окно Информация о группе лицензионных программ

В этом окне можно задать критерии включения обнаруженных приложений в группу лицензионных приложений.

Название группы лицензионных программ

Отслеживать нарушение ограничений

Критерии включения обнаруженных программ в эту группу лицензионных программ

Добавить

Просмотреть подходящие программы

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Создание групп лицензионных приложений

► Чтобы создать группу лицензионных приложений:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Учет сторонних лицензий**.
2. По кнопке **Добавить группу лицензионных приложений** запустите Мастер добавления группы лицензионных приложений.
Запускается Мастер добавления группы лицензионных приложений.
3. На шаге **Информация о группе лицензионных приложений** укажите, какие приложения вы хотите включить в группу приложений:
 - **Название группы лицензионных приложений**
 - **Отслеживать нарушение ограничений**
 - **Критерии включения обнаруженных приложений в эту группу лицензионных приложений**
4. На шаге **Введите данные о имеющихся лицензионных ключах** укажите лицензионные ключи, которые вы хотите отслеживать. Выберите параметр **Контролировать нарушение заданных лицензионных ограничений** и добавьте лицензионные ключи:
 - a. Нажмите на кнопку **Добавить**.
 - b. Выберите лицензионный ключ, который нужно добавить, и нажмите на кнопку **ОК**. Если необходимый лицензионный ключ отсутствует в списке, нажмите на кнопку **Добавить** и укажите свойства лицензионного ключа (см. раздел "Управление лицензионными ключами для групп лицензионных приложений" на стр. [588](#)).
5. На шаге **Добавление группы лицензионных приложений** нажмите на кнопку **Готово**.
Группа лицензионных приложений создана и отображается в папке **Учет сторонних лицензий**.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Управление лицензионными ключами для групп лицензионных приложений

► Чтобы создать лицензионный ключ для группы лицензионных приложений:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Учет сторонних лицензий**.
2. Нажмите на кнопку **Управлять лицензионными ключами лицензионных приложений** в рабочей области папки **Учет сторонних лицензий**.
Откроется окно **Управление лицензионными ключами лицензионных приложений**.

3. В окне **Управление лицензионными ключами лицензионных приложений** нажмите на кнопку **Добавить**.

Откроется окно **Лицензионный ключ**.

4. В окне **Лицензионный ключ** укажите свойства лицензионного ключа и ограничения, которые этот лицензионный ключ накладывает на группу лицензионных приложений.
 - **Название.** Название лицензионного ключа.
 - **Комментарий.** Примечания к выбранному лицензионному ключу.
 - **Ограничение.** Количество устройств, на которых может быть установлено приложение, использующая этот лицензионный ключ.
 - **Действителен до.** Дата окончания срока действия лицензионного ключа.

Созданные лицензионные ключи отображаются в окне **Управление лицензионными ключами лицензионных приложений**.

► *Чтобы применить лицензионный ключ к группе лицензионных приложений:*

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Учет сторонних лицензий**.
2. В папке **Учет сторонних лицензий** выберите группу лицензионных приложений, к которой вы хотите применить лицензионный ключ.
3. В контекстном меню группы лицензионных приложений выберите пункт **Свойства**.

Откроется окно свойств группы лицензионных приложений.

4. В окне свойств группы лицензионных приложений в разделе **Лицензионные ключи** выберите вариант **Контролировать нарушение заданных лицензионных ограничений**.

5. Нажмите на кнопку **Добавить**.

Откроется окно **Выбор лицензионного ключа**.

6. В окне **Выбор лицензионного ключа** выберите лицензионный ключ, который вы хотите применить к группе лицензионных приложений.

7. Нажмите на кнопку **ОК**.

Ограничения для группы лицензионных приложений, указанные в лицензионном ключе, будут распространены на выбранную группу лицензионных приложений.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Инвентаризация исполняемых файлов

Вы можете получить список исполняемых файлов, хранящихся на управляемых устройствах. Для инвентаризации исполняемых файлов вам нужно создать задачу инвентаризации.

Функция инвентаризации исполняемых файлов доступна для следующих приложений:

- Kaspersky Endpoint Security для Windows

- Kaspersky Endpoint Security для Linux
- Kaspersky Security для виртуальных сред 4.0 Легкий агент и выше

Количество исполняемых файлов, получаемых от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

Прежде чем начать, включите уведомления о запуске приложений в политике Kaspersky Endpoint Security и в политике Агента администрирования, чтобы можно было передавать данные на Сервер администрирования.

► *Чтобы включить уведомления о запуске приложения:*

- Откройте параметры политики Kaspersky Endpoint Security и выполните следующие действия:
 1. Перейти к **Общие параметры** → **Отчеты и хранилища**.
 2. В разделе **Передача данных на Сервер администрирования**, установите флажок **О запускаемых приложениях**.
 3. Сохраните изменения.
- Откройте параметры политики Агента администрирования и выполните следующие действия:
 1. Перейти в раздел **Хранилища**.
 2. Установите флажок **Информация об установленных приложениях**.
 3. Сохраните изменения.

► *Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:*

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Новая задача** нажмите на кнопку **Задачи**.
Запустится мастер создания задачи.
3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Инвентаризация** и нажмите на кнопку **Далее**.
4. Следуйте дальнейшим шагам мастера.

В результате работы мастера создается задача инвентаризации для Kaspersky Endpoint Security. Созданная задача отображается в списке задач в рабочей области папки **Задачи**.

Список исполняемых файлов, обнаруженных на устройствах в результате выполнения инвентаризации, отображается в рабочей области папки **Исполняемые файлы**.

При выполнении инвентаризации приложение обнаруживает исполняемые файлы следующих форматов: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, а также HTML-файлы.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Просмотр информации об исполняемых файлах

- *Чтобы просмотреть список всех исполняемых файлов, обнаруженных на клиентских устройствах,*

В дереве консоли в папке **Управление приложениями** выберите вложенную папку **Исполняемые файлы**.

В рабочей области папки **Исполняемые файлы** отображается список исполняемых файлов, которые запускались на устройствах или были обнаружены в процессе работы задачи инвентаризации Kaspersky Endpoint Security для Windows.

Для просмотра данных об исполняемых файлах, удовлетворяющих определенным критериям, вы можете воспользоваться фильтрацией.

- *Чтобы просмотреть свойства исполняемого файла,*

в контекстном меню файла выберите пункт **Свойства**.

Откроется окно, содержащее информацию об исполняемом файле, а также список устройств, на которых присутствует исполняемый файл.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Мониторинг и отчеты

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky Security Center. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky Security Center можно настраивать функции мониторинга и параметры отчетов.

- Индикаторы

В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Security Center и управляемых устройств с помощью цветowych индикаторов.

- Статистика

Статистическая информация о состоянии системы защиты и управляемых устройств отображается в виде настраиваемых информационных панелей.

- Отчеты

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

- События

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события, Отказы функционирования, Предупреждения и Информационные события.**
- Время: **Последние события.**
- Тип: **Запросы пользователей и События аудита.**

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center Web Console.

В этом разделе

Сценарий: мониторинг и отчеты	593
Мониторинг цветowych индикаторов и зарегистрированных событий в Консоли администрирования	595
Работа с отчетами, статистикой и уведомлениями	601
Мониторинг установки и удаления приложений	636
События компонентов Kaspersky Security Center	636
Блокировка частых событий	678
Контроль изменения состояния виртуальных машин	681
Отслеживание состояния антивирусной защиты с помощью информации в системном реестре ...	682
Просмотр и настройка действий, когда устройство неактивно	683
Выключение объявлений "Лаборатории Касперского"	685

Сценарий: мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Kaspersky Security Center.

Предварительные требования

После развертывания Kaspersky Security Center в сети организации вы можете приступить к мониторингу состояния безопасности сети с помощью Kaspersky Security Center и к формированию отчетов.

Этапы

Мониторинг и работа с отчетами в сети организации состоят из следующих этапов:

a. Настройка переключения статусов устройств

Ознакомьтесь с параметрами, определяющими присвоение статусов устройствам в зависимости от конкретных условий. Изменяя эти параметры (см. раздел "Настройка переключения статусов устройств" на стр. [766](#)), вы можете изменить количество событий с уровнями важности *Критический* или *Предупреждение*.

При настройке переключения статусов устройств убедитесь, что новые параметры не конфликтуют с политиками информационной безопасности вашей организации и что вы можете своевременно реагировать на важные события безопасности в сети вашей организации.

b. Настройка параметров уведомлений о событиях на клиентских устройствах

Настройте уведомления (по электронной почте, по SMS или с помощью запуска исполняемого файла) о событиях на клиентских устройствах (см. раздел "Настройка параметров уведомлений о событиях" на стр. [311](#)), в соответствии с потребностями вашей организации.

c. Изменение ответа вашей сети безопасности на событие Вирусная атака

Чтобы настроить ответ сети на новые события, вы можете изменить пороговые значения (см. стр. [718](#)) в свойствах Сервера администрирования. Вы также можете создать более строгую политику (см. раздел "Автоматическая активация политики по событию "Вирусная атака"" см. стр. [437](#)), которая будет активирована, или создать задачу (см. раздел "Создание задачи" на стр. [416](#)), которая будет запускаться при возникновении этого события.

d. Работа со статистической информацией

Настройте отображение статистики (см. раздел "Работа со статистической информацией" на стр. [613](#)) в соответствии с потребностями вашей организации.

e. Просмотр состояния безопасности сети вашей организации

Чтобы проверить состояние безопасности сети вашей организации, вы можете выполнить любое из следующих действий:

- В рабочей области узла **Сервер администрирования**, на вкладке **Статистика** откройте вкладку второго уровня (страницу) **Состояние защиты** и просмотрите информационную панель **Статус постоянной защиты**.
- Генерация и просмотр отчета **Отчет о состоянии защиты** (см. раздел "Создание и просмотр отчета" на стр. [607](#)).
- Генерация и просмотр отчета **Отчет об ошибках** (см. раздел "Создание и просмотр отчета" на стр. [607](#)).

f. Нахождение незащищенных клиентских устройств

Чтобы найти незащищенные клиентские устройства, перейдите в рабочую область узла **Сервер администрирования**, на вкладке **Статистика** откройте вкладку второго уровня (страницу) **Состояние защиты** и просмотрите информационную панель **История обнаружения новых устройств в сети**. Также можно создать и просмотреть **Отчет о развертывании защиты** (см. раздел "Создание и просмотр отчета" на стр. [607](#)).

g. Проверка защиты клиентских устройств

Чтобы проверить защиту клиентских устройств, перейдите в рабочую область узла **Сервер администрирования**, на вкладке **Статистика** откройте **Развертывание** или вкладку второго уровня (страницу) **Статистика угроз** и просмотрите соответствующие информационные панели. Вы также можете начать и просматривать выборку событий **Критические события** (см. раздел "Просмотр выборки событий" см. стр. [620](#)).

h. Оценка и ограничение загрузки событий в базу данных

Информация о событиях, которые возникают во время работы управляемых приложений, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

Чтобы оценить загрузку событий в базе данных, рассчитайте место в базе данных. Вы также можете ограничить максимальное количество событий (см. раздел "Настройка количества событий в хранилище событий" см. стр. [413](#)) чтобы избежать переполнения базы данных.

i. Просмотр информации о лицензии

Чтобы просмотреть информацию о лицензии, перейдите в рабочую область узла **Сервер администрирования**, на вкладке **Статистика** откройте вкладку второго уровня (страницу) **Развертывание** и просмотрите информационную панель **Использование лицензионных ключей**. Также можно создать и просмотреть **Отчет об использовании лицензионных ключей** (см. раздел "Создание и просмотр отчета" на стр. [607](#)).

Результаты

После завершения сценария вы будете проинформированы о защите сети вашей организации и, таким образом, сможете планировать действия для дальнейшей защиты.

Мониторинг цветowych индикаторов и зарегистрированных событий в Консоли администрирования

В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Security Center и управляемых устройств с помощью цветowych индикаторов. Индикаторы отображаются в рабочей области узла **Сервер администрирования** на вкладке **Мониторинг**. На вкладке имеется шесть информационных блоков с цветowymi индикаторами и зарегистрированными событиями. Цветной индикатор – это цветная вертикальная полоса на левой стороне панели. Каждый блок с индикатором отвечает за отдельную функциональную область Kaspersky Security Center (см. таблицу ниже).

Таблица 59. Области ответственности цветowych индикаторов в Консоли администрирования

Название панели	Область ответственности цветowego индикатора
Развертывание	Установка Агента администрирования и приложений безопасности на устройства сети организации.
Структура управления	Структура групп администрирования. Сканирование сети. Правила перемещения устройств
Настройка защиты	Функции приложения безопасности: состояние защиты, поиск вредоносного ПО.
Обновление	Обновления и патчи.
Мониторинг	Состояние защиты
Сервер администрирования	Функции и свойства Сервера администрирования.

Индикатор может быть одного из пяти цветов (см. таблицу ниже). Цвет индикатора зависит от текущего состояния Kaspersky Security Center и от зарегистрированных событий.

Таблица 60. Цветовые кодировки индикаторов

Состояние	Цвет индикатора	Значение цвета индикатора
Информационное	Зеленый	Вмешательство администратора не требуется.
Предупреждение.	Желтый	Требуется вмешательство администратора.
Предельный.	Красный	Имеются серьезные проблемы. Требуется вмешательство администратора для их решения.
Информационное	Голубой	Зарегистрированы события, не связанные с угрозами для безопасности управляемых устройств.
Информационное	Серый	Информация о событиях недоступна или еще не получена.

Цель администратора – поддерживать индикаторы в состоянии "зеленый" на всех информационных панелях вкладки **Мониторинг**.

На информационных панелях также отображаются зарегистрированные события, влияющие на цветowych индикаторы, и состояние Kaspersky Security Center (см. таблицу ниже).

Таблица 61. Название, описание и цвет индикатора зарегистрированных событий

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	Количество устройств, на которых срок действия лицензии истек: %1	IDS_AK_STATUS_LIC_EXPIRED	События этого типа возникают, если срок действия коммерческой лицензии (см. раздел "О лицензии" на стр. 342) окончен. Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии. После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. 354). Чтобы продолжить использование Kaspersky Security Center, продлите срок действия коммерческой лицензии.
Красный	Устройств с не запущенным приложением безопасности: %1	IDS_AK_STATUS_AV_NOT_RUNNING	События этого типа возникают, когда приложение безопасности, установленное на устройстве, не запущено. Убедитесь, что на устройстве запущено приложение Kaspersky Endpoint Security.

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	Устройств с выключенной защитой: %1	IDS_AK_STATUS_RTP_NOT_RUNNING	События такого типа возникают, когда приложение защиты на устройстве отключено больше указанного времени. Проверьте текущий статус постоянной защиты (см. раздел "Параметры управляемого устройства" на стр. 782) на устройстве и убедитесь, что все необходимые вам компоненты защиты включены.

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	Обнаружена уязвимость в программном обеспечении на устройствах	IDS_AK_STATUS_VULNERABILITIES_FOUND	События этого типа происходят, когда задача <i>Поиск уязвимостей и требуемых обновлений</i> обнаружила уязвимости с указанным уровнем критичности (см. раздел "Правила установки обновлений" см. стр. 567) в приложениях, установленных на устройстве. Проверьте список доступных обновлений (см. раздел "Просмотр информации о доступных обновлениях для приложений сторонних производителей" см. стр. 503) в подпапке Обновления программного обеспечения, вложенной в папку Управление приложениями. Эта папка содержит список полученных Сервером администрирования обновлений приложений Microsoft и других производителей программного обеспечения, которые могут быть распространены на устройства. Просмотрите информацию о доступных обновлениях и установите их на устройство (см. раздел "Установка обновлений на устройства вручную" на стр. 513).

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	На Сервере администрирования зарегистрированы критические события	IDS_AK_STATUS_EVENTS_OCCURED	События этого типа возникают при обнаружении критических событий Сервера администрирования. Проверьте список событий (см. раздел "Просмотр выборки событий" см. стр. 620), хранящихся на Сервере администрирования, а затем последовательно исправьте критические события.
Красный	На Сервере администрирования зарегистрированы ошибки в событиях	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	События этого типа возникают при регистрации непредвиденных ошибок на стороне Сервера администрирования. Проверьте список событий (см. раздел "Просмотр выборки событий" см. стр. 620), хранящихся на Сервере администрирования, а затем последовательно исправьте критические события.
Красный	Потеряно соединение с устройствами: %1	IDS_AK_STATUS_ADM_LOST_CONTROL1	События этого типа возникают при потере соединения между Сервером администрирования и устройством. Просмотрите список отключенных устройств и попробуйте подключить их снова.

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	Устройств, которые давно не соединялись с Сервером администрирования: %1	IDS_AK_STATUS_ADM_NOT_CONNECTED1	События этого типа возникают, когда устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено. Убедитесь, что устройство включено и запущен Агент администрирования.
Красный	Устройств со статусом отличным от "ОК": %1	IDS_AK_STATUS_HOST_NOT_OK	События этого типа происходят, когда статус устройства <i>ОК</i> , подключенного к Серверу администрирования, меняется на <i>Критический</i> или <i>Предупреждение</i> . Устранить неполадку можно с помощью утилиты удаленной диагностики Kaspersky Security Center (см. раздел "Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center" см. стр. 773).
Красный	Базы устарели: %1 устройств	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	События этого типа возникают, когда антивирусные базы на устройстве не обновлялись в течение заданного интервала времени. Следуйте инструкциям, чтобы обновить антивирусные базы "Лаборатории Касперского" (см. раздел "Создание задачи для загрузки обновлений в хранилище Сервера администрирования" на стр. 469).

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	Устройств, на которых давно не осуществлялась проверка обновлений Центра обновления Windows: %1	IDS_AK_STATUS_WUA_DATA_OBSOLETE	События этого типа возникают, когда задача <i>Синхронизация обновлений Windows Update</i> не выполнялась больше указанного времени. Следуйте инструкциям, чтобы синхронизировать обновления из Центра обновления Windows Update с Сервером администрирования (см. раздел "Синхронизация обновлений Windows Update с Сервером администрирования" на стр. 506).
Красный	Для Kaspersky Security Center требуется установка плагинов: %1	IDS_AK_STATUS_PLUGINS_REQUIRED2	События этого типа возникают, когда вам нужно установить дополнительные плагины для приложений "Лаборатории Касперского". Загрузите и установите необходимые плагины управления для приложения "Лаборатории Касперского" с веб-сайта Службы технической поддержки "Лаборатории Касперского" https://support.kaspersky.com/9333 .

Работа с отчетами, статистикой и уведомлениями

В этом разделе представлена информация о работе с отчетами, статистикой и выборками событий и устройств в Kaspersky Security Center, а также о настройке параметров уведомлений Сервера администрирования.

В этом разделе

Работа с отчетами	602
Работа со статистической информацией	613
Настройка параметров уведомлений о событиях.....	614
Создание сертификата для SMTP-сервера	619
Выборки событий	619
Выборки устройств.....	622

Работа с отчетами

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования. Вы можете создавать отчеты для следующих объектов:

- для выборок устройств, созданных по определенным параметрам;
- для групп администрирования;
- для наборов устройств из разных групп администрирования;
- для всех устройств в сети (в отчете о развертывании).

В приложении есть набор стандартных шаблонов отчетов. Предусмотрена также возможность создавать пользовательские шаблоны отчетов. Отчеты отображаются в главном окне приложения, в папке дерева консоли **Сервер администрирования**.

В этом разделе

Создание шаблона отчета	602
Просмотр и изменение свойств шаблона отчета.....	603
Расширенный формат фильтра в шаблонах отчета	605
Создание и просмотр отчета	607
Сохранение отчета	607
Создание задачи рассылки отчета.....	608

Создание шаблона отчета

► Чтобы создать шаблон отчета:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**.

В результате запустится мастер создания шаблона отчета. Следуйте далее указаниям мастера.

После окончания работы мастера сформированный шаблон отчета будет добавлен в состав выбранной папки **Сервер администрирования** дерева консоли. Этот шаблон можно использовать для создания и просмотра отчетов.

Просмотр и изменение свойств шаблона отчета

Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

► *Чтобы просмотреть и изменить свойства шаблона отчета:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. В списке шаблонов отчетов выберите требуемый шаблон отчета.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Свойства**.

В качестве альтернативы, можно сначала сформировать отчет, а затем нажать на кнопку **Открыть свойства шаблона отчета** или **Настроить столбцы отчета**.

5. В открывшемся окне вы можете изменить свойства шаблона отчета. Свойства каждого отчета могут содержать только некоторые из разделов, описанных ниже.

- Раздел **Общие**:

- Название шаблона отчета
- **Максимальное число отображаемых записей**

Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение.

Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Столбцы** → **Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

По умолчанию параметр включен. По умолчанию указано значение 1000.

- **Версия для печати**

Отчет оптимизирован для печати: добавлены пробелы, между некоторыми значениями для лучшей визуальной доступности.

По умолчанию параметр включен.

- Раздел **Столбцы**.

Выберите поля, которые будут отображаться в отчете и порядок этих полей. Также настройте, должна ли информация в отчете сортироваться и фильтроваться по каждому из полей.

- Раздел **Период**.

Измените отчетный период. Доступные значения:

- между двумя указанными датами;
- от указанной даты до даты создания отчета;
- от даты создания отчета минус указанное количество дней до даты создания отчета.

- Разделы **Группа**, **Выборка устройств**, или **Устройства**.

Измените набор клиентских устройств, для которых создается отчет. В зависимости от параметров, указанных при создании шаблона, может присутствовать только один из этих разделов.

- Раздел **Параметры**.

Измените параметры отчета. Набор параметров зависит от конкретного отчета.

- Раздел **Безопасность. Наследовать параметры Сервера администрирования**

Если этот параметр включен, параметры отчета наследуются с Сервера администрирования.

Если этот параметр выключен, вы можете настроить параметры отчета. Вы можете назначить роль пользователю или группе пользователей (см. раздел "Назначение роли пользователю или группе безопасности" на стр. [838](#)) или назначить права пользователю или группе пользователей (см. раздел "Назначение прав пользователям или группам пользователей" на стр. [838](#)), применительно к отчету.

По умолчанию параметр включен.

Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности** (см. раздел "**Настройка общих параметров Сервера администрирования**" на стр. [716](#)).

- Раздел **Иерархия Серверов администрирования**:

- **Включать данные подчиненных и виртуальных Серверов администрирования**

Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

По умолчанию параметр включен.

- **До уровня вложенности**

Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

- **Интервал ожидания данных (мин)**

- **Кешировать данные с подчиненных Серверов администрирования**

Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

Включение этого параметра позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

По умолчанию параметр выключен.

- **Период обновления данных в кеше (ч)**

Подчиненные Серверы администрирования через заданные интервалы времени (указанные в часах) передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Вы можете указать этот период в часах. Если установлено значение 0, данные передаются только во время генерации отчета.

По умолчанию указано значение 0.

- **Передавать подробную информацию с подчиненных Серверов администрирования**

В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все данные в одном отчете.

Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

По умолчанию параметр выключен.

Расширенный формат фильтра в шаблонах отчета

В приложении Kaspersky Security Center вы можете применить расширенный формат фильтра к шаблонам отчета. Расширенный формат фильтра обеспечивает большую гибкость по сравнению с форматом по умолчанию. Вы можете создавать сложные условия фильтрации, используя набор фильтров, которые будут применяться к отчету с помощью логического оператора OR при создании отчета, как показано ниже:

Фильтр[1](Поле[1] AND Поле[2]... AND Поле[n]) OR Фильтр[2](Поле[1] AND Поле[2]... AND Поле[n]) OR... Фильтр[n](Поле[1] AND Поле[2]... AND Поле[n])

Кроме того, с помощью расширенного формата фильтра вы можете установить значение временного интервала в формате относительного времени (например, с помощью условия "За последние N дней") для определенных полей фильтра. Доступность и набор условий временного интервала зависят от типа шаблона отчета.

Конвертация фильтра в расширенный формат

Расширенный формат фильтра для шаблонов отчета поддерживается только в версии Kaspersky Security Center 12 и выше. После конвертации фильтра по умолчанию в расширенный формат, шаблон отчета становится несовместимым с Серверами администрирования вашей сети, на которых установлены более ранние версии Kaspersky Security Center. Информация с этих Серверов администрирования не будет получена для отчета.

► Чтобы конвертировать из формата по умолчанию в расширенный формат:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. В списке шаблонов отчетов выберите требуемый шаблон отчета.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Свойства**.
5. В отобразившемся окне свойств выберите раздел **Столбцы**.
6. На вкладке **Детальные данные** перейдите по ссылке **Конвертировать фильтр**.
7. В появившемся окне нажмите на кнопку **ОК**.

Конвертация в расширенный формат фильтра необратима для шаблона отчета, к которому он применяется. Если вы случайно перешли по ссылке **Конвертировать фильтр**, вы можете отменить изменения, нажав на кнопку **Отмена** в окне свойств шаблона отчета.

8. Чтобы применить изменения, закройте окно свойств шаблона отчета, нажав на кнопку **ОК**.

Когда снова откроется окно свойств шаблона отчета, отобразится новый доступный раздел **Фильтры**. В этом разделе вы можете настроить расширенный формат фильтра (см. раздел "Настройка расширенного фильтра" на стр. [606](#)).

Настройка расширенного фильтра

► Чтобы настроить параметры расширенного фильтра в шаблоне отчета:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. В списке шаблонов отчетов выберите шаблон отчета, который ранее был конвертирован в расширенный формат фильтра (см. раздел "Конвертация фильтра в расширенный формат" на стр. [606](#)).
4. В контекстном меню выбранного шаблона отчета выберите пункт **Свойства**.
5. В отобразившемся окне свойств выберите раздел **Фильтры**.

Раздел **Фильтры** не отображается, если шаблон отчета не был сконвертирован в расширенный формат фильтра (см. раздел "Конвертация фильтра в расширенный формат" на стр. [606](#)).

В окне свойства шаблона отчета в разделе **Фильтры** вы можете просмотреть и изменить список примененных фильтров к отчету. Каждый фильтр в списке имеет уникальное имя и представляет собой набор фильтров для соответствующих полей в отчете.

6. Откройте окно свойств фильтра одним из следующих способов:

- Чтобы создать фильтр, нажмите на кнопку **Добавить**.
- Чтобы изменить существующий фильтр, выберите необходимый фильтр и нажмите на кнопку **Изменить**.

7. В открывшемся окне выберите и укажите значения обязательных полей фильтра.

8. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно.

Если вы создаете фильтр, имя фильтра должно быть указано в поле **Имя фильтра**, прежде чем нажать на кнопку **ОК**.

9. Закройте окно свойств шаблона отчета, нажав на кнопку **ОК**.

Расширенный фильтр в шаблоне отчета настроен. Теперь вы можете создавать отчеты (см. раздел "Создание и просмотр отчета" на стр. [607](#)) используя это шаблон отчета.

Создание и просмотр отчета

► *Чтобы сформировать и просмотреть отчет:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов двойным нажатием клавиши мыши. Отобразится выбранный шаблон отчета.

В отчете отображаются следующие данные:

- тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
- графическая диаграмма с наиболее характерными данными отчета;
- сводная таблица с вычисляемыми показателями отчета;
- таблица с детальными данными отчета.

См. также:

Сценарий: обновление приложений сторонних производителей	499
Сценарий: мониторинг и отчеты	593

Сохранение отчета

► *Чтобы сохранить сформированный отчет:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В рабочей области узла выберите вкладку **Отчеты**.
 3. Выберите интересующий вас шаблон отчета в списке шаблонов.
 4. В контекстном меню выбранного шаблона отчета выберите пункт **Сохранить**.
- В результате запустится мастер сохранения отчета. Следуйте далее указаниям мастера.

После завершения работы мастера откроется папка, в которую вы сохранили файл отчета.

Когда вы сохраняете отчет в виде файла XLS, все связанные изображения, такие как логотип и датаграмма, сохраняются как отдельные файлы.

Создание задачи рассылки отчета

Отчеты можно рассылать по электронной почте. Рассылка отчетов в Kaspersky Security Center осуществляется с помощью задачи рассылки отчета.

► Чтобы создать задачу рассылки одного отчета:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Рассылка отчетов**.

В результате запускается мастер создания задачи рассылки выбранного отчета. Следуйте далее указаниям мастера.

► Чтобы создать задачу рассылки нескольких отчетов:

1. В дереве консоли в узле с именем нужного вам Сервера администрирования выберите папку **Задачи**.

2. Нажмите на кнопку **Создать задачу** в рабочей области папки **Задачи**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Созданная задача рассылки отчета отображается в папке дерева консоли **Задачи**.

Задача рассылки отчета создается автоматически в случае, если при установке Kaspersky Security Center были заданы параметры электронной почты (см. раздел "Мастер первоначальной настройки Сервера администрирования" на стр. [281](#)).

Шаг 1. Выбор типа отчета

В окне **Выбор типа задачи** в списке задач выберите тип задачи **Рассылка отчетов**.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 2. Выбор типа отчета

В окне **Выбор типа отчета** в списке шаблонов для создания задачи выберите тип отчета.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 3. Действия над отчетом

В разделе **Действия с отчетами** укажите следующие параметры:

- **Посылать отчеты по электронной почте**

Если флажок установлен, приложение отправляет сформированные отчеты по электронной почте.

Параметры отправки отчета по электронной почте можно настроить по ссылке **Параметры отправки по электронной почте**. Ссылка доступна, когда флажок установлен.

Если флажок снят, приложение сохраняет отчеты в указанной папке для хранения отчетов.

По умолчанию флажок снят.

- **Сохранять отчеты в папке общего доступа**

Если флажок установлен, приложение сохраняет отчеты в папке, указанной в поле под флажком. Чтобы сохранять отчеты в папке общего доступа, укажите UNC-путь к этой папке. В таком случае в окне **Выбор учетной записи для запуска задачи** необходимо задать учетную запись и пароль пользователя для доступа к этой папке.

Если флажок снят, приложение не сохраняет отчеты в папке, а отправляет их по электронной почте.

По умолчанию флажок снят.

- **Замещать предыдущие отчеты того же типа**

Если флажок установлен, при каждом запуске задачи новый файл отчета замещает в папке для хранения отчетов файл, сохраненный при предыдущем запуске задачи.

Если флажок снят, файлы отчетов не перезаписываются. При каждом запуске задачи в папке сохраняется отдельный файл отчета.

Флажок доступен, если установлен флажок **Сохранять отчет в папке**.

По умолчанию флажок снят.

- **Задать учетную запись для доступа к папке общего доступа**

Если флажок установлен, можно указать учетную запись, от имени которой отчет записывается в папку. Если в окне **Действия с отчетом** в качестве параметра **Сохранять отчет в папке** указан UNC-путь к папке общего доступа, необходимо указать учетную запись и пароль для доступа к этой папке.

Если флажок снят, отчет записывается в папку от имени учетной записи Сервера администрирования.

Флажок доступен, если установлен флажок **Сохранять отчет в папке**.

По умолчанию флажок снят.

Когда вы сохраняете или отправляете отчет в виде файла XLS, все связанные изображения, такие как логотип и датаграмма, сохраняются как отдельные файлы.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 4. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** можно указать, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **Учетная запись по умолчанию**

Задача будет запускаться под той же учетной записью, под которой была установлено и запущено приложение, выполняющее эту задачу.

По умолчанию выбран этот вариант.

- **Задать учетную запись**

Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

- **Учетная запись**

Учетная запись, от имени которой будет запускаться задача.

- **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 5. Настройка расписания задачи

В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости задайте следующие параметры:

- **Запуск по расписанию:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала

каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрывающимся списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемым списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемом списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.
- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

Шаг 6. Определение названия задачи

В окне **Определение названия задачи** укажите название создаваемого правила. Имя задачи не может превышать 100 символов и не может содержать специальные символы (" * < > ? \ : |).

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 7. Завершение создания задачи

В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Работа со статистической информацией

Статистическая информация о состоянии системы защиты и управляемых устройств отображается в виде настраиваемых информационных панелей. Статистическая информация отображается в рабочей области узла **Сервер администрирования** на вкладке **Статистика**. Эта вкладка также содержит несколько вкладок второго уровня (страниц). На каждой странице отображаются информационные панели со статистической информацией, а также ссылки на корпоративные новости и другие материалы "Лаборатории Касперского". Статистическая информация представлена на информационных панелях в виде круговых или столбчатых

диаграмм или таблиц. Данные на информационных панелях обновляются в процессе работы приложения и отражают текущее состояние приложения безопасности.

Можно изменить набор вкладок второго уровня, содержащихся на вкладке **Статистика**, набор информационных панелей на каждой странице с вкладками, а также способ представления данных на информационных панелях.

► *Чтобы добавить новую вкладку второго уровня с информационными панелями на вкладке **Статистика**:*

1. Нажмите на кнопку **Настроить вид** в правом верхнем углу вкладки **Статистика**.

В результате откроется окно свойств статистики. В окне содержится список страниц с вкладками, которые содержатся на вкладке **Статистика** в настоящее время. В окне можно изменять порядок отображения страниц на вкладке, добавлять и удалять страницы, переходить к настройке свойств страниц по кнопке **Свойства**.

2. Нажмите на кнопку **Добавить**.

Откроется окно свойств новой страницы.

3. Настройте новую страницу:

- В разделе **Общие** укажите название страницы.
- В разделе **Информационные панели** по кнопке **Добавить** добавьте информационные панели, которые должны отображаться на странице.

По кнопке **Свойства** в разделе **Информационные панели** можно настраивать свойства добавленных информационных панелей: название, тип и вид диаграммы в панели, данные, по которым строится диаграмма.

4. Нажмите на кнопку **ОК**.

Добавленная страница с вкладками с информационными панелями отобразится на вкладке

Статистика. Нажав на значок параметров (⚙) можно сразу перейти к настройке страницы или выбранной информационной панели на странице.

Настройка параметров уведомлений о событиях

Kaspersky Security Center позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений:

- Электронная почта. При возникновении события приложение посылает уведомление на указанные адреса электронной почты. Вы можете настроить текст уведомления.
- SMS. При возникновении события приложение посылает уведомления на указанные номера телефонов. Вы можете настроить отправку SMS оповещений с помощью почтового шлюза.
- Исполняемый файл. При возникновении события на устройстве, исполняемый файл запускается на рабочем месте администратора. С помощью исполняемого файла администратор может получать параметры произошедшего события (см. раздел "Уведомление о событиях с помощью исполняемого файла" на стр. [316](#)).

► *Чтобы настроить параметры уведомлений о событиях на клиентских устройствах:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.

3. Перейдите по ссылке **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

Откроется окно **Свойства:События**.

4. В разделе **Уведомление** выберите способ уведомления (электронная почта, SMS, исполняемый файл для запуска) и настройте параметры уведомлений:

- **Электронная почта**

На вкладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей. По умолчанию параметр выключен.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

Вам нужно указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

- Параметры TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования

TLS.

- **Всегда использовать TLS, проверить срок действия сертификата Сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы решите использовать значение **Всегда использовать TLS, для проверки срока действия сертификата Сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать параметры TLS для SMTP-сервера:

- Выберите файл сертификата SMTP-сервера:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

Вам нужно указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер с сертификатом в формате PKCS#12:

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два

раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

Нажмите на кнопку **Отправить тестовое сообщение** можно проверить правильность настройки сообщений. Приложение отправляет тестовые сообщения на указанные адреса электронной почты.

- **SMS**

На вкладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

Если необходимо, вы можете указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

- Параметры TLS для SMTP-сервера

Вы можете отключить использование TLS, использовать TLS, если SMTP-сервер поддерживает этот протокол, или вы можете принудительно использовать только TLS. Если вы решите использовать только TLS, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также, если вы решили использовать только TLS, вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

- Выберите файл сертификата SMTP-сервера

Вы можете получить файл со списком сертификатов от аккредитованного центра сертификации и загрузить его в Kaspersky Security Center. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ

сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован. В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления. Приложение отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

Если выбран этот способ уведомления, в поле ввода можно указать, какое приложение будет запущено при возникновении события.

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения на указанные адреса электронной почты.

1. В поле **Текст уведомления** введите текст, который приложение будет отправлять при возникновении события.

Из раскрывающегося списка, расположенного справа от текстового поля, можно добавлять в сообщение подстановочные параметры с деталями события (например, описание события, время возникновения и прочее).

Если текст уведомления содержит символ %, нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

2. По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления. Приложение отправляет тестовое уведомление указанному получателю.
3. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Можно изменить значения параметров уведомлений для определенных событий в разделе **Настройка событий** параметров Сервера администрирования, параметров политики (см. раздел «Общие параметры политик» см. стр. [788](#)) или параметров приложения (см. раздел «Выбор событий приложений» «Лаборатории

Касперского» для экспорта в формате Syslog» см. стр. [886](#)).

См. также:

Обработка и хранение событий на Сервере администрирования.....	717
Сценарий: мониторинг и отчеты.....	593

Создание сертификата для SMTP-сервера

Сертификат для SMTP-сервера необходим для идентификации и верификации почтового сервера, к которому производится подключение. Сертификат используется для защиты пересылаемых писем от перехвата, например, в процессе передачи писем от почтового клиента к серверу и обратно.

► Чтобы создать сертификат для SMTP-сервера, выполните следующие действия:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.
Откроется окно свойств событий.
4. На вкладке **Электронная почта** по ссылке **Параметры** откройте окно **Параметры**.
5. В окне **Параметры** по ссылке **Задать сертификат** откройте окно **Сертификат для подписи**.
6. В окне **Сертификат для подписи** нажмите на кнопку **Задать**.
В результате откроется окно **Сертификат**.
7. В раскрывающемся списке **Тип сертификата** выберите открытый или закрытый тип сертификата:
 - Если выбран сертификат закрытого типа (**Контейнер PKCS#12**), укажите файл сертификата и пароль.
 - Если выбран сертификат открытого типа (**X.509-сертификат**):
 - a. укажите файл закрытого ключа (файл с расширением pkc или pem);
 - b. укажите пароль закрытого ключа;
 - c. укажите файл открытого ключа (файл с расширением cer).
8. Нажмите на кнопку **ОК**.

В результате будет выписан сертификат для SMTP-сервера.

Выборки событий

Информация о событиях в работе Kaspersky Security Center и управляемых приложений сохраняется как в базе данных Сервера администрирования, так и в системном журнале Microsoft Windows. Вы можете просматривать информацию из базы данных Сервера администрирования в рабочей области узла **Сервер администрирования** на вкладке **События**.

Информация на вкладке **События** представлена в виде списка выборок событий. Каждая выборка включает в себя только события определенного типа. Например, выборка "Статус устройства –

"Критический" содержит только записи об изменении статусов устройств на "Критический". После установки приложения на вкладке **События** содержится ряд стандартных выборок событий. Вы можете создавать дополнительные (пользовательские) выборки событий, а также экспортировать информацию о событиях в файл.

Просмотр выборки событий

► *Чтобы просмотреть выборку событий:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. В раскрывающемся списке **Выборки событий** выберите нужную вам выборку событий.

Если вы хотите, чтобы события этой выборки отображались в рабочей области постоянно, нажмите на значок "Избранное" (☆) рядом с выборкой.

В результате в рабочей области будет представлен список событий выбранного типа, хранящихся на Сервере администрирования.

Вы можете сортировать информацию в списке событий по возрастанию или убыванию данных в любой графе списка.

Настройка параметров выборки событий

► *Чтобы настроить параметры выборки событий:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Откройте нужную вам выборку событий на вкладке **События**.
4. Нажмите на кнопку **Свойства выборки**.

В открывшемся окне свойств выборки событий вы можете настроить параметры выборки.

См. также:

Сценарий: мониторинг и отчеты[593](#)

Создание выборки событий

► *Чтобы создать выборку событий:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Нажмите на кнопку **Создать выборку**.
4. В открывшемся окне **Новая выборка событий** укажите имя создаваемой выборки и нажмите на кнопку **ОК**.

В результате в раскрывающемся списке **Выборки событий** будет создана выборка с указанным вами именем.

По умолчанию созданная выборка событий содержит все события, хранящиеся на Сервере администрирования. Чтобы в выборке отображались только интересующие вас события, нужно настроить параметры выборки.

См. также:

Сценарий: мониторинг и отчеты [593](#)

Экспорт выборки событий в текстовый файл

► Чтобы экспортировать выборку событий в текстовый файл:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Нажмите на кнопку **Импорт/Экспорт**.
4. В раскрывающемся списке выберите **Экспортировать события в файл**.

В результате запустится мастер экспорта событий. Следуйте далее указаниям мастера.

См. также:

Сценарий: мониторинг и отчеты [593](#)

Удаление событий из выборки

► Чтобы удалить события из выборки:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Выберите события, которые требуется удалить, с помощью мыши и клавиш **SHIFT** или **CTRL**.
4. Удалите выбранные события одним из следующих способов:

- В контекстном меню любого из выделенных событий выберите пункт **Удалить**.

При выборе пункта контекстного меню **Удалить все** из выборки будут удалены все отображаемые события, независимо от того, какие из них вы предварительно выбрали для удаления.

- По ссылке **Удалить событие**, если выбрано одно событие, или по ссылке **Удалить события**, если выбрано несколько событий, в блоке работы с выбранными событиями.

В результате выбранные события будут удалены.

Добавление приложений в исключения по запросам пользователей

Если вы получаете запросы пользователей для разблокирования ошибочно заблокированных приложений, вы можете создать исключение из правил Адаптивного контроля аномалий для этих приложений. Такие приложения больше не будут блокироваться на устройствах пользователей. Вы можете отслеживать количество запросов пользователей на вкладке **Мониторинг** в рабочей области Сервера администрирования.

► *Чтобы добавить приложение, заблокированное Kaspersky Endpoint Security, в исключения по запросам пользователей:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. В раскрывающемся списке **Выборки событий** выберите **Запросы пользователей**.
4. В контекстном меню запроса пользователя (или нескольких запросов пользователей), содержащих приложения, которые необходимо добавить в исключения, выберите пункт **Добавить исключения**.

Запустится мастер добавления исключений (см. раздел "Добавление исключений в правила Адаптивного контроля аномалий" на стр. [866](#)). Следуйте шагам мастера.

Выбранные приложения будут исключены из списка обнаружений **Правила срабатываний в статусе Интеллектуальное обучение** (в папке **Хранилища** дерева консоли) после следующей синхронизации клиентского устройства с Сервером администрирования. Такие приложения больше не будут отображаться в списке обнаружений.

Выборки устройств

Информация о состоянии устройств содержится в дереве консоли в папке **Выборки устройств**.

Информация в папке **Выборки устройств** представлена в виде списка выборок устройств. Каждая выборка включает в себя устройства, отвечающие определенным условиям. Например, выборка **Устройства со статусом "Критический"** содержит только устройства со статусом *Критический*. После установки приложения папка **Выборки устройств** содержит ряд стандартных выборок. Вы можете создавать дополнительные (пользовательские) выборки устройств, экспортировать параметры выборок в файл, а также создавать выборки с параметрами, импортированными из файла.

Просмотр выборки устройств

► *Чтобы просмотреть выборку устройств:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки в списке **Устройства выборки** выберите нужную вам выборку устройств.
3. Нажмите на кнопку **Запустить выборку**.
4. Выберите вкладку **Результаты выборки**.

В результате в рабочей области отобразится список устройств, отвечающих параметрам выборки.

Вы можете сортировать информацию в списке устройств по возрастанию или убыванию данных в любой из граф.

Настройка выборки устройств

► Чтобы настроить параметры выборки устройств:

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки перейдите на вкладку **Выборка** и выберите нужную вам выборку устройств в списке пользовательских выборок устройств.
3. Нажмите на кнопку **Свойства выборки**.
4. В открывшемся окне свойств задайте следующие параметры:
 - Общие параметры выборки.
 - Условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку. Чтобы настроить условия, выберите имя условия и нажмите на кнопку **Свойства**.
 - Параметры безопасности.
5. Нажмите на кнопку **ОК**.

Параметры применены и сохранены.

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

Инвертировать условие выборки

Если флажок установлен, заданное условие выборки будет инвертировано. В выборку попадут все устройства, не соответствующие условию.

По умолчанию флажок снят.

Сеть

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

- **Имя устройства или IP-адрес**
Имя устройства в сети Windows (NetBIOS-имя).
- **Windows-домен**
Будут отображаться все устройства, входящие в указанный домен Windows.
- **Группа администрирования**
Будут отображаться устройства, входящие в указанную группу администрирования.
- **Описание**
Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие** или в разделе **Заметки**.
Для описания текста в поле **Комментарий** допустимо использовать следующие символы:

- Внутри одного слова:

- *. Заменяет любую строку длиной 0 и более символов.

Пример:

Для описания слов **Сервер**, **Серверный** или **Серверная** можно использовать строку **Сервер***

- ?. Заменяет любой один символ.

Пример:

Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

Символ * или ? не может использоваться как первый символ в описании текста.

- Для связи нескольких слов:

- Пробел. Обозначает наличие в тексте хотя бы одного из слов, разделенных пробелами.

Пример:

Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

- +. При написании перед словом обозначает обязательное наличие слова в тексте.

Пример:

Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

- -. При написании перед словом обозначает обязательное отсутствие слова в тексте.

Пример:

Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

- "<фрагмент текста>". Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

Пример:

Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- IP-диапазон

Если флажок установлен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

По умолчанию флажок снят.

Теги

В разделе **Теги** можно настроить критерии включения устройств в выборку по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

- **Применить, если есть хотя бы один из выбранных тегов**

Если флажок установлен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если флажок снят, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию флажок снят.

- **Тег должен присутствовать**

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

По умолчанию выбран этот вариант.

- **Тег должен отсутствовать**

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Active Directory

В разделе **Active Directory** можно настроить критерии включения устройств в выборку на основании их данных Active Directory:

- **Устройство в подразделении Active Directory**

Если флажок установлен, в выборку будут включаться устройства из подразделения Active Directory, указанного в поле ввода.

По умолчанию флажок снят.

- **Включать дочерние подразделения**

Если флажок установлен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

По умолчанию флажок снят.

- **Устройство является членом группы Active Directory**

Если флажок установлен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

По умолчанию флажок снят.

Сетевая активность

В разделе **Сетевая активность** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- **Это устройство является точкой распространения**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** В выборку будут включены устройства, являющиеся агентами обновлений.
- **Нет.** Устройства, являющиеся агентами обновлений, не будут включены в выборку.
- **Значение не выбрано.** Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Включен.** В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
- **Выключен.** В выборку будут включаться устройства, на которых флажок **Не разрывать соединение с Сервером администрирования** снят.
- **Значение не выбрано.** Критерий не применяется.

- **Переключение профиля подключения**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Нет.** В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Значение не выбрано.** Критерий не применяется.

- **Последнее подключение к Серверу администрирования**

С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

Если флажок установлен, то в выборку попадают только новые устройства, обнаруженные при опросе сети за количество дней, которое указано в поле **Период обнаружения (сут)**.

Если флажок снят, то в выборку попадают все устройства, обнаруженные при опросе сети.

По умолчанию флажок снят.

- **Устройство в сети**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** Приложение включает в выборку устройства, которые видимы в сети в настоящий момент.
- **Нет.** Приложение включает в выборку устройства, которые не видимы в сети в

настоящий момент.

- **Значение не выбрано.** Критерий не применяется.

Приложение

В разделе **Приложение** можно настроить критерии включения устройств в выборку на основании выбранного управляемого приложения:

- **Название приложения**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию приложения "Лаборатории Касперского".

В списке представлены названия только тех приложений, для которых на рабочем месте администратора установлены плагины управления.

Если приложение не выбрано, то критерий не применяется.

- **Версия приложения**

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии приложений "Лаборатории Касперского".

Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для приложения наименованию или номеру пакета обновления.

Если поле не заполнено, то критерий не применяется.

- **Последнее обновление модулей приложения**

С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей приложений, установленных на устройствах.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей приложений, установленных на устройствах.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Устройство находится под управлением Kaspersky Security Center**

В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

- **Да.** Приложение включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
- **Нет.** Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
- **Значение не выбрано.** Критерий не применяется.

- **Приложение безопасности установлено**

В раскрывающемся списке можно включить в состав выборки устройства, на которых установлено приложение защиты:

- **Да.** Приложение включает в выборку устройства, на которых установлено

- приложение защиты.
- **Нет.** Приложение включает в выборку устройства, на которых не установлено приложение защиты.
- **Значение не выбрано.** Критерий не применяется.

Операционная система

В разделе **Операционная система** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы.

- **Версия операционной системы**

Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Архитектура операционной системы**

В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Неизвестно, x86, AMD64, IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Версия пакета обновления операционной системы**

В поле можно указать версию пакета установленной операционной системы (в формате X.Y), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Номер сборки операционной системы**

Этот параметр применим только для операционных систем Windows.

Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Идентификатор выпуска операционной системы**

Этот параметр применим только для операционных систем Windows.

Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

Статус устройства

В разделе **Статус устройства** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемого приложения:

- **Статус устройства**

Раскрывающийся список, в котором можно выбрать один из статусов устройства: *ОК, Критический, Предупреждение*.

- **Описание статуса устройства**

В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *ОК*, *Критический*, *Предупреждение*.

- **Статус устройства определен приложением**

Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

Компоненты защиты

В разделе **Компоненты защиты** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

Если флажок установлен, поиск клиентских устройств выполняется по дате выпуска баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

По умолчанию флажок снят.

- **Последняя проверка**

Если флажок установлен, поиск клиентских устройств выполняется по времени последнего поиска вирусов. В полях ввода можно указать интервал, в течение которого поиск вирусов выполнялся в последний раз.

По умолчанию флажок снят.

- **Total number of threats detected**

Если флажок установлен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

По умолчанию флажок снят.

Реестр приложений

В разделе **Реестр приложений** можно настроить критерии включения устройств в выборку в зависимости от того, какие приложения на них установлены:

- **Название приложения**

Раскрывающийся список, в котором можно выбрать приложение. Устройства, на которых установлено указанное приложение, будут включены в выборку.

- **Версия приложения**

Поле ввода, в котором указывается версия выбранного приложения.

- **Поставщик**

Раскрывающийся список, в котором можно выбрать производителя установленного на устройстве приложения.

- **Статус приложения**

Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указано приложение

установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

Если флажок установлен, поиск будет выполняться по данным об обновлении приложений, установленных на искомым устройствах. После установки флажка названия полей ввода **Название приложения** и **Версия приложения** меняются на **Имя обновления** и **Версия обновления**.

По умолчанию флажок снят.

- **Название несовместимого приложения безопасности**

Раскрывающийся список, в котором можно выбрать приложения защиты сторонних производителей. Во время поиска устройства, на которых установлено выбранное приложение, будут включены в выборку.

- **Тег приложения**

В раскрывающемся списке можно выбрать тег приложения. Все устройства, на которых установлены приложения, имеющие выбранный тег в описании, включаются в выборку устройств.

- **Применить к устройствам без выбранных тегов**

Если флажок установлен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

Если флажок снят, критерий не применяется.

По умолчанию флажок снят.

Реестр оборудования

В разделе **Реестр оборудования** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

- **Устройство**

В раскрывающемся списке можно выбрать тип оборудования, которое должно быть установлено на клиентском устройстве, чтобы оно отображалось в результатах поиска.

В поле поддерживается полнотекстовый поиск.

- **Поставщик**

В раскрывающемся списке можно выбрать производителя оборудования, которое должно быть установлено на устройстве, чтобы устройство отображалось в результатах поиска.

В поле поддерживается полнотекстовый поиск.

- **Имя устройства**

Имя устройства в Windows-сети. Устройство с указанным именем будет включено в выборку.

- **Описание**

Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Поставщик устройства**

Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

Название производителя можно ввести в окне свойств устройства.

- **Серийный номер**

Оборудование с серийным номером, указанным в поле, будет включено в выборку.

- **Инвентарный номер**

Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Пользователь**

Оборудование пользователя, указанного в поле, будет включено в выборку.

- **Расположение**

Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

- **Частота процессора (МГц)**

Диапазон частот процессора. Устройства с процессорами, соответствующими диапазону частот в полях ввода (включительно), будут включены в состав выборки.

- **Виртуальных ядер процессора**

Диапазон количества виртуальных ядер процессора. Устройства с процессорами, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ)**

Диапазон значений объема жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ)**

Диапазон значений объема оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону в полях ввода (включительно), будут включены в состав выборки.

Виртуальные машины

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**

В раскрывающемся списке можно выбрать следующие элементы:

- **Да.** Искомые устройства должны являться виртуальными машинами.
- **Нет.** Искомые устройства не должны являться виртуальными машинами.

- **Тип виртуальной машины**

В раскрывающемся списке можно выбрать производителя виртуальной машины.

Раскрывающийся список доступен, если в раскрывающемся списке **Является виртуальной машиной** указано значение **Да**.

- **Часть Virtual Desktop Infrastructure**

В раскрывающемся списке можно выбрать следующие элементы:

- **Да**. Искомые устройства должны являться частью Virtual Desktop Infrastructure.
- **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.

Уязвимости и обновления

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Центра обновления Windows:

WUA переключен на Сервер администрирования

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **Да**. Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Windows Update с Сервера администрирования.
- **Нет**. Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Windows Update из другого источника.

Пользователи

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся указанным пользователем.

- **Пользователь, когда-либо выполнявший вход в систему**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Проблемы, связанные со статусом управляемых приложений

В разделе **Проблемы, связанные со статусом управляемых приложений** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемым приложением. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких приложений, у вас есть возможность автоматически выбрать эту проблему во всех списках.

Описание статуса устройства

Вы можете установить флажки для описаний статусов от управляемого приложения, при получении которых устройства будут включаться в выборку.

Статусы компонентов управляемых приложений

В разделе **Статусы компонентов управляемых приложений** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых приложений:

- **Статус защиты данных от утечек**

Поиск устройств по статусу компонента защиты от утечки данных (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус защиты для серверов совместной работы**

Поиск устройств по статусу компонента защиты для серверов совместной работы (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу компонента антивирусной защиты почтовых серверов (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

Шифрование

Алгоритм шифрования

Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Возможные значения: *AES56, AES128, AES192, AES256*.

Облачные сегменты

В разделе **Облачные сегменты** можно настроить критерии включения устройств в выборку в соответствии с облачными сегментами:

- **Устройство находится в облачном сегменте**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать сегмент поиска.

Если также установлен флажок **Включая вложенные объекты**, то поиск ведется по всем вложенным объектам указанного сегмента.

В результаты поиска включаются устройства только из выбранного сегмента.

- **Устройство обнаружено с помощью API**

В раскрывающемся списке можно выбрать, обнаруживается ли устройство средствами API.

- **Да.** Устройство обнаруживается с помощью AWS API. Это значит, что устройство обязательно находится в облачном окружении.
- **Нет.** Устройство не обнаруживается с помощью AWS API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но по каким-то причинам недоступно для поиска с помощью AWS API.

- **Значение не выбрано.** Критерий не применяется.

Компоненты приложения

Этот раздел содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в Консоли администрирования.

В разделе **Компоненты приложения** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранному приложению:

- **Статус**

Поиск устройств в соответствии со статусом компонента, отправленным управляемым приложением на Сервер администрирования. Вы можете выбрать один из следующих статусов: *Нет данных от устройства*, *Остановлено*, *Запускается*, *Приостановлено*, *Выполняется*, *Сбой* или *Не установлено*. Если выбранный компонент приложения, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

Статусы, отправленные приложениями:

- *Запускается* – компонент в настоящее время находится в процессе инициализации.
- *Выполняется* – компонент включен и работает правильно.
- *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемом приложении.
- *Сбой* – во время выполнения операции компонента произошла ошибка.
- *Остановлено* – компонент отключен и в данный момент не работает.
- *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки приложения.

В отличие от других статусов, статус *Нет данных от устройства* не отправляется управляемым приложением. Этот параметр показывает, что приложения не имеют информации о выбранном статусе компонента. Например, это может произойти, если выбранный компонент не принадлежит ни одному из приложений, установленных на устройстве, или устройство выключено.

- **Версия**

Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, 3.4.1.0, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

Экспорт параметров выборки устройств в файл

► Чтобы экспортировать параметры выборки устройств в текстовый файл:

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки на вкладке **Выборка** выберите нужную вам выборку устройств в списке пользовательских выборок устройств.

Параметры можно экспортировать только из выборок устройств, созданных пользователем.

3. Нажмите на кнопку **Запустить выборку**.
4. На вкладке **Результаты выборки** нажмите на кнопку **Экспортировать параметры**.
5. В открывшемся окне **Сохранить как** задайте имя файла для экспорта параметров выборки, укажите папку, в которую будет сохранен файл, и нажмите на кнопку **Сохранить**.

Параметры выборки устройств будут сохранены в указанный файл.

Создание выборки устройств

► Чтобы создать выборку устройств:

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Создать выборку**.
3. В открывшемся окне **Новая выборка устройств** укажите имя создаваемой выборки и нажмите на кнопку **ОК**.

В результате в дереве консоли в папке **Выборки устройств** будет создана новая папка с указанным вами именем. По умолчанию созданная выборка устройств содержит все устройства, входящие в группы администрирования того Сервера, под управлением которого создана выборка. Чтобы в выборке отображались только интересующие вас устройства, нужно настроить параметры выборки по кнопке **Свойства выборки**.

Создание выборки устройств по импортированным параметрам

► Чтобы создать выборку устройств по импортированным параметрам:

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Импортировать выборку из файла**.
3. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать параметры выборки. Нажмите на кнопку **Открыть**.

В результате в папке **Выборки устройств** будет создана выборка **Новая выборка**. Параметры новой выборки параметры импортированы из указанного файла.

Если в папке **Новая выборка** уже существует выборка с названием **Выборки устройств**, к имени созданной выборки добавится окончание вида (**<порядковый номер>**), например: **(1)**, **(2)**.

Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

► *Чтобы удалить устройства из групп администрирования:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. Выберите устройства, которые требуется удалить, с помощью клавиш **Shift** или **Ctrl**.
3. Удалите выбранные устройства из групп администрирования одним из следующих способов:
 - В контекстном меню любого из выделенных устройств выберите пункт **Удалить**.
 - Нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите значение **Удалить из группы**.

В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Мониторинг установки и удаления приложений

Вы можете контролировать установку и удаление определенных приложений на управляемых устройствах, например, определенного браузера. Чтобы использовать эту функцию, вы можете добавить приложения из реестра приложений в список наблюдаемых приложений. При установке или удалении контролируемого приложения Агент администрирования публикует соответствующие события (см. раздел "Информационные события Агента администрирования" на стр. [676](#)): **Установлено наблюдаемое приложение** или **Удалено наблюдаемое приложение**. Вы можете контролировать эти события, используя, например, выборки событий (на стр. [619](#)) или отчеты (см. раздел "Работа с отчетами" на стр. [602](#)).

Вы можете контролировать эти события, только если они хранятся в базе данных Сервера администрирования.

► *Чтобы добавить приложение в список наблюдаемых приложений:*

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Реестр приложений**.
2. Нажмите на кнопку **Открыть окно свойств реестра приложений** над отобразившимся списком приложений.
3. В открывшемся окне **Наблюдаемые приложения** нажмите на кнопку **Добавить**.
4. В открывшемся окне **Выберите название приложения** в реестре приложений выберите, для каких приложений вы хотите контролировать установку и удаление.
5. В окне **Выберите название приложения** нажмите на кнопку **ОК**.

После того, как вы настроили список контролируемых приложений, и наблюдаемое приложение было установлено или удалено с управляемых устройств в вашей организации, вы можете контролировать соответствующие события, например, с помощью выборки событий Последние события.

События компонентов Kaspersky Security Center

Каждый компонент Kaspersky Security Center имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования Kaspersky Security Center,

Агенте администрирования и Сервере iOS MDM. Типы событий, которые возникают в приложениях "Лаборатории Касперского", в этом разделе не перечислены.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Структура данных описания типа события

Для каждого типа событий отображаются его имя, идентификатор, буквенный код, описание и время хранения по умолчанию.

- **Отображаемое имя типа события.** Этот текст отображается в Kaspersky Security Center, когда вы настраиваете события и при их возникновении.
- **Идентификатор типа события.** Этот цифровой код используется при обработке событий с использованием инструментов анализа событий сторонних производителей.
- **Тип события** (буквенный код). Этот код используется при просмотре и обработке событий с использованием публичных представлений базы данных Kaspersky Security Center и при экспорте событий в SIEM-системы.
- **Описание.** Этот текст содержит описание ситуации при возникновении события и описание того, что вы можете сделать в этом случае.
- **Срок хранения по умолчанию.** Это количество дней, в течение которых событие хранится в базе данных Сервера администрирования и отображается в списке событий Сервера администрирования. После окончания этого периода событие удаляется. Если значение времени хранения события указано 0, такие события регистрируются, но не отображаются в списке событий Сервера администрирования. Если вы настроили хранение таких событий в журнале событий операционной системы, вы можете найти их там.

Можно изменить время хранения событий:

- Консоль администрирования: Настройка срока хранения события (см. раздел "Обработка и хранение событий на Сервере администрирования" на стр. [717](#)).
- Kaspersky Security Center Web Console: Настройка срока хранения события.

Другие данные могут включать следующие поля:

- **event_id:** уникальный номер события в базе данных, генерируемый и присваиваемый автоматически. Его не нужно путать с **Идентификатором типа события**.
- **task_id:** идентификатор задачи, в результате выполнения которой возникло событие (если такая есть).
- **severity:** один из следующих уровней важности (в порядке возрастания важности):
 - 0) Недопустимый уровень важности.
 - 1) Информационное.
 - 2) Предупреждение.
 - 3) Ошибка.
 - 4) Критическое.

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

В этом разделе

Критические события Сервера администрирования	638
События отказа функционирования Сервера администрирования	646
События предупреждения Сервера администрирования	652
Информационные события Сервера администрирования	666

Критические события Сервера администрирования

В таблице ниже приведены типы событий Сервера администрирования Kaspersky Security Center с уровнем важности **Критическое**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Если вы указали порт в окне свойств Сервера администрирования в Консоли администрирования (см. раздел "Шаг 10. Подключение мобильных устройств" на стр. [290](#)), Kaspersky Security Center публикует его метрики и критические события, которые будет получать Prometheus (система мониторинга и оповещения). Prometheus получает метрики и критические события, а затем генерирует алерты для каждого события.

Таблица 62. Критические события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионное ограничение превышено	4099	KLSRV_EV_LICENSE_CHECK_MORE_10	Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц (см. раздел "О лицензионном сертификате" на стр. 343), охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования). Kaspersky Security Center определяет правила генерации событий (см. раздел "События превышения лицензионного ограничения" см. стр. 341) при превышении лицензионного ограничения.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Вирусная атака	26 (для компонента Защита от файловых угроз)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования (см. стр. 718). • Создайте более строгую политику (см. раздел "Автоматическая активация политики по событию "Вирусная атака"" см. стр. 437), которая будет активирована, или создайте задачу (см. раздел "Создание задачи" на стр. 416), которая будет запускаться при возникновении этого события.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Вирусная атака	27 (для компонента Защита от почтовых угроз)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования (см. стр. 718). • Создайте более строгую политику (см. раздел "Автоматическая активация политики по событию "Вирусная атака"" см. стр. 437), которая будет активирована, или создайте задачу (см. раздел "Создание задачи" на стр. 416), которая будет запускаться при возникновении этого события.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Вирусная атака	28 (для сетевого экрана)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования (см. стр. 718). • Создайте более строгую политику (см. раздел "Автоматическая активация политики по событию "Вирусная атака"" см. стр. 437), которая будет активирована, или создайте задачу (см. раздел "Создание задачи" на стр. 416), которая будет запускаться при возникновении этого события.	180 дней
Устройство стало неуправляемым	4111	KLSRV_HOST_OUT_CONTROL	События этого типа возникают, если управляемое устройство видимо в сети, но не подключено к Серверу администрирования в течение заданного периода. Определите, что мешает правильной работе Агента администрирования на устройстве. Возможные причины могут включать проблемы сети и удаление Агента администрирования с устройства.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Статус устройства "Критический"	4113	KLSRV_HOST_STATUS_CRITICAL	События этого типа возникают, если управляемому устройству назначен статус <i>Критический</i> . Вы можете настроить условия (см. раздел "Настройка переключения статусов устройств" на стр. 766) при выполнении которых, статус устройства изменяется на <i>Критический</i> .	180 дней
Файл ключа добавлен в список запрещенных	4124	KLSRV_LICENSE_BLOCKLISTED	События этого типа возникают, если "Лаборатория Касперского" добавила код активации или лицензионный ключ, который вы используете, в запрещенный список. Обратитесь в Службу технической поддержки для получения подробной информации.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Режим ограниченной функциональности	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	События этого типа возникают, если Kaspersky Security Center начинает работать в режиме базовой функциональности (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. 354), без поддержки Управления мобильными устройствами и Системного администрирования. Ниже приведены причины и соответствующие ответы на событие: - Срок действия лицензии истек. Предоставьте лицензию на полную функциональность Kaspersky Security Center (добавьте действительный код активации или файл ключа на Сервер администрирования). - Сервер администрирования управляет большим количеством устройств, чем может использоваться по предоставленной лицензии. Переместите устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера (если лицензионное ограничение другого Сервера не превышено).	180 дней

Срок действия лицензии скоро истекает	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	События этого типа возникают, если приближается дата окончания срока действия коммерческой лицензии (см. раздел "О лицензии" на стр. 342). Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии. События этого типа публикуются за 30 дней, 15 дней, 5 дней и 1 день, до истечения срока действия лицензии. Вы не можете изменить количество дней. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня. После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. 354). Вы можете ответить на событие следующими способами: • Убедитесь, что резервный лицензионный ключ (см. раздел "О лицензионном ключе" на стр. 344) добавлен на Сервер администрирования. • Если вы используете подписку (см. раздел "О подписке" на стр. 345), продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена.	180 дней
Срок действия сертификата истек	4132	KLSRV_CERTIFICATE_EXPIRED	События этого типа возникают, если истекает срок действия сертификата Сервера администрирования для	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			Управления мобильными устройствами. Вам необходимо обновить сертификат, срок действия которого истекает.	
Обновления модулей приложений "Лаборатории Касперского" отозваны	4142	KLSRV_SEAMLESS_UPDATE_REVOKE D	События этого типа возникают, если обновления были отозваны техническими специалистами "Лаборатории Касперского", например, по причине их замены на более новые версии. Для таких обновлений отображается статус <i>Отозвано</i> . Событие не относится к патчам Kaspersky Security Center и не относится к модулям управляемых приложений "Лаборатории Касперского". Событие содержит причину, из-за которой обновления не установлены.	180 дней
Аудит: Не удалось выполнить экспорт в SIEM-систему	5130	KLAUD_EV_SIEM_EXPORT_ERROR	События этого типа возникают при сбое экспорта событий в SIEM-систему из-за ошибки соединения с SIEM-системой.	180 дней

См. также:

События отказа функционирования Сервера администрирования	646
События предупреждения Сервера администрирования	652
О событиях в Kaspersky Security Center	881

События отказа функционирования Сервера администрирования

В таблице ниже приведены типы событий Сервера администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Таблица 63. События отказа функционирования Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Ошибка времени выполнения	4125	KLSRV_RUNTIME_ERROR	События этого типа возникают из-за неизвестных проблем. Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением. Подробную информацию о событии можно найти в его описании.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных приложений превышено ограничение числа установок	4126	KLSRV_INVLICPR OD_EXCEDED	Сервер администрирования генерирует события такого типа периодически (каждый час). События этого типа возникают, если в Kaspersky Security Center вы управляете лицензионными ключами приложений сторонних производителей и если количество установок превысило заданное в лицензионном ключе приложения стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите приложение стороннего производителя с устройств, на которых оно не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять лицензионными ключами приложений сторонних производителей (см. раздел "Управление лицензионными ключами для групп лицензионных приложений" на стр. 588), используя функциональность групп лицензионных приложений. В группу лицензионных приложений входят приложения сторонних производителей, отвечающие заданным вами критериям.	180 дней
Не удалось выполнить опрос облачного сегмента	4143	KLSRV_KLCLOUD _SCAN_ERROR	События этого типа возникают, если Сервер администрирования не может опросить сегмент сети в облачном окружении. Прочтите информацию в описании события и отреагируйте соответствующим образом.	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось выполнить копирование обновлений в заданную папку	4123	KLSRV_UPD_REPL_FAIL	События этого типа возникают, если обновления программного обеспечения копируются в общую папку (или папки). Вы можете ответить на событие следующими способами: • Проверьте, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись. • Проверьте, не были ли изменены имя пользователя и/или пароль к папке (к папкам). • Проверьте подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и модулей приложений (см. раздел "Создание задачи для загрузки обновлений в хранилище Сервера администрирования" на стр. 469).	180 дней
Нет свободного места на диске	4107	KLSRV_DISK_FULL	События этого типа возникают, если на жестком диске устройства, на котором установлен Сервер администрирования, заканчивается дисковое пространство. Освободите дисковое пространство на устройстве.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Общая папка недоступна	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	События этого типа возникают, если общая папка Сервера администрирования (см. раздел "Задание папки общего доступа" на стр. 227) недоступна. Вы можете ответить на событие следующими способами: • Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен. • Проверьте, были ли изменены имя пользователя и/или пароль к папке. • Проверьте подключение к сети.	180 дней
База данных Сервера администрирования недоступна	4109	KLSRV_DATABASE_UNAVAILABLE	События этого типа возникают, если база Сервера администрирования становится недоступной. Вы можете ответить на событие следующими способами: • Проверьте, доступен ли удаленный сервер, на котором установлен SQL-сервер. • Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования. Например, из-за профилактических работ удаленный сервер с установленным SQL Server может быть недоступен.	180 дней

Недостаточно места в базе данных Сервера администрирования	4110	KLSRV_DATABAS E_FULL	События этого типа возникают, если нет свободного места в базе Сервера администрирования. Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие: • Вы используете SQL Server Express Edition: Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования превысила ограничение размера базы данных. Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. • Вы используете СУБД, отличную от SQL Server Express Edition: Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	180 дней

См. также:

Критические события Сервера администрирования	638
События предупреждения Сервера администрирования	652
О событиях в Kaspersky Security Center	881

События предупреждения Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Таблица 64. События предупреждения Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Обнаружено получение частого события		KLSRV_EVENT_SPAM_EVENTS_DETECTED	События этого типа возникают, если Сервер администрирования регистрирует частые события на управляемом устройстве. Дополнительную информацию см. в следующих разделах: Блокировка частых событий (на стр. 678).	90 дней
Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского",	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			установленных на клиентских устройствах, и если количество используемых лицензионных единиц (см. раздел "О лицензионном сертификате" на стр. 343) одной лицензии составляет от 100% до 110% от общего количества единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования). Kaspersky Security Center определяет правила генерации событий (см. раздел "События превышения лицензионного ограничения" см. стр. 341) при превышении лицензионного ограничения.	
Устройство долго не проявляет	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	События этого типа возникают, если управляемое устройство	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
активности в сети			неактивно в течение некоторого времени. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: - Удалите устройство из списка управляемых устройств вручную. - Укажите интервал, по истечении которого создается событие Устройство долго не проявляет активности в сети с помощью Консоли администрирования (см. раздел "Просмотр и настройка действий, когда устройство неактивно" на стр. 683) или с помощью Kaspersky Security Center Web Console. - Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Консоли администрирования (см. раздел "Просмотр и настройка действий, когда устройство неактивно" на стр. 683) или Kaspersky Security Center Web Console.	
Конфликт имен устройств	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			рассматривает два или более управляемых устройства как одно устройство. Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания приложений на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве. Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска (см. раздел "Режим клонирования диска Агента администрирования" на стр. 914) на эталонном устройстве.	
Статус устройства "Предупреждение"	4114	KLSRV_HOST_STATUS_WARNING	События этого типа возникают, если управляемому устройству назначен статус <i>Предупреждение</i>. Вы можете настроить условия (см. раздел "Настройка переключения статусов устройств" на стр. 766) при выполнении которых, статус устройства изменяется на <i>Предупреждение</i>.	90 дней
Для одной из групп лицензионн	4127	KLSRV_INVLICPROD_FILLED	События этого типа возникают, если количество установок	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
ых приложений скоро будет превышено ограничение числа установок			приложений сторонних производителей, включенных в группу лицензионных приложений (см. раздел "Группы приложений" на стр. 571), достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа (см. раздел "Управление лицензионными ключами для групп лицензионных приложений" на стр. 588). Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			производителей (см. раздел "Управление лицензионными ключами для групп лицензионных приложений" на стр. 588), используя функциональность групп лицензионных приложений.	
Сертификат запрошен	4133	KLSRV_CERTIFICATE_REQUESTED	События этого типа возникают, если не удастся автоматически перевыпустить сертификат для Управления мобильными устройствами. Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: - Автоматический перевыпуск был инициирован для сертификата, для которого параметр Автоматически перевыпускать сертификат, если это возможно. Это могло произойти из-за ошибки, которая возникла при создании сертификата. Может потребоваться перевыпуск сертификата вручную. - Если вы используете интеграцию с инфраструктурой открытых ключей, причиной может быть отсутствие атрибута	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			SAM-Account-Name учетной записи, которая используется для интеграции с PKI и для выпуска сертификата. Просмотрите свойства учетной записи.	
Сертификат удален	4134	KLSRV_CERTIFICATE_REMOVED	События этого типа возникают, если администратор удаляет сертификат любого типа (общий, почтовый, VPN) для Управления мобильными устройствами. После удаления сертификата мобильные устройства, подключенные по этому сертификату, не смогут подключиться к Серверу администрирования. Это событие может быть полезно при исследовании неисправностей, связанных с Управлением мобильными устройствами.	90 дней
Срок действия APNs-сертификата истек	4135	KLSRV_APN_CERTIFICATE_EXPIRED	События этого типа происходят, если истекает срок действия APNs-сертификата. Вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM.	Не хранится
Срок действия APNs-сертификата истекает	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	События этого типа возникают, если до истечения срока действия APNs-сертификата остается менее 14 дней.	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			При истечении срока действия APNs-сертификата, вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. Рекомендуется запланировать обновление APNs-сертификата до истечения срока его действия.	
Не удалось отправить FCM-сообщение на мобильное устройство	4138	KLSRV_GCM_DEVICE_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Firebase Cloud Messaging (FCM) для подключения к управляемым мобильным устройствам с операционной системой Android, а FCM-сервер не может обработать некоторые запросы, полученные от Сервера администрирования. Это означает, что некоторые управляемые мобильные устройства не будут получать push-уведомление. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Firebase https://firebase.google.com/	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			docs/cloud-messaging/http-server-ref (см. главу "Downstream message error response codes").	
HTTP-ошибка при отправке FCM-сообщения на FCM-сервер	4139	KLSRV_GCM_HTTP_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Firebase Cloud Messaging (FCM) для подключения управляемых мобильных устройств с операционной системой Android, а FCM-сервер возвращает запрос Серверу администрирования с кодом HTTP, отличным от 200 (ОК). Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Проблемы на стороне FCM-сервера. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Firebase https://firebase.google.com/docs/cloud-messaging/http-server-ref (см. главу	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			"Downstream message error response codes"). Проблемы на стороне прокси-сервера (если вы используете прокси-сервер). Прочтите HTTP код в описании события и ответьте соответствующим образом.	
Не удалось отправить FCM-сообщение на FCM-сервер	4140	KLSRV_GCM_GENERAL_ERROR	События этого типа возникают из-за непредвиденных ошибок на стороне Сервера администрирования при работе с HTTP-протоколом Firebase Cloud Messaging. Прочтите информацию в описании события и отреагируйте соответствующим образом. Если вы не можете найти решение проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки "Лаборатории Касперского".	90 дней
Мало свободного места на жестком диске	4105	KLSRV_NO_SPACE_ON_VOLUMES	События этого типа возникают, если на устройстве, на котором установлен Сервер администрирования, почти закончилось дисковое пространство. Освободите дисковое пространство на устройстве.	90 дней
Мало свободного места в базе	4106	KLSRV_NO_SPACE_IN_DATABASE	События этого типа возникают, если свободное место в базе	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Сервера администрирования			Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие. Вы используете SQL Server Express Edition: • Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования достигла ограничения размера базы данных. • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. Вы используете СУБД, отличную от SQL Server Express Edition: • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	
Разорвано соединение с подчиненным Сервером администрирования	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с подчиненным Сервером администрирования. Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Разорвано соединение с главным Сервером администрирования	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с главным Сервером администрирования. Прочтите журнал событий Kaspersky Event Log на	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			устройстве, на котором установлен главный Сервер администрирования, и отреагируйте соответствующим образом.	
Зарегистрированы новые обновления модулей приложений "Лаборатории Касперского"	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	События этого типа возникают, если Сервер администрирования регистрирует новые обновления приложений "Лаборатории Касперского", установленных на управляемых устройствах, для установки которых требуется одобрение. Одобрите или отклоните обновления с помощью Консоли администрирования (см. раздел "Одобрение и отклонение обновлений программного обеспечения" на стр. 505) или Kaspersky Security Center Web Console.	90 дней
Превышено ограничение числа событий, началось удаление событий из базы данных	4145	KLSRV_EVP_DB_TRUNCATING	События такого типа возникают, если удаление старых событий из базы данных Сервера администрирования началось после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования (см. раздел "Обработка и хранение событий на Сервере администрирования" на стр. 717).	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			Вы можете ответить на событие следующими способами: - Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования. - Сократите список событий для хранения в базе данных Сервера администрирования.	
Превышено ограничение числа событий, удалены события из базы данных	4146	KLSRV_EVP_DB_TRUNCATE D	События такого типа возникают, если старые события удалены из базы данных Сервера администрирования после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования (см. раздел "Обработка и хранение событий на Сервере администрирования" на стр. 717). Вы можете ответить на событие следующими способами: - Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования. - Сократите список событий для хранения в базе данных Сервера администрирования.	Не хранится

См. также:

Критические события Сервера администрирования	638
События отказа функционирования Сервера администрирования	646
О событиях в Kaspersky Security Center	881

Информационные события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Информационное сообщение**.

Таблица 65. Информационные события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Лицензионный ключ использован более чем на 90%	4097	KLSRV_EV_LICENSE_CHECK_90	30 дней	
Обнаружено новое устройство	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 дней	
Устройство автоматически добавлено в группу	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 дней	
Устройство было автоматически перемещено с помощью правила	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 дней	
Устройство удалено из группы: долгое отсутствие активности в сети	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 дней	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Для одной из групп лицензионных приложений число разрешенных установок исчерпано более чем на 95%	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 дней	
Появились файлы для отправки на анализ в "Лабораторию Касперского"	4131	KLSRV_APS_FILE_APPEARED	30 дней	
Идентификатор экземпляра FCM мобильного устройства изменен	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 дней	
Обновления успешно скопированы в заданную папку	4122	KLSRV_UPD_REPL_OK	30 дней	
Установлено соединение с подчиненным Сервером администрирования	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 дней	
Установлено соединение с главным Сервером администрирования	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 дней	
Базы обновлены	4144	KLSRV_UPD_BASES_UPDATED	30 дней	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Аудит: Подключение к Серверу администрирования	4147	KLAUD_EV_SERVERCONNECT	30 дней	
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	30 дней	Это событие отслеживает изменения в следующих объектах: • группах администрирования; • группах безопасности; • пользователях; • инсталляционных пакетах; • задачах; • политиках; • Серверах; • виртуальный Сервер.
Аудит: Изменение статуса объекта	4150	KLAUD_EV_TASK_STATE_CHANGED	30 дней	Например, это событие возникает, если задача завершилась ошибкой.
Аудит: Изменение параметров группы	4149	KLAUD_EV_ADMGROUP_CHANGED	30 дней	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Аудит: Подключение к Серверу администрирования было прервано	4151	KLAUD_EV_SERVERDISCONNECT	30 дней	
Аудит: Свойства объекта были изменены	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 дней	Это событие отслеживает изменения в следующих параметрах: • пользователь; • лицензия; • Сервер; • виртуальный Сервер.
Аудит: Права пользователя были изменены	4153	KLAUD_EV_OBJECTACLMODIFIED	30 дней	
Аудит: Импорт или экспорт ключей шифрования с Сервера администрирования	5100	KLAUD_EV_DPEKEYSEXPORT	30 дней	

События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

В этом разделе

События отказа функционирования Агента администрирования	670
События предупреждения Агента администрирования	674
Информационные события Агента администрирования	676

События отказа функционирования Агента администрирования

В таблице ниже приведены типы событий Агента администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Таблица 66. События отказа функционирования Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Ошибка при установке обновления	7702	KLNAG_EV_PATCH_INSTALL_ERROR	События этого типа возникают, если автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center (на стр. 487) прошла unsuccessfully. Событие не относится к обновлениям управляемых приложений "Лаборатории Касперского". Прочтите описание события. Причиной этого события может быть проблема операционной системы Windows на Сервере администрирования. Если в описании упоминается какая-либо проблема конфигурации Windows, устраните эту проблему.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось установить обновление стороннего производителя	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	События этого типа возникают, если используются возможности Системного администрирования и Управления мобильными устройствами (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. 354), и если обновление программного обеспечения сторонних производителей (см. раздел "Установка обновлений приложений сторонних производителей" на стр. 498) прошло unsuccessfully. Проверьте, корректна ли ссылка на приложение стороннего производителя. Прочтите описание события.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось установить обновления Центра обновления Windows	7717	KLNAG_EV_WUA_INSTALL_ERROR	События этого типа возникают, если обновления Центра обновления Windows были unsuccessful. Настройте обновления Microsoft Windows в политике Агента администрирования (см. раздел "Настройка обновлений Windows в политике Агента администрирования" на стр. 526). Прочтите описание события. Поищите описание ошибки в базе знаний Microsoft. Обратитесь в службу технической поддержки Microsoft, если вы не можете решить проблему самостоятельно.	30 дней
Управление учетными записями: ошибки	7723	KLNAG_EV_USR_MNG_ERR	Общее событие предупреждения.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось восстановить файл sudoers до референсного значения	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Событие содержит описание ошибки замены файла sudoers.	30 дней
Не удалось установить корневые сертификаты	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Событие содержит описание ошибки установки сертификатов.	30 дней
Не удалось удалить корневые сертификаты	7730	KLNAG_EV_ROOT_CERT_REMOVAL_ERR	Событие содержит описание ошибки удаления сертификатов.	30 дней

См. также:

События предупреждения Агента администрирования[674](#)

Информационные события Агента администрирования[676](#)

События предупреждения Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Таблица 67. События предупреждения Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Возвращено предупреждение во время установки обновлений модулей приложений	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 дней
Установка обновления стороннего ПО завершена с предупреждением	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 дней
Установка обновления стороннего программного обеспечения отложена	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 дней
Произошла проблема безопасности	549	GNRL_EV_APP_INCIDENT_OCCURED	30 дней
Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 дней
Управление учетными записями: предупреждения	7722	KLNAG_EV_USR_MNG_WRN	30 дней
Обнаружен файл sudoers, который не соответствует референсному значению	7724	KLNAG_EV_SUDOER_DIFFERENT	30 дней

См. также:

События отказа функционирования Агента администрирования	670
Информационные события Агента администрирования	676

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Таблица 68. Информационные события Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Обновление модулей приложений успешно установлено	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления модулей приложений	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 дней
Установлено приложение	7703	KLNAG_EV_INV_APP_INSTALLED	30 дней
Приложение удалено	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 дней
Установлено наблюдаемое приложение	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 дней
Удалено наблюдаемое приложение	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 дней
Установлено стороннее приложение	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Новое устройство добавлено	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Устройство удалено	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Обнаружено новое устройство	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство авторизовано	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней
Совместный доступ к рабочему столу Windows: файл был прочитан	7712	KLUSRLOG_EV_FILE_READ	30 дней
Совместный доступ к рабочему столу Windows: файл был изменен	7713	KLUSRLOG_EV_FILE_MODIFIED	30 дней
Совместный доступ к рабочему столу Windows: приложение было запущено	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 дней
Совместный доступ к рабочему столу Windows: предоставлен	7715	KLUSRLOG_EV_WDS_BEGIN	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Совместный доступ к рабочему столу Windows: завершен	7716	KLUSRLOG_EV_WDS_END	30 дней
Обновление для приложений стороннего производителя установлено успешно	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления стороннего ПО	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 дней
Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно	7719	KSNPROXY_STARTED_CON_CHK_OK	30 дней
Прокси-сервер KSN остановлен	7720	KSNPROXY_STOPPED	30 дней

См. также:

- События отказа функционирования Агента администрирования[670](#)
- События предупреждения Агента администрирования[674](#)

Блокировка частых событий

В этом разделе представлена информация о частых событиях, блокировке отмене блокировки частых событий, экспорте списка частых событий в файл.

В этом разделе

О блокировке частых событий	679
Управление блокировкой частых событий	680
Отмена блокировки частых событий	680
Экспорт списка частых событий в файл	681

О блокировке частых событий

Управляемое приложение, например Kaspersky Endpoint Security для Windows, установленное на одном или нескольких управляемых устройствах, может отправлять на Сервер администрирования множество однотипных событий. Прием частых событий может привести к перегрузке базы данных Сервера администрирования и перезаписи других событий. Сервер администрирования начинает блокировать наиболее частые события, когда количество всех полученных событий превышает установленное ограничение для базы данных.

Сервер администрирования автоматически блокирует получение частых событий. Вы не можете заблокировать частые события самостоятельно или выбрать, какие события заблокировать.

Заблокированные события можно проверить в свойствах Сервера администрирования в разделе **Блокировка частых событий**. Если событие заблокировано, можно выполнить следующие действия:

- Если вы хотите предотвратить перезапись базы данных, вы можете продолжать блокировать (см. раздел "Управление блокировкой частых событий" на стр. [680](#)) получение событий такого типа.
- Если вы хотите, например, выяснить причину отправки частых событий на Сервер администрирования, вы можете разблокировать (см. раздел "Управление блокировкой частых событий" на стр. [680](#)) частые события и в любом случае продолжить получение событий этого типа.
- Если вы хотите продолжать получать частые события до тех пор, пока они снова не будут заблокированы, вы можете отменить блокировку (см. раздел "Отмена блокировки частых событий" на стр. [680](#)) частых событий.

См. также:

Управление блокировкой частых событий	680
Отмена блокировки частых событий	680

Управление блокировкой частых событий

Сервер администрирования автоматически блокирует получение частых событий, но вы можете отменить блокировку и продолжать получать частые сообщения. Также можно заблокировать получение частых событий, которые вы разблокировали ранее.

► Чтобы управлять блокировкой частых событий:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Блокировка частых событий**.
3. В разделе **Блокировка частых событий**:
 - Выберите параметр **Тип события** для событий, получение которых вы хотите заблокировать.
 - Отмените выбор параметра **Тип события** для событий, которые вы хотите получать и дальше.
4. Нажмите на кнопку **Применить**.
5. Нажмите на кнопку **ОК**.

Сервер администрирования получает частые события, для которых вы отменили выбор параметра **Тип события**, и блокирует получение частых событий, для которых вы выбрали параметр **Тип события**.

См. также:

О блокировке частых событий [679](#)

Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует этот тип частых событий.

► Чтобы отменить блокировку частых событий:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Блокировка частых событий**.
3. В разделе **Блокировка частых событий** нажмите строку частого события, для которого вы хотите отменить блокировку.
4. Нажмите на кнопку **Удалить**.

Частое событие удаляется из списка частых событий. Сервер администрирования будет получать события этого типа.

См. также:

О блокировке частых событий [679](#)

Экспорт списка частых событий в файл

► Чтобы экспортировать список частых событий в файл:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Блокировка частых событий**.
3. Нажмите на кнопку **Экспортировать в файл**.
4. В открывшемся окне **Сохранить как** укажите путь к файлу, в которых вы хотите сохранить список.
5. Нажмите на кнопку **Сохранить**.

Все записи списка частых событий экспортируются в файл.

См. также:

О блокировке частых событий	679
Управление блокировкой частых событий	680

Контроль изменения состояния виртуальных машин

Сервер администрирования хранит информацию о состоянии управляемых устройств, например, реестр оборудования и список установленных приложений, параметры управляемых приложений, задач и политик. Если управляемым устройством является виртуальная машина, пользователь может в любой момент восстановить ее состояние из образа виртуальной машины (snapshot), сделанного ранее. В результате информация о состоянии виртуальной машины на Сервере администрирования может стать неактуальной.

Например, администратор создал политику защиты на Сервере администрирования в 12:00, которая начала работать на виртуальной машине VM_1 в 12:01. В 12:30 пользователь виртуальной машины VM_1 изменил ее статус, восстановив ее из снимка, сделанного в 11:00. Политика защиты перестает работать на виртуальной машине. Однако на Сервере администрирования сохранится неактуальная информация о том, что политика защиты на виртуальной машине VM_1 продолжает действовать.

Kaspersky Security Center позволяет контролировать изменение состояния виртуальных машин.

После каждой синхронизации с устройством Сервер администрирования формирует уникальный идентификатор, который хранится как на устройстве, так и на Сервере администрирования. Перед началом следующей синхронизации Сервер администрирования сравнивает значения идентификаторов на обеих сторонах. Если значения идентификаторов не совпадают, Сервер администрирования считает виртуальную машину восстановленной из образа. Сервер администрирования сбрасывает действующие для этой виртуальной машины параметры политик и задач и отправляет на нее актуальные политики и список групповых задач.

Отслеживание состояния антивирусной защиты с помощью информации в системном реестре

- Чтобы отследить состояние антивирусной защиты на клиентском устройстве с помощью информации, записанной Агентом администрирования в системный реестр, в зависимости от операционной системы устройства:
- На устройствах под управлением Windows:
 - Откройте системный реестр клиентского устройства (например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**).
 - Перейдите в раздел:
 - для 32-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState
 - для 64-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

В результате в системном реестре отобразится информация о состоянии антивирусной защиты клиентского устройства.
 - На устройствах под управлением Linux:
 - Информация содержится в отдельных текстовых файлах, по одному для каждого типа данных, расположенных /var/opt/kaspersky/klagent/1103/1.0.0.0/Statistics/AVState/.
 - На устройствах под управление macOS:
 - Информация содержится в отдельных текстовых файлах, по одному для каждого типа данных, расположенных /Library/Application Support/Kaspersky Lab/klagent/Data/1103/1.0.0.0/Statistics/AVState/.

Состояние антивирусной защиты соответствует значениям ключей, описанных в таблице ниже.

Таблица 69. Ключи реестра и их возможные значения

Ключ (тип данных)	Значение	Описание
Protection_LastConnected (REG_SZ)	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) последнего соединения с Сервером администрирования.
Protection_AdmServer (REG_SZ)	IP, DNS-имя или NetBIOS-имя	Имя Сервера администрирования, который управляет устройством.
Protection_NagentVersion (REG_SZ)	a.b.c.d	Номер сборки Агента администрирования, установленного на устройстве.
Protection_NagentFullVersion (REG_SZ)	a.b.c.d (патч1; патч2; ...; патчN)	Номер версии Агента администрирования (с патчами), установленного на устройстве.

Ключ (тип данных)	Значение	Описание
Protection_HostId (REG_SZ)	Идентификатор устройства	Идентификатор устройства.
Protection_DynamicVM (REG_DWORD)	0 – нет 1 – да	Агент администрирования установлен в динамический режим для VDI.
Protection_AvInstalled (REG_DWORD)	0 – нет 1 – да	Приложение безопасности установлено на устройстве.
Protection_AvRunning (REG_DWORD)	0 – нет 1 – да	Постоянная защита устройства включена.
Protection_HasRtp (REG_DWORD)	0 – нет 1 – да	Установлен компонент постоянной защиты.
Protection_RtpState (REG_DWORD)	Статус постоянной защиты:	
	0	Неизвестно.
	1	Выключен
	2	Приостановлена.
	3	Запускается.
	4	Включен.
	5	Включен с высоким уровнем защиты (максимальная защита).
	6	Включен с низким уровнем защиты (максимальная скорость).
	7	Включен с параметрами по умолчанию (рекомендуемые параметры).
	8	Включен с пользовательскими параметрами.
	9	Сбой в работе.
Protection_LastFscan (REG_SZ)	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) последней полной проверки.
Protection_BasesDate (REG_SZ)	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) выпуска баз приложения.

Просмотр и настройка действий, когда устройство неактивно

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

- Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования:

1. Нажмите правой клавишей мыши на название требуемой группы администрирования.
2. В контекстном меню выберите пункт **Свойства**.
Откроется окно свойств группы администрирования.
3. В окне **Свойства** перейдите в раздел **Устройства**.
4. При необходимости включите или выключите следующие параметры:

- **Уведомлять администратора, если устройство неактивно больше (сут)**

Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

По умолчанию параметр включен.

- **Удалять устройство из группы, если оно неактивно больше (сут)**

Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. Временной интервал, установленный по умолчанию, составляет 60 дней.

По умолчанию параметр включен.

- **Наследовать из родительской группы**

Если флажок установлен, параметры в этом разделе будут наследоваться из родительской группы, в которую входит клиентское устройство. Если флажок установлен, параметры в блоке параметров **Активность устройств в сети** недоступны для изменения.

Этот параметр доступен только для группы администрирования, у которой есть родительская группа администрирования.

По умолчанию параметр включен.

- **Обеспечить принудительное наследование для дочерних групп**

Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

По умолчанию параметр выключен.

5. Нажмите на кнопку **ОК**.

Ваши изменения сохранены и применены.

Выключение объявлений "Лаборатории Касперского"

В Kaspersky Security Center Web Console раздел объявлений "Лаборатории Касперского" (**Мониторинг и отчеты** → **Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center и управляемых приложениях, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Объявления "Лаборатории Касперского" включают в себя информацию двух типов: объявления, связанные с безопасностью, и рекламные объявления. Вы можете выключить объявления каждого типа отдельно.

► *Чтобы выключить объявления, связанные с безопасностью:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно выключить объявления, связанные с безопасностью.
2. В контекстном меню объекта выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервера администрирования в разделе **Объявления "Лаборатории Касперского"** выберите вариант **Включить отображение объявлений "Лаборатории Касперского"** в Kaspersky Security Center Web Console.
4. Нажмите на кнопку **ОК**.

Объявления "Лаборатории Касперского" выключены.

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN (см. раздел "Включение и отключение KPSN" на стр. [875](#)).

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.
Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область действия политик задается с помощью тегов, местоположения устройств в подразделениях Active Directory, членства в группах безопасности Active Directory (см. раздел "Иерархия политик, использование профилей политик" на стр. [431](#)) и прочего.
- Задание области действия групповых задач.
Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.
- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.
- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- Один офис.
- Множество небольших изолированных офисов.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455
Основной сценарий установки	56

В этом разделе

Типовая конфигурация точек распространения: один офис	686
Типовая конфигурация точек распространения: множество небольших удаленных офисов	687
Назначение управляемого устройства точкой распространения	688
Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне	691
Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения	692
Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения	693
Автоматическое назначение точек распространения	694
О локальной установке Агента администрирования на устройство, выбранное точкой распространения	694
Об использовании точки распространения в качестве шлюза соединений	695
Добавление IP-диапазонов в список диапазонов, опрашиваемых точкой распространения	696
Использование точки распространения в качестве извещающего сервера	697

Типовая конфигурация точек распространения: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных частей (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Можно

использовать автоматическое назначение точек распространения, либо назначать точки распространения вручную.

- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение точек распространения и в каждой выделенной части сети назначить одно или несколько устройств точками распространения на корневую группу администрирования, например, на группу **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracer.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского" [455](#)

Типовая конфигурация точек распространения: множество небольших удаленных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).

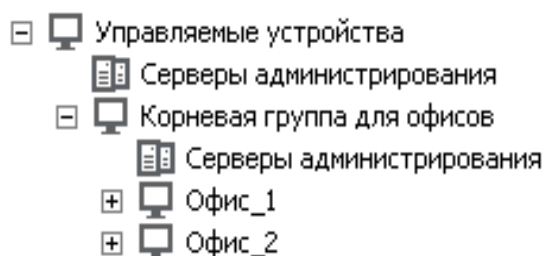


Рисунок 1. Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить одну или несколько точек распространения. Точками распространения нужно назначать устройства удаленного офиса, имеющие достаточно места на диске. Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутому выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Ноутбук, находившийся в группе администрирования **Офис 1**, но физически перемещенный в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения

окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

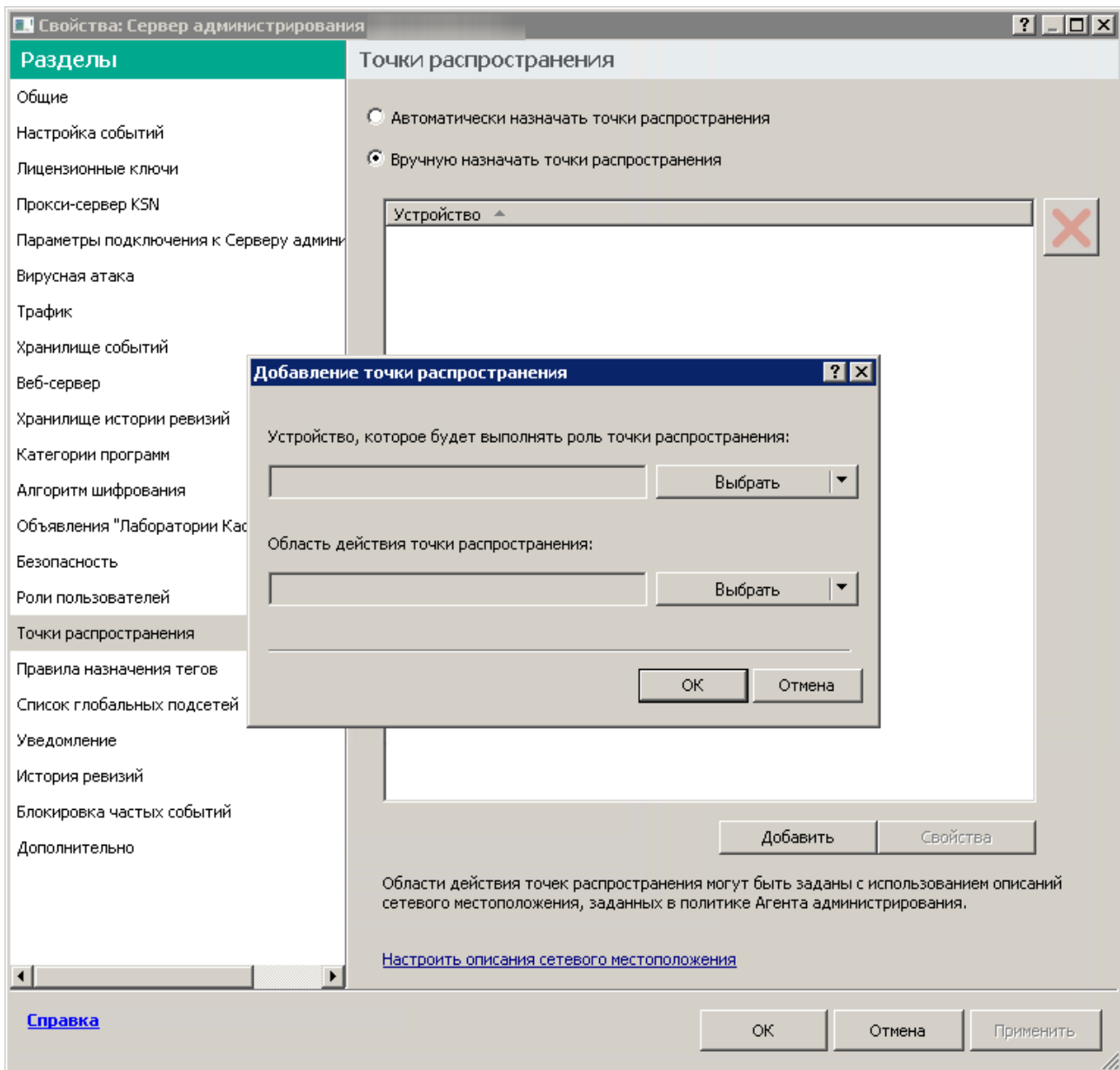
Назначение управляемого устройства точкой распространения

Вы можете вручную назначить устройство точкой распространения для группы администрирования и настроить ее как шлюз соединений в Консоли администрирования.

► *Чтобы назначить устройство точкой распространения группы администрирования:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В правой части окна выберите параметр **Вручную назначать точки распространения**.

5. Нажмите на кнопку **Добавить**.

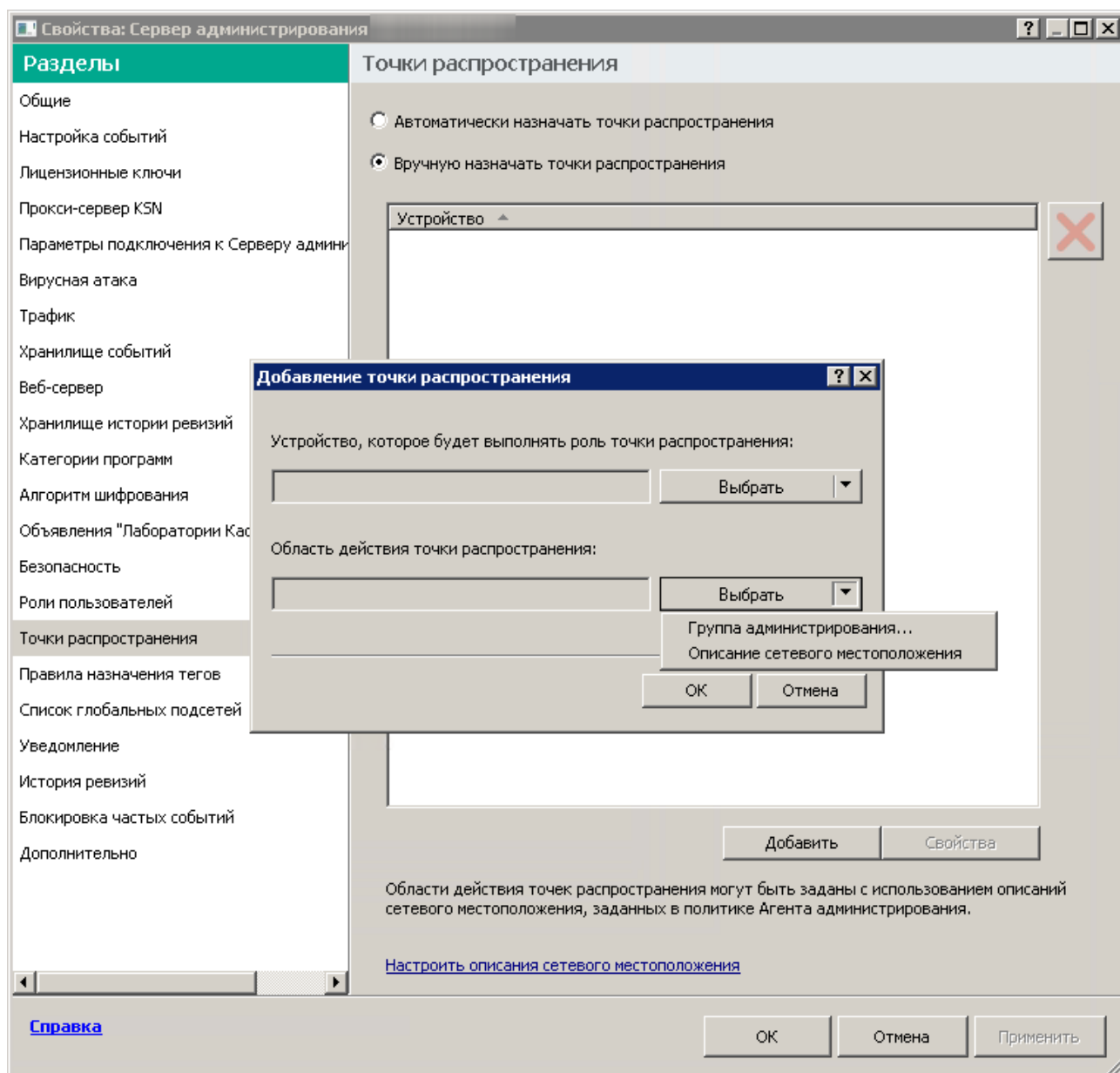


Откроется окно **Добавление точки распространения**.

6. В окне **Добавление точки распространения** выполните следующие действия:

- В разделе **Устройство выполняет роль точки распространения** нажмите на стрелку вниз (▼) рядом с кнопкой **Выбрать** и выберите вариант **Добавить устройство из группы**.
- В открывшемся окне **Выбрать устройства** выберите устройство, которое будет выполнять роль точки распространения.
- В разделе **Область действия точки распространения** нажмите на стрелку вниз (▼) рядом с разворачивающейся кнопкой **Выбрать**.
- Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.

е. Нажмите на кнопку **ОК**, чтобы закрыть окно **Добавление точки распространения**.



Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

Первое устройство с установленным Агентом администрирования, которое подключится к виртуальному Серверу администрирования, будет автоматически назначено точкой распространения и настроено в качестве шлюза соединений.

См. также:

Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения..[693](#)

Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне

► Чтобы подключить устройство под управлением Linux в качестве шлюза в демилитаризованной зоне (DMZ):

1. Загрузите и установите Агент администрирования на устройство Linux (см. раздел "Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)" см. стр. [195](#)).

2. Запустите послеустановочный скрипт и следуйте указаниям мастера, чтобы настроить конфигурацию локальной среды. В командной строке выполните следующую команду:

```
$ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

3. На шаге с запросом режима Агента администрирования выберите параметр **Использовать как шлюз соединения**.

4. В открывшемся окне свойств Сервера администрирования выберите раздел **Точки распространения**.

5. В открывшемся окне **Точки распространения** в правой части окна:

a. Выберите параметр **Вручную назначать точки распространения**.

b. Нажмите на кнопку **Добавить**.

Откроется окно **Добавление точки распространения**.

6. В окне **Добавление точки распространения** выполните следующие действия:

a. В разделе **Устройство выполняет роль точки распространения** нажмите на стрелку вниз () рядом с разворачивающейся кнопкой **Выбрать** и выберите вариант **Добавить шлюз соединений, находящийся в демилитаризованной зоне, по адресу**.

b. В разделе **Область действия точки распространения** нажмите на стрелку вниз () рядом с разворачивающейся кнопкой **Выбрать**.

c. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования.

d. Нажмите на кнопку **ОК**, чтобы закрыть окно **Добавление точки распространения**.

7. Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

8. Запустите утилиту klnagchk, чтобы проверить, успешно ли настроено соединение с Kaspersky Security Center. В командной строке введите команду:

```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

9. В главном меню перейдите в Kaspersky Security Center и найдите устройство (см. раздел "Обнаружение устройств" на стр. [324](#)).

10. В появившемся окне нажмите на <Имя устройства>.

11. В раскрывающемся списке выберите ссылку **Переместить в группу**.

12. В открывшемся окне **Выбрать группу** перейдите по ссылке **Точки распространения**.

13. Нажмите на кнопку **ОК**.

14. Перезапустите службу Агента администрирования на клиенте Linux, выполнив в командной строке команду:

```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
```

Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне завершено.

После этого вы можете подключить устройство под управлением Linux к Серверу администрирования (см. раздел "Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения" см. стр. [692](#)) с помощью настроенного шлюза соединения. Выполняйте эти процедуры только после завершения основного сценария установки (см. раздел "Основной сценарий установки" на стр. [56](#)).

См. также:

Сценарий: подключение автономных устройств через шлюз соединения[297](#)

Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения

Шлюз соединения позволяет подключать клиентские устройства из демилитаризованной зоны (DMZ) к Серверу администрирования. Устройства на базе Windows (см. раздел "Сценарий: подключение автономных устройств через шлюз соединения" см. стр. [297](#)) и на базе Linux (см. раздел "Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне" см. стр. [691](#)) могут выступать в качестве шлюза соединения. После того как вы подключили и настроили шлюз соединения (см. раздел "Об использовании точки распространения в качестве шлюза соединений" на стр. [695](#)), вы можете использовать этот шлюз для подключения устройства под управлением Linux к Серверу администрирования. Выполняйте процедуру, описанную ниже, только после завершения основного сценария установки (см. раздел "Основной сценарий установки" на стр. [56](#)).

- Чтобы подключить устройство под управлением Linux к Серверу администрирования с помощью шлюза соединения, выполните на этом устройстве следующие действия:

1. Загрузите и установите Агент администрирования на устройство Linux (см. раздел "Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)" см. стр. [195](#)).
2. Запустите послеустановочный скрипт Агента администрирования, выполнив в командной строке следующую команду:

```
$ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

3. На шаге с запросом режима Агента администрирования выберите параметр **Подключаться к Серверу через шлюз соединений** и введите адрес шлюза соединения.
4. Проверьте соединение с Kaspersky Security Center и шлюзом соединения распространения с помощью следующей команды в командной строке:

```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

В выходных данных отображается адрес шлюза соединения.

Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения завершено. Вы можете использовать это устройство для распространения обновлений, для удаленной установки приложений и для получения информации о сетевых устройствах.

См. также:

Сценарий: подключение автономных устройств через шлюз соединения[297](#)

Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения

Шлюз соединения (см. стр. [54](#)) ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования. Это означает, что сразу после установки шлюза соединения на устройстве в демилитаризованной зоне Сервер администрирования не перечисляет устройство среди управляемых устройств. Следовательно, вам потребуется особая процедура, чтобы Сервер администрирования инициировал соединение со шлюзом соединения.

► Чтобы добавить устройство со шлюзом соединения в качестве точки распространения:

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В правой части окна выберите параметр **Вручную назначать точки распространения**.
5. Нажмите на кнопку **Добавить**.

Откроется окно **Добавление точки распространения**.

6. В окне **Добавление точки распространения** выполните следующие действия:
 - a. В разделе **Устройство выполняет роль точки распространения** нажмите на стрелку вниз () рядом с разворачивающейся кнопкой **Выбрать** и выберите вариант **Добавить шлюз соединения, находящийся в демилитаризованной зоне, по адресу**.
 - b. В открывшемся окне **Ввод адреса шлюза соединений** введите IP-адрес шлюза соединения (или введите имя, если шлюз соединения доступен по имени).
 - c. В разделе **Область действия точки распространения** нажмите на стрелку вниз () рядом с разворачивающейся кнопкой **Выбрать**.
 - d. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.

Рекомендуется создать отдельную группу для внешних управляемых устройств.

После того, как вы выполнили это действие, список точек распространения содержит новую запись с именем **Временная запись для шлюза соединений**.

Сервер администрирования практически сразу пытается подключиться к шлюзу соединения по указанному адресу. В случае успеха имя записи меняется на имя устройства шлюза соединения. Этот процесс занимает до пяти минут.

Пока временная запись для шлюза соединения преобразуется в именованную запись, шлюз соединения также появляется в группе **Нераспределенные устройства**.

Чтобы добавить шлюз соединения в ранее настроенную сеть, переустановите Агент администрирования на устройствах, которые вы хотите подключить к вновь добавленному шлюзу соединения.

См. также:

Назначение управляемого устройства точкой распространения	688
Сценарий: подключение автономных устройств через шлюз соединения	297

Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения.

► Чтобы назначить точки распространения автоматически:

1. Откройте главное окно приложения.
2. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется автоматически назначать точки распространения.
3. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
4. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Точки распространения**.
5. В правой части окна выберите параметр **Автоматически назначать точки распространения**.

Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

6. Нажмите на кнопку **ОК**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455

О локальной установке Агента администрирования на устройство, выбранное точкой распространения

Чтобы устройство, выбранное точкой распространения, могло напрямую связаться с виртуальным Сервером администрирования для выполнения роли шлюза соединений, на это устройство требуется локально установить Агент администрирования.

Порядок локальной установки Агента администрирования на устройство, выбранное точкой распространения, совпадает с порядком локальной установки Агента администрирования на любое устройство сети.

Для устройства, выбранного точкой распространения, должны быть выполнены следующие условия:

- В процессе локальной установки Агента администрирования в окне мастера установки **Сервер администрирования** в поле **Адрес Сервера** требуется указать адрес виртуального Сервера администрирования, под управлением которого находится устройство. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.

Используется следующая форма записи адреса виртуального Сервера: <Полный адрес физического Сервера администрирования, которому подчинен виртуальный Сервер>/<Имя виртуального Сервера администрирования>.

- Для выполнения роли шлюза соединений на устройстве должны быть открыты все порты, необходимые для связи с Сервером администрирования.

В результате установки на устройство Агента администрирования с указанными параметрами приложение Kaspersky Security Center автоматически выполняет следующие действия:

- включает это устройство в группу **Управляемые устройства** виртуального Сервера администрирования;
- назначает это устройство точкой распространения группы **Управляемые устройства** виртуального Сервера администрирования.

Необходимо и достаточно выполнить локальную установку Агента администрирования на устройстве, назначенном точкой распространения группы **Управляемые устройства** в сети организации. На устройства, выполняющие роль точек распространения во вложенных группах администрирования, Агент администрирования можно установить удаленно. Для этого используйте точку распространения группы **Управляемые устройства** в качестве шлюза соединений.

См. также:

Локальная установка Агента администрирования.....	193
Приложения "Лаборатории Касперского". Централизованное развертывание	357

Об использовании точки распространения в качестве шлюза соединений

Если Сервер администрирования находится вне демилитаризованной зоны (DMZ), Агенты администрирования, находящиеся в демилитаризованной зоне, теряют возможность соединения с ним.

Для соединения Сервера администрирования с Агентами администрирования в качестве шлюза соединений можно использовать точку распространения. Точка распространения предоставляет Серверу администрирования порт для создания соединения. В момент запуска Сервер администрирования подключается к точке распространения и не разрывает соединение с ней в течение всего времени работы.

Получив сигнал от Сервера администрирования, точка распространения посылает Агентам администрирования UDP-сигнал на подключение к Серверу администрирования. При получении сигнала

Агенты администрирования подключаются к точке распространения, которая передает информацию между Агентом администрирования и Сервером администрирования. Обмен информацией может происходить по IPv4-сети или IPv6-сети.

Рекомендуется использовать в качестве шлюза соединений выделенное устройство и назначать на один шлюз соединений не более 10 000 клиентских устройств (включая мобильные устройства).

► *Чтобы добавить шлюз соединения в ранее настроенную сеть:*

1. Установите Агент администрирования в режиме шлюза соединения.
2. Переустановите Агент администрирования на устройствах, которые вы хотите подключить к вновь добавленному шлюзу соединения.

См. также:

Назначение управляемого устройства точкой распространения.....	688
Локальная установка Агента администрирования.....	193

Добавление IP-диапазонов в список диапазонов, опрашиваемых точкой распространения

Вы можете добавить IP-диапазон в список диапазонов, опрашиваемых точкой распространения.

► *Чтобы добавить IP-диапазон в список опрашиваемых диапазонов:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В списке выберите требуемую точку распространения и нажмите на кнопку **Свойства**.
5. В открывшемся окне свойств точки распространения в панели **Разделы** выберите раздел **Обнаружение устройств → IP-диапазоны**.
6. Установите флажок **Разрешить опрос диапазона**.
7. Нажмите на кнопку **Добавить**.
Кнопка **Добавить** активна, если установлен флажок **Разрешить опрос диапазона**.
Откроется окно **IP-диапазон**.
8. В окне **IP-диапазон** введите имя нового IP-диапазона (по умолчанию указано имя Новый диапазон).
9. Нажмите на кнопку **Добавить**.
10. Выполните одно из следующих действий:
 - Задайте IP-диапазон начальным и конечным IP-адресом.
 - Задайте IP-диапазон адресом и маской подсети.
 - Нажмите на кнопку **Обзор** и добавьте подсеть из глобального списка подсетей (см. раздел "Глобальный список подсетей" на стр. [966](#)).

11. Нажмите на кнопку **ОК**.
 12. Нажмите на кнопку **ОК**, чтобы добавить диапазон с заданным именем.
- Новый диапазон отобразится в списке опрашиваемых диапазонов.

Использование точки распространения в качестве извещающего сервера

В Kaspersky Security Center точка распространения может работать как push-сервер (см. раздел "Использование точки распространения в качестве извещающего сервера" на стр. [697](#)) для устройств, которые управляются по мобильному протоколу, и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой из них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Push-сервер поддерживает нагрузку до 50 000 одновременных подключений.

Возможно, вы захотите использовать точки распространения в качестве push-серверов, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Постоянное соединение необходимо для некоторых операций, таких как запуск и остановка локальных задач, получение статистики для управляемого приложения или создание туннеля. Если вы используете точку распространения в качестве сервера push-сервера, вам не нужно использовать параметр **Не разрывать соединение с Сервером администрирования** на управляемых устройствах или отправлять пакеты на UDP-порт Агента администрирования.

► *Чтобы использовать точку распространения в качестве push-сервера:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В списке выберите требуемую точку распространения и нажмите на кнопку **Свойства**.
5. В открывшемся окне свойств точки распространения в разделе **Общие** в панели **Разделы** выберите параметр **Использовать точку распространения в качестве push-сервера**.
6. Укажите номер порта push-сервера, то есть того порта на точке распространения, который клиентские устройства будут использовать для подключения.
По умолчанию номер порта – 13295.
7. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств точки распространения.
8. Откройте окно свойств политики Агента администрирования (см. раздел "Параметры политики Агента администрирования" см. стр. [789](#)).

9.

В разделе **Подключения** перейдите в подраздел **Сети**.
10.

В подразделе **Сеть** выберите вариант **Использовать точку распространения для принудительного подключения к Серверу администрирования**.
11.

Нажмите на кнопку **ОК**, чтобы закрыть окно.
- Точка распространения начинает выполнять роль push-сервера. Теперь он может отправлять push-уведомления на клиентские устройства.

Если вы управляете устройствами с установленной операционной системой KasperskyOS или планируете это сделать, вам нужно использовать точку распространения в качестве push-сервера. Вы также можете использовать точку распространения в качестве push-сервера, если хотите отправлять push-уведомления на клиентские устройства.

См. также:

Обновление программного обеспечения на клиентском устройстве с помощью точки распространения.....	109
Порты, используемые Kaspersky Security Center	63
Точка распространения	51
Настройка точек распространения и шлюзов соединений	685

Другие повседневные задачи

Этот раздел содержит рекомендации о ежедневной работе с Kaspersky Security Center.

В этом разделе

Управление Серверами администрирования	699
Управление группами администрирования	742
Управление клиентскими устройствами	747
Управление учетными записями пользователей	803
Удаленная установка операционных систем и приложений	843
Работа с ревизиями объектов	852
Удаление объектов	858
Хранилища данных	861
Kaspersky Security Network и Kaspersky Private Security Network	873
Переключение между онлайн-справкой и офлайн-справкой	878

Управление Серверами администрирования

Этот раздел содержит информацию о работе с Серверами администрирования и о настройке параметров Сервера администрирования.

В этом разделе

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования	700
Подключение к Серверу администрирования и переключение между Серверами администрирования	703
Права доступа к Серверу администрирования и его объектам	706
Условия подключения к Серверу администрирования через интернет	707
Защищенное подключение к Серверу администрирования	707
Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования	708
Использование утилиты klsclflag для закрытия порта 13291	710
Отключение от Сервера администрирования	711
Добавление Сервера администрирования в дерево консоли	711
Удаление Сервера администрирования из дерева консоли	711
Добавление виртуального Сервера администрирования в дерево консоли	711
Смена учетной записи службы Сервера администрирования. Утилита klsrvswch	712
Изменение учетных данных СУБД	714
Решение проблем с узлами Сервера администрирования	714
Просмотр и изменение параметров Сервера администрирования	715
Массовая передача устройств между серверами	721
Перенос данных мобильных устройств между серверами	721
Резервное копирование и восстановление параметров Сервера администрирования	721
Резервное копирование и восстановление данных Сервера администрирования	723
Перенос Сервера администрирования на другое устройство	729
Избегание конфликтов между Серверами администрирования	732
Двухэтапная проверка	732

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер". Добавление возможно независимо от того, доступен ли Сервер, который вы хотите сделать подчиненным, для подключения через Консоль администрирования.

При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен. Порт 13291 необходим для приема подключений от Консоли администрирования к Серверу администрирования (см. раздел "Сервер администрирования и Консоль администрирования" на стр. [107](#)).

Подключение Сервера администрирования в качестве подчиненного к главному Серверу

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера с подключением к главному Серверу по порту 13000. Вам потребуется устройство с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования:

► *Чтобы добавить Сервер администрирования, доступный для подключения через Консоль, в качестве подчиненного Сервера:*

1. Убедитесь, что порт 13000 поддерживаемого главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.
2. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.
3. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.
4. В рабочей области узла **Серверы администрирования** выбранной группы перейдите по ссылке **Добавить подчиненный Сервер администрирования**.
Запустится мастер добавления подчиненного Сервера администрирования.
5. На первом шаге мастера (ввод адреса Сервера администрирования, добавляемого в группу) введите сетевое имя будущего подчиненного Сервера администрирования.
6. Следуйте далее указаниям мастера.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Подчиненный Сервер будет принимать подключение от главного Сервера (см. раздел "Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования" на стр. [111](#)).

Если у вас нет устройства с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования (например, если будущий подчиненный Сервер находится в удаленном офисе, а системный администратор удаленного офиса из соображений безопасности не делает доступным порт 13291 через интернет), вы все равно можете добавить подчиненный Сервер.

► *Чтобы добавить Сервер администрирования, недоступный для подключения через Консоль, в качестве подчиненного Сервера:*

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для подключения от подчиненных Серверов администрирования.
2. Запишите файл сертификата будущего главного Сервера администрирования на внешнее устройство (например, съемный диск) либо перешлите системному администратору того удаленного офиса, в котором находится Сервер администрирования.

Файл сертификата Сервера администрирования находится на Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Запишите файл сертификата будущего подчиненного Сервера администрирования на внешнее устройство (например, съемный диск). Если будущий подчиненный Сервер находится в удаленном офисе, попросите системного администратора удаленного офиса переслать вам сертификат.

Файл сертификата Сервера администрирования находится на Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.

5. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.
6. Нажмите на кнопку **Добавить подчиненный Сервер администрирования** в рабочей области узла **Серверы администрирования**.
Запустится мастер добавления подчиненного Сервера администрирования.
7. На первом шаге мастера (ввод адреса) оставьте поле **Адрес подчиненного Сервера администрирования (необязательно)** пустым.
8. В окне **Файл сертификата подчиненного Сервера администрирования** нажмите на кнопку **Обзор** и выберите сохраненный ранее файл сертификата подчиненного Сервера.
9. После завершения работы мастера подключитесь с помощью другой Консоли администрирования к будущему подчиненному Серверу администрирования. Если этот Сервер находится в удаленном офисе, попросите системного администратора удаленного офиса подключиться к будущему подчиненному Серверу администрирования и выполнить на нем дальнейшие шаги.
10. В контекстном меню узла **Сервер администрирования** выберите **Свойства**.
11. В свойствах Сервера администрирования перейдите в раздел **Дополнительно** и затем в раздел **Иерархия Серверов администрирования**.
12. Установите флажок **Данный Сервер администрирования является подчиненным в иерархии**.
Поля ввода станут доступными для ввода и редактирования.
13. В поле **Адрес главного Сервера администрирования** введите сетевое имя будущего главного Сервера администрирования.
14. Выберите ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.
15. Нажмите на кнопку **ОК**.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Вы сможете подключаться к подчиненному Серверу через Консоль администрирования. Подчиненный Сервер будет принимать подключение от главного Сервера (см. раздел "Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования" на стр. [111](#)).

Подключение главного Сервера администрирования к подчиненному Серверу

Вы можете добавить новый Сервер администрирования в качестве подчиненного Сервера так, чтобы главный Сервер подключался к подчиненному Серверу по порту 13000. Это целесообразно, например, если вы размещаете подчиненный Сервер в демилитаризованной зоне.

Вам потребуется устройство с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования:

► *Чтобы добавить новый Сервер администрирования в качестве подчиненного и подключить главный Сервер к нему по порту 13000:*

1. Убедитесь, что порт 13000 будущего подчиненного Сервера доступен для приема подключений от главного Сервера администрирования.
2. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.
3. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.

4. В рабочей области узла **Серверы администрирования** нужной группы администрирования перейдите по ссылке **Добавить подчиненный Сервер администрирования**.
Запустится мастер добавления подчиненного Сервера администрирования.
5. На первом шаге мастера (ввод адреса Сервера администрирования, добавляемого в группу) введите сетевое имя будущего подчиненного Сервера администрирования, и установите флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.
6. Если вы подключаетесь к будущему подчиненному Серверу через прокси-сервер, на первом шаге мастера установите флажок **Использовать прокси-сервер** и введите параметры подключения.
7. Следуйте далее указаниям мастера.

Будет установлена иерархия Серверов администрирования. Подчиненный Сервер будет принимать подключение от главного Сервера (см. раздел "Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне" на стр. [112](#)).

См. также:

Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне	112
Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования	111
Порты, используемые Kaspersky Security Center	63

Подключение к Серверу администрирования и переключение между Серверами администрирования

При запуске приложение Kaspersky Security Center предпринимает попытку соединения с Сервером администрирования. Если в сети существует несколько Серверов администрирования, запрашивается тот Сервер, с которым было установлено соединение во время предыдущего сеанса работы приложения Kaspersky Security Center.

Если приложение запускается в первый раз после установки, выполняется попытка соединения с Сервером администрирования, указанным при установке Kaspersky Security Center.

После соединения с Сервером администрирования структура папок этого Сервера отображается в дереве консоли.

Если в дерево консоли добавлено несколько Серверов администрирования, вы можете переключаться между ними.

Для работы с каждым Сервером администрирования необходима Консоль администрирования. Перед первым подключением к новому Серверу администрирования убедитесь, что на нем открыт порт 13291, по которому принимаются подключения от Консоли (см. раздел "Сервер администрирования и Консоль администрирования" на стр. [107](#)), и все остальные порты для связи Сервера администрирования с другими компонентами Kaspersky Security Center (см. раздел "Порты, используемые Kaspersky Security Center" на стр. [63](#)).

► *Чтобы переключиться на другой Сервер администрирования:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню узла Сервера администрирования выберите пункт **Подключиться к Серверу администрирования**.
3. В открывшемся окне **Параметры подключения** в поле **Адрес Сервера администрирования** укажите имя Сервера администрирования, к которому вы хотите подключиться. В качестве имени Сервера администрирования вы можете указать IP-адрес или имя устройства в сети Windows. При нажатии на кнопку **Дополнительно** в нижней части окна вы можете настроить параметры подключения к Серверу администрирования (см. рис. ниже).

Для подключения к Серверу администрирования через порт, отличный от установленного по умолчанию, в поле **Адрес Сервера администрирования** требуется ввести значение в формате <Имя Сервера администрирования>:<Порт>.

Чтобы подключиться к виртуальному Серверу администрирования, введите значение в поле **Адрес Сервера администрирования** в формате <Адрес Сервера администрирования>/<имя виртуального Сервера>.

Пользователям, не обладающим правами на **Чтение**, будет отказано в доступе к Серверу администрирования.

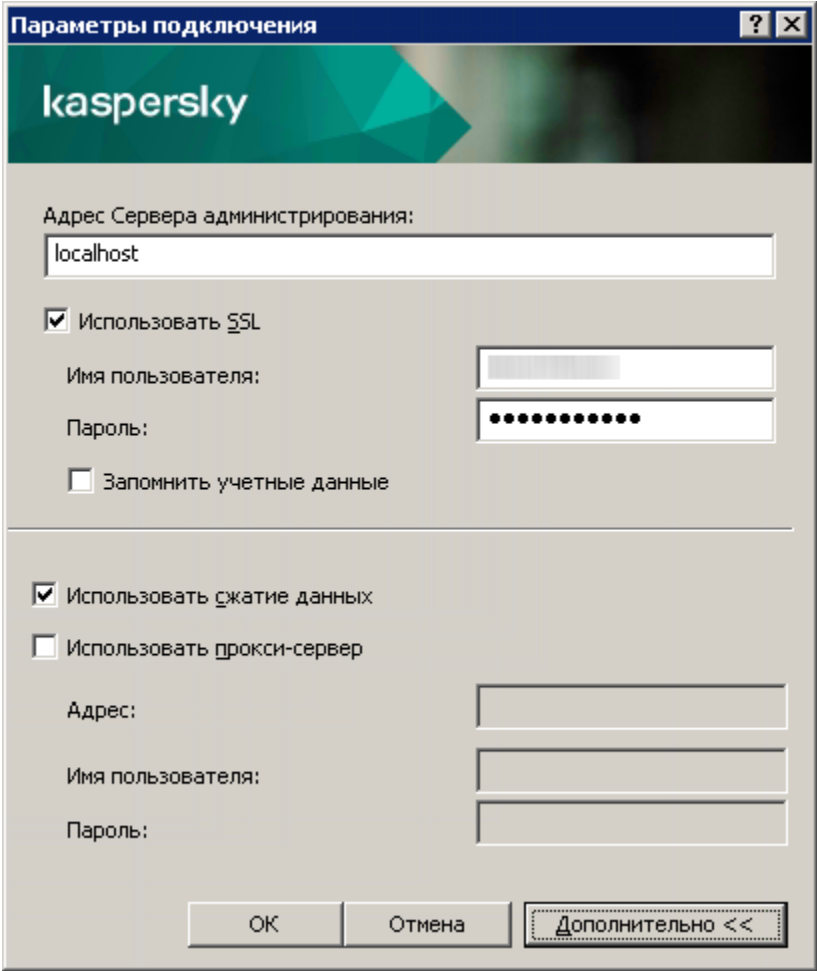


Рисунок 2. Установка соединения с Сервером администрирования

4. Нажмите на кнопку **ОК** для завершения переключения между Серверами.
- После соединения с Сервером администрирования структура папок соответствующего ему узла в дереве консоли обновляется.

См. также:

Порты, используемые Kaspersky Security Center	63
Сервер администрирования и Консоль администрирования	107

Права доступа к Серверу администрирования и его объектам

Группы пользователей **KLAdmins** и **KLOperators** создаются автоматически во время установки Kaspersky Security Center. Этим группам предоставляются права на подключение к Серверу администрирования и на работу с его объектами.

В зависимости от того, под какой учетной записью проводится установка Kaspersky Security Center, группы **KLAdmins** и **KLOperators** создаются следующим образом:

- Если установка проводится под учетной записью пользователя, входящего в домен, группы создаются в домене, в который входит Сервер администрирования, и на Сервере администрирования.
- Если установка проводится под учетной записью системы, группы создаются только на Сервере администрирования.

Просмотр групп **KLAdmins** и **KLOperators** и внесение необходимых изменений в права пользователей групп **KLAdmins** и **KLOperators** можно осуществлять при помощи стандартных средств администрирования операционной системы.

Группе **KLAdmins** предоставлены все права, группе **KLOperators** – права на чтение и выполнение. Набор прав, предоставленных группе **KLAdmins**, недоступен для изменения.

Пользователи, входящие в группу **KLAdmins**, называются администраторами Kaspersky Security Center, пользователи из группы **KLOperators** – *операторами Kaspersky Security Center*.

Помимо пользователей, входящих в группу **KLAdmins**, права администратора Kaspersky Security Center предоставляются локальным администраторам устройств, на которых установлен Сервер администрирования.

Локальных администраторов можно исключать из списка пользователей, имеющих права администратора Kaspersky Security Center.

Все операции, запущенные администраторами Kaspersky Security Center, выполняются с правами учетной записи Сервера администрирования.

Для каждого Сервера администрирования в сети можно сформировать свою группу **KLAdmins**, обладающую правами только в рамках работы с этим Сервером.

Если устройства, относящиеся к одному домену, входят в группы администрирования разных Серверов, то администратор домена является администратором Kaspersky Security Center в рамках всех этих групп администрирования. Группа **KLAdmins** для этих групп администрирования едина и создается при установке первого Сервера администрирования. Операции, запущенные администратором Kaspersky Security Center, выполняются с правами учетной записи того Сервера администрирования, для которого они запущены.

После установки приложения администратор Kaspersky Security Center может выполнять следующие действия:

- изменять права, предоставляемые группам **KLOperators**;
- определять права доступа к функциям приложения Kaspersky Security Center другим группам безопасности и отдельным пользователям, зарегистрированным на рабочем месте администратора;
- определять права доступа пользователей к работе в каждой группе администрирования.

Администратор Kaspersky Security Center может назначать права доступа к каждой группе администрирования или к другим объектам Сервера администрирования в разделе **Безопасность** окна свойств выбранного объекта.

Вы можете отследить действия пользователя при помощи записей о событиях в работе Сервера администрирования. Записи о событиях отображаются в узле **Сервер администрирования** на вкладке **События**. Эти события имеют уровень важности **Информационные события**; типы событий начинаются со слова **Аудит**.

См. также:

Изменения в системе после установки Kaspersky Security Center[271](#)

Условия подключения к Серверу администрирования через интернет

Если Сервер администрирования является удаленным, то есть находится вне сети организации, клиентские устройства подключаются к нему через интернет.

Для подключения устройств к Серверу администрирования через интернет должны быть выполнены следующие условия:

- Удаленный Сервер администрирования должен иметь внешний IP-адрес, и на нем должен быть открыт входящий порт 13000 (для подключения от Агентов администрирования). Рекомендуется также открыть порт UDP 13000 (для приема уведомлений о выключении устройств).
- На устройствах должны быть установлены Агенты администрирования.
- При установке Агента администрирования на устройства должен быть указан внешний IP-адрес удаленного Сервера администрирования. Если для установки используется инсталляционный пакет, внешний IP-адрес требуется указать вручную в свойствах инсталляционного пакета в разделе **Параметры**.
- Для управления приложениями и задачами устройства с помощью удаленного Сервера администрирования требуется установить флажок **Не разрывать соединение с Сервером администрирования** в окне свойств этого устройства в разделе **Общие**. После установки флажка необходимо дождаться синхронизации Сервера администрирования с удаленным устройством. Непрерывное соединение с Сервером администрирования могут поддерживать не более 300 клиентских устройств одновременно.

Для ускорения выполнения задач, поступающих от удаленного Сервера администрирования, можно открыть на устройстве порт 15000. В этом случае для запуска задачи Сервер администрирования посылает специальный пакет Агенту администрирования по порту 15000, не дожидаясь синхронизации с устройством.

Защищенное подключение к Серверу администрирования

Обмен информацией между клиентскими устройствами и Сервером администрирования, а также подключение Консоли администрирования к Серверу администрирования могут производиться с использованием протокола TLS (Transport Layer Security). Протокол TLS позволяет идентифицировать стороны, взаимодействующие при подключении, осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. В основе протокола TLS лежит аутентификация взаимодействующих сторон и шифрование данных по методу открытых ключей.

В этом разделе

Аутентификация Сервера при подключении устройства	708
Аутентификация Сервера при подключении Консоли администрирования	708

Аутентификация Сервера при подключении устройства

При первом подключении клиентского устройства к Серверу администрирования Агент администрирования на устройстве получает копию сертификата Сервера администрирования и сохраняет его локально.

При локальной установке Агента администрирования на устройство сертификат Сервера администрирования можно выбрать вручную.

На основании полученной копии сертификата осуществляется проверка прав и полномочий Сервера администрирования при следующих соединениях.

В дальнейшем, при каждом подключении устройства к Серверу администрирования Агент администрирования запрашивает сертификат Сервера администрирования и сравнивает его с локальной копией. Если они не совпадают, доступ Сервера администрирования к устройству не разрешается.

Аутентификация Сервера при подключении Консоли администрирования

При первом подключении к Серверу администрирования Консоль администрирования запрашивает сертификат Сервера администрирования и сохраняет его копию локально на рабочем месте администратора. На основании полученной копии сертификата при последующих подключениях Консоли администрирования к этому Серверу администрирования осуществляется идентификация Сервера администрирования.

Если сертификат Сервера администрирования не совпадает с копией сертификата, хранящейся на рабочем месте администратора, Консоль администрирования выводит запрос на подтверждение подключения к Серверу администрирования с заданным именем и на получение нового сертификата. После подключения Консоль администрирования сохраняет копию нового сертификата Сервера администрирования, которая будет использоваться для идентификации Сервера в дальнейшем.

Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования

По умолчанию пользователи могут войти в Kaspersky Security Center с любого устройства, на котором они могут открыть Kaspersky Security Center Web Console или на котором установлена Консоль администрирования на основе консоли Microsoft Management Console (MMC). Настроить Сервер администрирования можно таким образом, чтобы пользователи могли подключаться к нему только с устройств с разрешенными IP-адресами. В этом случае, даже если злоумышленник похитит учетную запись Kaspersky Security Center, он не сможет войти в Kaspersky Security Center, так как IP-адрес устройства злоумышленника отсутствует в списке разрешенных.

IP-адрес проверяется, когда пользователь входит в Kaspersky Security Center или запускает приложение, которое взаимодействует с Сервером администрирования через Kaspersky Security Center OpenAPI. В этот момент устройство пользователя пытается установить соединение с Сервером администрирования. Если

IP-адрес устройства отсутствует в списке разрешенных, возникает ошибка аутентификации и событие KLAUD_EV_SERVERCONNECT уведомляет о том, что соединение с Сервером администрирования не установлено.

Требования к списку разрешенных IP-адресов

IP-адреса проверяются только при попытке подключения к Серверу администрирования следующих приложений:

- Сервер Kaspersky Security Center Web Console
Если вы входите в Web Console на одном устройстве, а Сервер Web Console установлен на другом устройстве, вы можете настроить сетевой экран на устройстве с Сервером Web Console штатными средствами операционной системы. Тогда, если кто-то попытается войти в Web Console, сетевой экран поможет предотвратить вмешательство злоумышленников.
- Консоль администрирования.
- Приложения, взаимодействующие с Сервером администрирования через объекты автоматизации klakaut.
- Приложения, взаимодействующие с Сервером администрирования через OpenAPI, такие как Kaspersky Anti Targeted Attack Platform или Kaspersky Security для виртуальных сред.

Поэтому укажите адреса устройств, на которых установлены перечисленные выше приложения.

Вы можете установить IPv4-адреса и IPv6-адреса. Указать диапазоны IP-адресов невозможно.

Как создать список разрешенных IP-адресов

Если вы еще не установили список разрешенных, следуйте приведенным ниже инструкциям.

► Чтобы создать список разрешенных IP-адресов для входа в Kaspersky Security Center:

1. На устройстве Сервера администрирования запустите командную строку под учетной записью с правами администратора.
2. Измените текущую директорию на папку установки Kaspersky Security Center (обычно это <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).
3. Введите следующую команду, используя права администратора:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v  
"<IP addresses>" -t s
```

Укажите IP-адреса, соответствующие перечисленным выше требованиям. Несколько IP-адресов должны быть разделены точкой с запятой.

Пример того, как разрешить подключение к Серверу администрирования только одному устройству:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v  
"192.0.2.0" -t s
```

Пример того, как разрешить нескольким устройствам подключаться к Серверу администрирования:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v  
"192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
```

4. Перезапустите службу Сервера администрирования.

Узнать, успешно настроен список разрешенных IP-адресов, можно в журнале событий Kaspersky Event Log на Сервере администрирования.

Как изменить список разрешенных IP-адресов

Вы можете изменить список разрешенных точно так же, как и при его создании. Для этого выполните ту же команду и укажите новый список разрешенных:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v  
"<IP addresses>" -t s
```

Если вы хотите удалить некоторые IP-адреса из списка разрешенных, перепишите его. Например, ваш список разрешенных включает следующие IP-адреса: 192.0.2.0; 198.51.100.0; 203.0.113.0. Вы хотите удалить IP-адрес 198.51.100.0. Для этого в командной строке введите следующую команду:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v  
"192.0.2.0; 203.0.113.0" -t s
```

Не забудьте перезапустить службу Сервера администрирования.

Как сбросить настроенный список разрешенных IP-адресов

► *Чтобы сбросить уже настроенный список разрешенных IP-адресов:*

1. Введите следующую команду в командной строке с правами администратора:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v  
"" -t s
```

2. Перезапустите службу Сервера администрирования.

После этого IP-адреса больше не проверяются.

Использование утилиты klscflag для закрытия порта 13291

Порт 13291 Сервера администрирования используется для приема подключений от Консолей администрирования. По умолчанию порт открыт. Если вы не хотите использовать Консоль администрирования на основе консоли Microsoft Management Console (MMC) или утилиту klakaut, вы можете закрыть этот порт с помощью утилиты klscflag. Эта утилита изменяет значение параметра KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

► *Чтобы закрыть порт 13291:*

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Выполните следующую команду в командной строке:

```
klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN  
-sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

3. Перезапустите службу Сервера администрирования Kaspersky Security Center.

Порт 13291 закрыт.

► *Чтобы проверить, был ли успешно закрыт порт 13291:*

Выполните следующую команду в командной строке:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN  
-svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

Эта команда возвращает следующий результат:

```
+--- (PARAMS_T)  
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

Значение `false` означает, что порт закрыт. В противном случае отображается значение `true`.

Отключение от Сервера администрирования

► *Чтобы отключиться от Сервера администрирования:*

1. В дереве консоли выберите узел, соответствующий Серверу администрирования, от которого нужно отключиться.
2. В контекстном меню узла выберите пункт **Отключиться от Сервера администрирования**.

Добавление Сервера администрирования в дерево консоли

► *Чтобы добавить в дерево консоли Сервер администрирования:*

1. В главном окне приложения Kaspersky Security Center выберите в дереве консоли узел **Kaspersky Security Center**.
2. В контекстном меню узла выберите пункт **Новый** → **Сервер администрирования**.

В результате в дереве консоли будет создан узел с именем **Сервер администрирования – <Имя устройства> (Не подключен)**, с которого вы можете подключиться к любому из установленных в сети Серверов администрирования.

Удаление Сервера администрирования из дерева консоли

► *Чтобы удалить Сервер администрирования из дерева консоли:*

1. В дереве консоли выберите узел, соответствующий удаляемому Серверу администрирования.
2. В контекстном меню узла выберите пункт **Удалить**.

Добавление виртуального Сервера администрирования в дерево консоли

► *Чтобы добавить в дерево консоли виртуальный Сервер администрирования:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования, для которого нужно создать виртуальный Сервер администрирования.
2. В узле Сервера администрирования выберите папку **Серверы администрирования**.
3. В рабочей области папки **Серверы администрирования** перейдите по ссылке **Добавить виртуальный Сервер администрирования**.

Запустится мастер создания виртуального Сервера администрирования.

4. В окне **Имя виртуального Сервера администрирования** укажите имя создаваемого виртуального Сервера.

Имя виртуального Сервера администрирования не может превышать 255 символов и содержать специальные символы ("*<>?\\:|).

5. В окне **Ввод адреса подключения устройств к виртуальному Серверу** укажите адрес подключения устройств.

Адрес подключения виртуального Сервера администрирования – это сетевой адрес, по которому к нему будут подключаться устройства. Адрес подключения состоит из двух частей: сетевого адреса физического Сервера администрирования и имени виртуального Сервера, разделенных символом косой черты (слешем). Имя виртуального Сервера будет подставлено автоматически. Указанный адрес будет использоваться на этом виртуальном Сервере как адрес по умолчанию в установочных пакетах Агента администрирования.

6. В окне **Создание учетной записи администратора виртуального Сервера** назначьте администратором виртуального Сервера пользователя из списка или добавьте новую учетную запись для администратора по кнопке **Создать**.

Вы можете указать несколько учетных записей.

В результате в дереве консоли будет создан узел с именем **Сервер администрирования – <Имя виртуального Сервера>**.

Смена учетной записи службы Сервера администрирования. Утилита klsrvswch

Если вам требуется изменить учетную запись службы Сервера администрирования, заданную при установке приложения Kaspersky Security Center, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования klsrvswch.

При установке Kaspersky Security Center утилита автоматически копируется в папку установки приложения.

Количество запусков утилиты не ограничено.

Вам нужно запустить утилиту klsrvswch на устройстве Сервера администрирования под учетной записью с правами администратора, которая использовалась для установки Сервера администрирования.

Утилита klsrvswch позволяет менять тип учетной записи. Например, если вы используете локальную учетную запись, вы можете сменить ее на доменную учетную запись либо на управляемую учетную запись службы (и наоборот). Утилита klsrvswch не позволяет изменить тип учетной записи на групповую управляемую учетную запись службы (gMSA).

Windows Vista и более поздние версии Windows не позволяют использовать учетную запись LocalSystem для Сервера администрирования. В этих версиях операционных систем Windows учетная запись **LocalSystem** неактивна.

► *Чтобы изменить учетную запись службы Сервера администрирования на доменную учетную запись:*

1. Запустите утилиту klsrvswch из папки установки Kaspersky Security Center. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

В результате запускается мастер изменения учетной записи службы Сервера администрирования. Следуйте далее указаниям мастера.

2. В окне **Учетная запись службы Сервера администрирования** выберите **Учетная запись LocalSystem**.

В результате работы мастера учетная запись Сервера администрирования изменяется. Служба Сервера администрирования запустится под учетной записью LocalSystem и будет использовать ее учетные данные.

Для правильной работы Kaspersky Security Center требуется, чтобы учетная запись для запуска службы Сервера администрирования обладала правами администратора ресурса для размещения информационной базы Сервера администрирования.

► *Чтобы изменить учетную запись службы Сервера администрирования на учетную запись пользователя или на управляемую учетную запись службы:*

1. Запустите утилиту klsrvswch из папки установки Kaspersky Security Center. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

В результате запускается мастер изменения учетной записи службы Сервера администрирования. Следуйте далее указаниям мастера.

2. В окне **Учетная запись службы Сервера администрирования** выберите **Учетная запись пользователя**.

3. Нажмите на кнопку **Найти**.

Откроется окно **Выбор пользователя**.

4. В окне **Выбор пользователя** нажмите на кнопку **Типы объекта**.

5. В списке типов объекта выберите **Пользователи** (если вы хотите использовать учетную запись пользователя) или **Учетная запись для служб** (если вы хотите использовать управляемую учетную запись службы) и нажмите на кнопку **ОК**.

6. В поле для имени объекта введите имя учетной записи или часть имени и нажмите на кнопку **Проверить имена**.

7. В списке соответствующих имен выберите необходимое имя и нажмите на кнопку **ОК**.

8. Если вы выбрали **Учетные записи служб**, в окне **Пароль учетной записи**, оставьте поля **Пароль** и **Подтверждение пароля** пустыми. Если вы выбрали **Пользователи**, введите пароль для пользователя и подтвердите его.

Учетная запись службы Сервера администрирования будет запускаться под выбранной вами учетной записью.

При использовании Microsoft SQL-сервера в режиме аутентификации учетной записи пользователя средствами Windows требуется обеспечить доступ к базе данных. Учетная запись пользователя должна быть владельцем базы данных Kaspersky Security Center. По умолчанию требуется использовать схему dbo.

Изменение учетных данных СУБД

Иногда может потребоваться изменить учетные данные СУБД, например, чтобы выполнить ротацию учетных данных в целях безопасности.

► Чтобы изменить учетные данные СУБД в среде Windows с помощью утилиты `klsrvswch.exe`:

1. Запустите утилиту `klsrvswch`, которая расположена в папке установки Kaspersky Security Center. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Вам нужно запустить утилиту `klsrvswch` на устройстве Сервера администрирования под учетной записью с правами администратора, которая использовалась для установки Сервера администрирования.

2. Нажимайте на кнопку **Далее** мастера, пока не дойдете до шага **Изменить учетные данные для доступа к СУБД**.
3. На шаге мастера **Изменить учетные данные для доступа к СУБД** выполните следующие действия:
 - Выберите параметр **Применить новые учетные данные**.
 - Укажите новое имя учетной записи в поле **Учетная запись**.
 - Укажите новый пароль для учетной записи в поле **Пароль**.
 - Подтвердите новый пароль в поле **Подтвердить пароль**.

Вам нужно указать учетные данные учетной записи, которая существует в СУБД.

4. Нажмите на кнопку **Далее**.

После завершения работы мастера учетные данные СУБД изменяются.

Решение проблем с узлами Сервера администрирования

Дерево в левой панели Консоли администрирования содержит узлы, соответствующие Серверам администрирования. Вы можете добавить в дерево консоли столько Серверов администрирования, сколько вам нужно (см. раздел "Добавление Сервера администрирования в дерево консоли" на стр. [711](#)).

Консоль управления Microsoft Management Console (MMC) сохраняет список узлов Сервера администрирования в дереве консоли в теневую копию файла `.msc`. Теневая копия этого файла хранится в папке `%USERPROFILE%\AppData\Roaming\Microsoft\MMC\` на устройстве, на котором установлена Консоль администрирования. Для каждого узла Сервера администрирования в файле содержится следующая информация:

- Адрес Сервера администрирования.
- Номер порта.
- используется ли TLS.

Этот параметр зависит от номера порта (см. раздел "Настройка подключения Консоли администрирования к Серверу администрирования" на стр. [296](#)), используемого для подключения Консоли администрирования к Серверу администрирования.

- Имя пользователя.
- сертификат Сервера администрирования.

Устранение неисправностей

При подключении Консоли администрирования к Серверу администрирования (см. раздел "Аутентификация Сервера при подключении Консоли администрирования" на стр. [708](#)) сохраненный локально сертификат сравнивается с сертификатом Сервера администрирования. Если сертификаты не совпадают, в Консоли администрирования возникает ошибка. Несовпадение сертификатов может произойти, например, при замене сертификата Сервера администрирования (см. раздел "О сертификате Сервера администрирования" см. стр. [75](#)). В этом случае необходимо повторно создать узел Сервер администрирования в консоли.

► Чтобы повторно создать узел Сервера администрирования:

1. Закройте окно Консоли администрирования Kaspersky Security Center.
2. Удалите файл Kaspersky Security Center 15.1 из папки %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.
3. Запустить Консоль администрирования Kaspersky Security Center.
Отобразится предложение подключиться к Серверу администрирования и принять его существующий сертификат.
4. Выполните одно из следующих действий:
 - Примите существующий сертификат, нажав на кнопку **Да**.
 - Чтобы указать ваш сертификат, нажмите на кнопку **Нет** и перейдите к файлу сертификата, используемого для аутентификации Сервера администрирования.

Проблема с сертификатом решена. Вы можете использовать Консоль администрирования для подключения к Серверу администрирования.

Просмотр и изменение параметров Сервера администрирования

Вы можете настраивать параметры Сервера администрирования в окне свойств Сервера администрирования.

► Чтобы открыть окно *Свойства: Сервер администрирования*,

в контекстном меню узла Сервера администрирования в дереве консоли выберите пункт **Свойства**.

В этом разделе

Настройка общих параметров Сервера администрирования	716
Параметры интерфейса Консоли администрирования	716
Обработка и хранение событий на Сервере администрирования	717
Просмотр журнала подключений к Серверу администрирования	717
Контроль возникновения вирусных эпидемий	718
Ограничение трафика.....	719
Настройка параметров Веб-сервера.....	720
Работа с внутренними пользователями	720

Настройка общих параметров Сервера администрирования

Вы можете настраивать общие параметры Сервера администрирования в разделах **Общие**, **Параметры подключения к Серверу администрирования**, **Хранилище событий** и **Безопасность** окна свойств Сервера администрирования.

Раздел **Безопасность** не отображается в окне свойств Сервера администрирования, если его отображение выключено в интерфейсе Консоли администрирования.

► *Чтобы включить отображение раздела **Безопасность** в Консоли администрирования:*

1. В дереве консоли выберите требуемый Сервер администрирования.
2. В меню **Вид** главного окна приложения выберите пункт **Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса** установите флажок **Отображать разделы с параметрами безопасности** и нажмите на кнопку **ОК**.
4. В окне с сообщением приложения нажмите на кнопку **ОК**.

Раздел **Безопасность** отобразится в окне свойств Сервера администрирования.

Параметры интерфейса Консоли администрирования

Вы можете настроить параметры интерфейса Консоли администрирования для отображения или скрытия элементов управления пользовательского интерфейса, связанных со следующими функциями:

- Системное администрирование.
- Шифрование и защита данных.
- Параметры контроля рабочего места.
- Управление мобильными устройствами.
- Подчиненные Серверы администрирования.
- Разделы с параметрами безопасности.

► Чтобы настроить параметры интерфейса Консоли администрирования:

1. В дереве консоли выберите требуемый Сервер администрирования.
2. В меню **Вид** главного окна приложения выберите пункт **Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса** установите флажок рядом с функциональностью, которая должна отображаться, и нажмите на кнопку **ОК**.
4. В окне с сообщением приложения нажмите на кнопку **ОК**.

Выбранная функциональность отображается в интерфейсе Консоли администрирования.

Обработка и хранение событий на Сервере администрирования

Информация о событиях в работе приложения и управляемых устройств сохраняется в базе данных Сервера администрирования. Каждое событие относится к определенному типу и уровню важности (*Критическое событие*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*). В зависимости от условий, при которых произошло событие, приложение может присваивать событиям одного типа разные уровни важности.

Вы можете просматривать типы и уровни важности событий в разделе **Настройка событий** окна свойств Сервера администрирования. В разделе **Настройка событий** вы также можете настроить параметры обработки каждого события Сервером администрирования:

- регистрацию событий на Сервере администрирования и в журналах событий операционной системы на устройстве и на Сервере администрирования;
- способ уведомления администратора о событиях (например, SMS, сообщение электронной почты).

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

Можно изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи. Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

Просмотр журнала подключений к Серверу администрирования

Можно сохранить в файл журнала историю подключений и попыток подключения к Серверу администрирования в процессе его работы. Информация в файле позволит отследить не только

подключения внутри инфраструктуры сети, но и попытки несанкционированного доступа к Серверу администрирования.

► *Чтобы настроить регистрацию событий подключения к Серверу администрирования:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить регистрацию событий подключения.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств в разделе **Параметры подключения к Серверу администрирования** выберите вложенный раздел **Порты подключения**.
4. Включите параметр **Записывать события соединения с Сервером администрирования в журнал**.
5. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл %ProgramData%\KasperskyLab\adminikit\logs\sc.syslog.

Контроль возникновения вирусных эпидемий

Kaspersky Security Center позволяет вам своевременно реагировать на возникновение угроз вирусных эпидемий. Оценка угрозы вирусной эпидемии производится путем контроля вирусной активности на устройствах.

Вы можете настраивать правила оценки угрозы вирусной эпидемии и действия в случае ее возникновения в разделе **Вирусная атака** окна свойств Сервера администрирования.

Порядок оповещения о событии *Вирусная атака* можно задать в разделе **Настройка событий** окна свойств Сервера администрирования (см. раздел "Обработка и хранение событий на Сервере администрирования" на стр. [717](#)), в окне свойств события *Вирусная атака*.

Событие *Вирусная атака* формируется при возникновении событий *Обнаружен вредоносный объект* в работе приложений безопасности. Поэтому для распознавания вирусной эпидемии информацию о событиях *Обнаружен вредоносный объект* требуется сохранять на Сервере администрирования.

Параметры сохранения информации о событии *Обнаружен вредоносный объект* задаются в политиках приложений безопасности.

При подсчете событий *Обнаружен вредоносный объект* учитывается только информация с устройств главного Сервера администрирования. Информация с подчиненных Серверов администрирования не учитывается. Для каждого подчиненного Сервера параметры события *Вирусная атака* требуется настраивать индивидуально.

См. также:

Сценарий: мониторинг и отчеты [593](#)

Ограничение трафика

Для снижения трафика в сети предусмотрена возможность ограничения скорости передачи данных на Сервер администрирования с отдельных IP-диапазонов и IP-интервалов.

Вы можете создавать и настраивать правила ограничения трафика в разделе **Трафик** окна свойств Сервера администрирования.

► *Чтобы создать правила ограничения трафика:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования, для которого нужно создать правила ограничения трафика.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Трафик**.
4. Нажмите на кнопку **Добавить**.
5. В разделе **Новое правило** укажите следующие параметры:

В блоке **Интервал IP-адресов, для которых нужно ограничивать трафик** можно выбрать способ задания подсети или диапазона, для которого ограничивается скорость передачи, и указать значения параметров для выбранного способа. Выберите один из следующих способов:

- **Задать интервал адресом и маской подсети**

Трафик ограничивается по параметрам подсети. Укажите в полях ввода адрес подсети и маску подсети для определения интервала, в пределах которого будет ограничен трафик.

Нажмите на кнопку **Обзор**, чтобы добавить подсеть из глобального списка подсетей (см. раздел "Просмотр и изменение свойств подсети в глобальном списке подсетей" на стр. [967](#)).

- **Задать интервал начальным и конечным IP-адресом**

Трафик ограничивается по интервалу IP-адресов. Укажите интервал IP-адресов в полях ввода **Начальный IP-адрес** и **Конечный IP-адрес**.

Этот вариант выбран по умолчанию.

В блоке **Ограничение трафика** можно настроить следующие параметры ограничения скорости передачи данных:

- **Период**

Временной интервал, во время которого будет действовать ограничение трафика. Границы временного интервала можно указать в полях ввода.

- **Ограничение (КБ/сек)**

Предельное значение суммарной скорости передачи входящих и исходящих данных Сервера администрирования. Ограничение действует только в течение временного интервала, заданного в поле **Период**.

- **Ограничивать трафик на оставшееся время (КБ/сек)**

Трафик ограничивается не только в течение интервала, указанного в поле **Период**, но и в остальное время.

По умолчанию флажок снят. Значение поля может не совпадать со значением поля **Ограничение (КБ/сек)**.

В первую очередь правила ограничения трафика влияют на передачу файлов. Эти правила не применяются к трафику, который возникает при синхронизации между Сервером администрирования и Агентом администрирования, или между главным Сервером администрирования и подчиненным Сервером администрирования.

Настройка параметров Веб-сервера

Веб-сервер используется для публикации автономных инсталляционных пакетов, iOS MDM-профилей, а также файлов из папки общего доступа.

Вы можете настроить параметры подключения Веб-сервера к Серверу администрирования и задать сертификат Веб-сервера в разделе **Веб-сервер** окна свойств Сервера администрирования.

Работа с внутренними пользователями

Учетные записи *внутренних пользователей* используются для работы с виртуальными Серверами администрирования. В приложении Kaspersky Security Center внутренние пользователи обладают правами реальных пользователей.

Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Вы можете настраивать параметры учетных записей внутренних пользователей в папке **Учетные записи пользователей** дерева консоли (см. раздел "Работа с учетными записями пользователей" на стр. [803](#)).

Перенос данных мобильных устройств между серверами

Резервное копирование и восстановление параметров Сервера администрирования

Для резервного копирования параметров Сервера администрирования и используемой им базы данных предусмотрены задача резервного копирования и утилита klbackup. Резервная копия включает в себя все основные параметры и объекты Сервера администрирования: сертификаты Сервера администрирования, мастер-ключи шифрования дисков управляемых устройств, ключи для лицензий, структуру групп администрирования со всем содержимым, задачи, политики и так далее. Имея резервную копию, можно восстановить работу Сервера администрирования в кратчайшие сроки – от десятков минут до двух часов.

В случае отсутствия резервной копии сбой может привести к безвозвратной потере сертификатов и всех параметров Сервера администрирования. Это повлечет необходимость заново настраивать Kaspersky Security Center, а также заново выполнять первоначальное развертывание Агента администрирования в сети организации. Кроме того, будут потеряны и мастер-ключи шифрования дисков управляемых устройств, что создаст риск безвозвратной потери зашифрованных данных на устройствах с Kaspersky Endpoint Security. Поэтому не следует отказываться от регулярного создания резервных копий Сервера администрирования с помощью штатной задачи резервного копирования.

Мастер первоначальной настройки приложения создает задачу резервного копирования параметров Сервера администрирования с ежедневным запуском в четыре часа ночи. Резервные копии по умолчанию сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskySC.

Если в качестве СУБД используется экземпляр Microsoft SQL Server, установленный на другом устройстве, следует изменить задачу резервного копирования: указать в качестве папки для хранения сделанных резервных копий UNC-путь, доступный на запись как службе Сервера администрирования, так и службе SQL Server. Это требование является следствием особенности резервного копирования в СУБД Microsoft SQL Server.

Если в качестве СУБД используется локальный экземпляр Microsoft SQL Server, также рекомендуется сохранять резервные копии на отдельном носителе, чтобы обезопасить их от повреждения одновременно с Сервером администрирования.

Поскольку резервная копия содержит важные данные, в задаче резервного копирования и в утилите klbackup предусмотрена защита резервных копий паролем. По умолчанию задача резервного копирования создается с пустым паролем. Следует обязательно задать пароль в свойствах задачи резервного копирования. Несоблюдение этого требования приведет к тому, что ключи сертификатов Сервера администрирования, ключи для лицензий и мастер-ключи шифрования дисков управляемых устройств окажутся незашифрованными.

Помимо регулярного резервного копирования, следует также создавать резервную копию перед всеми значимыми изменениями, в том числе перед обновлением Сервера администрирования до новой версии и перед установкой патчей Сервера администрирования.

Если вы используете Microsoft SQL Server в качестве СУБД, вы можете минимизировать размер резервных копий. Для этого установите флажок **Сжимать резервные копии (Compress backup)** в параметрах SQL Server.

Восстановление из резервной копии выполняется с помощью утилиты klbackup на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой).

Инсталляция Сервера администрирования, на которую выполняется восстановление, должна использовать СУБД того же типа (например, тот же SQL Server или MariaDB) той же самой или более новой версии. Версия Сервера администрирования может быть той же самой (с аналогичным или более новым патчем) или более новой.

В этом разделе описаны типовые сценарии восстановления параметров и объектов Сервера администрирования.

В этом разделе

Использование снимка файловой системы для уменьшения времени резервного копирования	722
Вышло из строя устройство с Сервером администрирования	723
Повреждены параметры Сервера администрирования или база данных	723

Использование снимка файловой системы для уменьшения времени резервного копирования

В Kaspersky Security Center уменьшено по сравнению с более ранними версиями время простоя Сервера администрирования во время резервного копирования данных. Кроме того, в параметры задачи добавлена функция **Использовать моментальный снимок файловой системы для резервного копирования данных**. Эта функция позволяет дополнительно уменьшить время простоя за счет того, что утилита kbackup создает при выполнении резервного копирования теневую копию диска (это занимает несколько секунд) и одновременно производит копирование базы данных (это занимает не более нескольких минут). Создав теневую копию диска и сделав копию базы данных, kbackup снова делает Сервер администрирования доступным для соединения.

Вы можете пользоваться функцией создания снимка файловой системы только при соблюдении двух условий:

- Папка общего доступа Сервера администрирования и папка %ALLUSERSPROFILE%\KasperskyLab находятся на одном логическом диске и локальны по отношению к Серверу администрирования.
- Внутри папки %ALLUSERSPROFILE%\KasperskyLab нет созданных вручную символических ссылок.

Не используйте функцию, если хотя бы одно из этих условий не выполняется. В ответ на попытку создать снимок файловой системы приложение выдаст сообщение об ошибке.

Для использования функции необходимо иметь учетную запись с правами на создание снимков логического диска, на котором расположена папка %ALLUSERSPROFILE%. Учетная запись службы сервера администрирования не имеет таких прав.

► Чтобы воспользоваться функцией создания снимка файловой системы для уменьшения времени резервного копирования:

1. В разделе **Задачи** выберите задачу резервного копирования.
2. В контекстном меню выберите пункт **Свойства**.
3. В отобразившемся окне свойств задачи выберите раздел **Параметры**.
4. Установите флажок **Использовать моментальный снимок файловой системы для резервного копирования данных**.
5. В полях **Имя пользователя** и **Пароль** введите имя и пароль от учетной записи, имеющей право на создание снимков логического диска, на котором расположена папка %ALLUSERSPROFILE%.

6. Нажмите на кнопку **Применить**.

При следующих запусках задачи резервного копирования утилита klbackup будет создавать снимки файловой системы, и время простоя Сервера администрирования во время выполнения задачи уменьшится.

Вышло из строя устройство с Сервером администрирования

Если в результате сбоя вышло из строя устройство с Сервером администрирования, рекомендуется выполнить следующие действия:

- Новому Серверу назначить тот же самый адрес: NetBIOS-имя, FQDN-имя, статический IP – в зависимости от того, что было задано при развертывании Агентов администрирования.
- Установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
- Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Повреждены параметры Сервера администрирования или база данных

Если Сервер администрирования стал неработоспособен в результате повреждения параметров или базы данных (например, из-за сбоя питания), рекомендуется использовать следующий сценарий восстановления:

1. Выполнить проверку файловой системы на пострадавшем устройстве.
2. Деинсталлировать неработоспособную версию Сервера администрирования.
3. Заново установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
4. Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Недопустимо восстанавливать Сервер администрирования любым другим способом, кроме штатной утилиты klbackup.

Во всех случаях восстановления Сервера с помощью стороннего программного обеспечения неизбежно произойдет рассинхронизация данных на узлах распределенного приложения Kaspersky Security Center и, как следствие, неправильная работа приложения.

Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование данных позволяет переносить Сервер администрирования с одного устройства на другое без потерь информации. С помощью резервного копирования вы можете восстанавливать данные при переносе информационной базы Сервера администрирования на другое устройство или при переходе на более позднюю версию Kaspersky Security Center.

Обратите внимание, что резервные копии установленных плагинов управления не сохраняются. После восстановления данных Сервера администрирования из резервной копии необходимо загрузить и переустановить плагины управляемых программ.

Прежде чем создавать резервную копию данных Сервера администрирования, проверьте, добавлен ли виртуальный Сервер администрирования в группу администрирования. Если виртуальный Сервер администрирования добавляется перед резервным копированием, убедитесь, что этому виртуальному Серверу назначен администратор. Вы не можете предоставить права администратора к виртуальному Серверу администрирования после резервного копирования. Обратите внимание, если учетные данные администратора утеряны, вы не сможете назначить нового администратора виртуальному Серверу администратора.

Вы можете создать резервную копию данных Сервера администрирования одним из следующих способов:

- Создать и запустить задачу резервного копирования данных (см. раздел "Создание задачи резервного копирования данных" на стр. [724](#)) через Консоль администрирования.
- Запустить утилиту klbackup (см. раздел "Утилита резервного копирования и восстановления данных (klbackup)" на стр. [725](#)) на устройстве, где установлен Сервер администрирования. Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке приложения.

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- база данных Сервера администрирования (политики, задачи, параметры приложений, сохраненные на Сервере администрирования события);
- конфигурационная информация о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки;
- сертификат Сервера администрирования.

Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup.

В этом разделе

Создание задачи резервного копирования данных.....	724
Утилита резервного копирования и восстановления данных (klbackup)	725
Резервное копирование и восстановление данных в интерактивном режиме	725
Резервное копирование и восстановление данных в тихом режиме	728

Создание задачи резервного копирования данных

Задача резервного копирования является задачей Сервера администрирования и создается мастером первоначальной настройки. Если задача резервного копирования, созданная мастером первоначальной настройки, была удалена, вы можете создать ее вручную.

► Чтобы создать задачу резервного копирования данных Сервера администрирования:

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:
 - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать** → **Задачу**.
 - Нажмите на кнопку **Создать задачу**, расположенную в рабочей области.

Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне мастера **Выбор типа задачи** выберите тип задачи **Резервное копирование данных Сервера администрирования**.

Задачу **Резервное копирование данных Сервера администрирования** можно создать только в одном экземпляре. Если задача резервного копирования данных Сервера администрирования уже создана для Сервера администрирования, то она не отображается в окне выбора типа задачи мастера создания задачи резервного копирования.

Утилита резервного копирования и восстановления данных (klbackup)

Вы можете выполнять копирование данных Сервера администрирования для резервного хранения и последующего восстановления с помощью утилиты klbackup, входящей в состав дистрибутива Kaspersky Security Center.

Утилита klbackup может работать в двух режимах:

- интерактивный (см. раздел "Резервное копирование и восстановление данных в интерактивном режиме" на стр. [725](#));
- тихий (см. раздел "Резервное копирование и восстановление данных в тихом режиме" на стр. [728](#)).

Резервное копирование и восстановление данных в интерактивном режиме

► Чтобы создать резервную копию данных Сервера администрирования в интерактивном режиме:

1. Запустите утилиту klbackup, расположенную в папке установки Kaspersky Security Center.
В результате запустится мастер выполнения резервного копирования и восстановления данных.
2. В первом окне мастера выберите **Выполнить резервное копирование данных Сервера администрирования**.
При выборе параметра **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования** будет сохранена только резервная копия сертификата Сервера администрирования.
Нажмите **Далее**.
3. В следующем окне мастера укажите параметры:
 - **Целевая папка для резервной копии данных**
 - **Перенос данных в формате MySQL/MariaDB**

- **Перенести в формат Azure**
 - **Включать текущую дату и время в имя папки назначения для резервных копий**
 - **Пароль для резервной копии данных**
4. Нажмите на кнопку **Далее** для выполнения резервного копирования.
5. Если вы работаете с базой данных в облачном окружении, таком как Amazon Web Services (AWS) или Microsoft Azure, заполните следующие поля в окне **Войти в онлайн-хранилище**:
- **Для AWS:**
 - **Имя корзины S3**

Имя корзины S3, которое вы создали для резервной копии данных.
 - **ID ключа доступа**

Вы получили ID ключа (последовательность из букв и цифр), когда создали учетную запись IAM-пользователя для работы с корзиной S3 в хранилище инстансов.

Поле доступно, если вы выбрали базу RDS для контейнера S3.
 - **Секретный ключ**

Введите секретный ключ. Вы получили секретный ключ при создании учетной записи IAM-пользователя вместе с ID ключа.

Символы секретного ключа отображаются в виде звездочек. После того, как вы начали вводить секретный ключ, отображается кнопка **Показать секретный ключ**. Нажмите на эту кнопку и удерживайте ее необходимое вам время, чтобы посмотреть введенные символы.

Поле доступно, если вы выбрали для авторизации ключ доступа IAM AWS, а не IAM-роль.
 - **Для Microsoft Azure:**
 - **Имя учетной записи хранения Azure**

Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center.
 - **Идентификатор подписки Azure**

Вы создали подписку на портале Azure.
 - **Пароль Azure**

Вы получили пароль к идентификатору приложения при создании ID приложения в Azure.

Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.
 - **Идентификатор приложения в Azure.**

Вы создали этот идентификатор приложения на портале Azure.

Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вам нужно сначала удалить первый сегмент в существующем соединении Azure.
 - **Имя SQL-сервера Azure**

Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Группа источника SQL-сервера Azure**

Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Ключ доступа хранилища Azure**

Доступен в свойствах учетной записи хранения в разделе "Access Keys". Вы можете использовать любой ключ (key1 или key2).

► *Чтобы восстановить данные Сервера администрирования в интерактивном режиме:*

1. Запустите утилиту klbackup, расположенную в папке установки Kaspersky Security Center. Запустите утилиту под той же учетной записью, под которой был установлен Сервер администрирования. Рекомендуется запускать утилиту на только что установленном Сервере администрирования.

В результате запустится мастер выполнения резервного копирования и восстановления данных.

2. В первом окне мастера выберите **Выполнить восстановление данных Сервера администрирования** и нажмите на кнопку **Далее**.

Если вы выбрали параметр **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования** будет выполнено только восстановление сертификата Сервера администрирования.

При запуске утилиты klbackup на неактивном узле отказоустойчивого кластера вам будет предложено выбрать один из вариантов: указать сертификат Сервера администрирования или автоматически получать данные с Сервера администрирования.

3. В окне мастера **Параметры восстановления**:

- Укажите папку, содержащую резервную копию данных Сервера администрирования.

Если вы работаете в облачном окружении, таком как AWS или Azure, укажите адрес хранилища. Также убедитесь, что файл называется backup.zip.

- Укажите пароль, введенный при резервном копировании данных.

При восстановлении данных необходимо указать тот же пароль, который был введен во время резервного копирования. Если после резервного копирования путь к общей папке изменился, проверьте работу задач, использующих восстановленные данные (задачи восстановления и задачи удаленной установки). При необходимости отредактируйте параметры этих задач. Пока данные восстанавливаются из файла резервной копии, никто не должен иметь доступ к общей папке Сервера администрирования. Учетная запись, под которой запускается утилита klbackup, должна иметь полный доступ к общей папке.

4. Нажмите на кнопку **Далее** для восстановления данных.

См. также:

Резервное копирование и восстановление данных в тихом режиме[728](#)

Резервное копирование и восстановление данных в тихом режиме

- Чтобы создать резервную копию данных или восстановить данные Сервера администрирования в тихом режиме,

в командной строке устройства, на котором установлен Сервер администрирования, запустите утилиту `klbackup` с необходимым набором ключей.

Синтаксис командной строки утилиты:

```
klbackup -path BACKUP_PATH [-linux_path LINUX_PATH] [-node_cert CERT_PATH] [-logfile LOGFILE] [-use_ts][[-restore] [-password PASSWORD] [-cert_only] [-online]
```

Если не задать пароль в командной строке утилиты `klbackup`, утилита запросит его ввод интерактивно.

Описания ключей:

- `-path BACKUP_PATH` – сохранить информацию в папке `BACKUP_PATH` / использовать для восстановления данные из папки `BACKUP_PATH` (обязательный параметр).
Учетная запись сервера базы данных и утилита `klbackup` должны обладать правами на изменение данных в папке `BACKUP_PATH`.
- `-linux_path LINUX_PATH` – локальный путь к папке с резервной копией данных для SQL Server для Linux.
Учетная запись сервера базы данных и утилита `klbackup` должны обладать правами на изменение данных в папке `LINUX_PATH`.
- `-node_cert CERT_PATH` – файл сертификата Сервера для настройки неактивного узла отказоустойчивого кластера после восстановления. Если параметр не указан, он будет автоматически получен с Сервера.
При запуске утилиты `klbackup` на неактивном узле отказоустойчивого кластера используйте этот ключ, чтобы указать путь к сертификату Сервера администрирования.
- `-logfile LOGFILE` – сохранить отчет о копировании или восстановлении данных Сервера администрирования.
- `-use_ts` – при сохранении данных копировать информацию в папку `BACKUP_PATH`, во вложенную папку с именем, отображающим текущую системную дату и время операции в формате `klbackupГГГГ-ММ-ДД # ЧЧ-ММ-СС`. Если ключ не задан, информация сохраняется в корне папки `BACKUP_PATH`.
При попытке сохранить информацию в папку, в которой уже есть резервная копия, появится сообщение об ошибке. Обновление информации не произойдет.
Наличие ключа `-use_ts` позволяет вести архив данных Сервера администрирования. Например, если ключом `-path` была задана папка `C:\KLBBackups`, то в папке `klbackup2022-06-19 # 11-30-18`, сохранится информация о состоянии Сервера администрирования на дату 19 июня 2022 года, 11 часов 30 минут 18 секунд.
- `-restore` – выполнить восстановление данных Сервера администрирования. Восстановление данных осуществляется на основании информации, представленной в папке `BACKUP_PATH`. Если ключ отсутствует, производится резервное копирование данных в папку `BACKUP_PATH`.

- `-password PASSWORD` – пароль для защиты конфиденциальных данных.

Забытый пароль не может быть восстановлен. Требования к паролю отсутствуют. Длина пароля не ограничена, также возможна нулевая длина пароля (то есть без пароля).

При восстановлении данных необходимо указать тот же пароль, который был введен во время резервного копирования. Если после резервного копирования путь к общей папке изменился, проверьте работу задач, использующих восстановленные данные (задачи восстановления и задачи удаленной установки). При необходимости отредактируйте параметры этих задач. Пока данные восстанавливаются из файла резервной копии, никто не должен иметь доступ к общей папке Сервера администрирования. Учетная запись, под которой запускается утилита `klbackup`, должна иметь полный доступ к общей папке. Рекомендуется запускать утилиту на только что установленном Сервере администрирования.

- `-cert_only` – сохранить или восстановить только сертификат и закрытый ключ Сервера администрирования.
- `-online` – создать резервную копию данных Сервера администрирования, создав моментальный снимок, чтобы минимизировать время автономного состояния Сервера администрирования. Если вы используете утилиту резервного копирования и восстановления данных, этот параметр игнорируется.

Перенос Сервера администрирования на другое устройство

Если вам нужно использовать Сервер администрирования на новом устройстве, вы можете перенести его одним из следующих способов:

- Переместить Сервер администрирования и сервер баз данных на новое устройство.
- Оставить сервер баз данных на старом устройстве и перенести на новое устройство только Сервер администрирования.

Чтобы перенести Сервер администрирования на новое устройство:

1. На предыдущем устройстве создайте резервную копию данных Сервера администрирования.

Для этого запустите задачу резервного копирования данных (см. раздел "Создание задачи резервного копирования данных" на стр. [724](#)) с помощью Консоли администрирования или запустите утилиту `klbackup` (см. раздел "Утилита резервного копирования и восстановления данных (`klbackup`)" на стр. [725](#)).

Если вы используете SQL Server в качестве СУБД для Сервера администрирования, можно перенести данные с SQL Server на СУБД MySQL или MariaDB. Для создания резервной копии данных запустите утилиту `klbackup` в интерактивном режиме (см. раздел "Резервное копирование и восстановление данных в интерактивном режиме" на стр. [725](#)). Включите параметр **Перенос данных в формате MySQL/MariaDB** в окне **Параметры резервного копирования** мастера резервного копирования и восстановления данных. Kaspersky Security Center создаст резервную копию данных, совместимую с MySQL и MariaDB. После этого вы можете восстановить данные из резервной копии в MySQL или MariaDB. Также можно включить параметр **Перенести в формат Azure**, если вы хотите перенести данные из SQL Server в СУБД Azure SQL.

2. Выберите новое устройство, на которое будет установлен Сервер администрирования. Убедитесь, что аппаратное и программное обеспечение на выбранном устройстве соответствует требованиям

(см. раздел "Аппаратные и программные требования" на стр. [29](#)) для Сервера администрирования, Консоли администрирования и Агента администрирования. Проверьте, что порты, используемые на Сервере администрирования (см. раздел "Порты, используемые Kaspersky Security Center" на стр. [63](#)) доступны.

3. На новом устройстве установите систему управления базами данных (СУБД), которую будет использовать Сервер администрирования.

При выборе СУБД учитывайте количество устройств (см. раздел "Выбор СУБД для Сервера администрирования" на стр. [139](#)), которые обслуживает Сервер администрирования.

4. Запустите выборочную установку Сервера администрирования (см. раздел "Выборочная установка" на стр. [234](#)) на новом устройстве.
5. Установите компоненты Сервера администрирования в ту же папку (см. раздел "Шаг 3. Выбор компонентов для установки" на стр. [235](#)), где Сервер администрирования установлен на предыдущем устройстве. Нажмите на кнопку **Обзор**, чтобы указать путь к файлу.

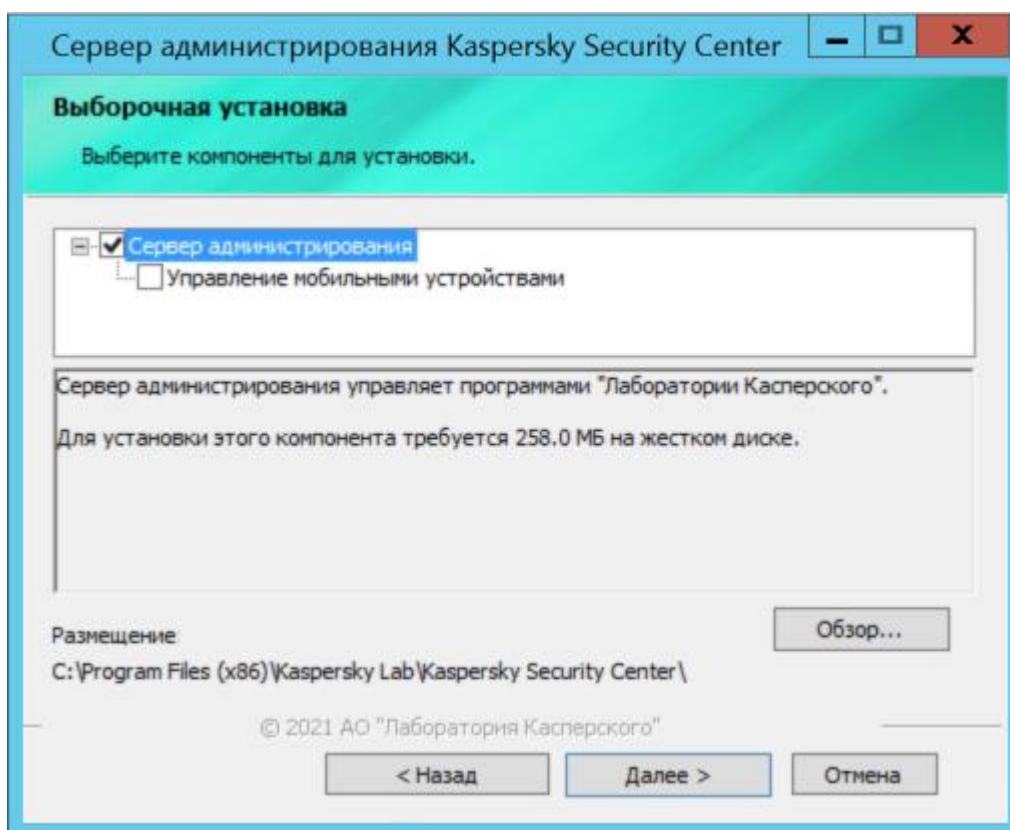


Рисунок 3. Окно выборочной установки

6. Настройте параметры подключения к серверу базы данных (см. раздел "Шаг 7. Настройка параметров SQL-сервера" на стр. [238](#)).

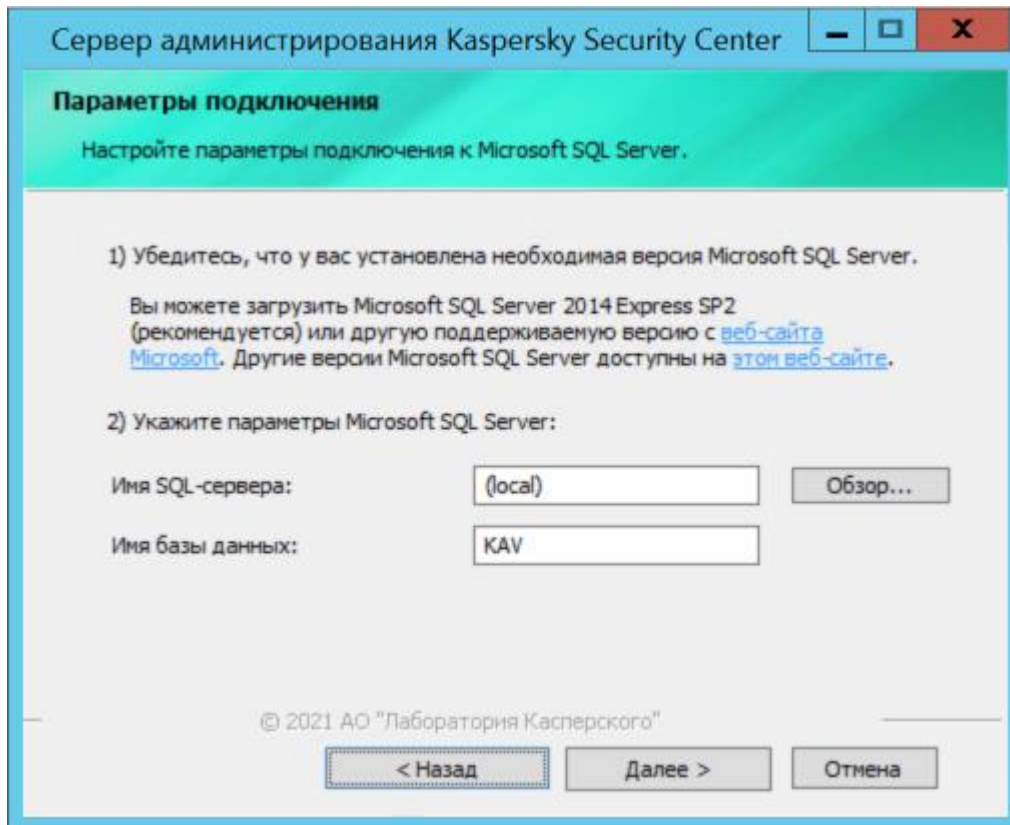


Рисунок 4. Окно параметров подключения

В зависимости от того, где вам нужно разместить сервер базы данных, выполните одно из следующих действий:

- Переместите сервер базы данных на новое устройство.
 - Оставьте сервер базы данных на предыдущем устройстве.
7. После завершения установки восстановите данные Сервера администрирования на новом устройстве с помощью утилиты klbackup (см. раздел "Утилита резервного копирования и восстановления данных (klbackup)" на стр. [725](#)).

Если вы используете SQL Server в качестве СУБД на предыдущем и новом устройствах, обратите внимание, что версия SQL Server, установленная на новом устройстве, должна быть такой же или выше, чем версия SQL Server, установленная на предыдущем устройстве. Иначе вы не сможете восстановить данные Сервера администрирования на новом устройстве.

8. Откройте Консоль администрирования и подключитесь к Серверу администрирования (см. раздел "Подключение к Серверу администрирования и переключение между Серверами администрирования" на стр. [703](#)).
9. Убедитесь, что все клиентские устройства подключены к Серверу администрирования.
10. Удалите Сервер администрирования и сервер баз данных с предыдущего устройства.

Также можно использовать Kaspersky Security Center Web Console, чтобы перенести Сервер администрирования и сервер баз данных на другое устройство.

См. также:

Смена Сервера администрирования для клиентских устройств.....	762
Параметры политики Агента администрирования.....	789
Установка Kaspersky Security Center.....	206
Резервное копирование и восстановление данных Сервера администрирования.....	723

Избегание конфликтов между Серверами администрирования

Если в сети имеется несколько Серверов администрирования, они могут видеть одни и те же клиентские устройства. Это может привести к тому, что, например, несколько Серверов администрирования будут выполнять удаленную установку одного и того же приложения на одно устройство, а также к другим конфликтам. Чтобы избежать такой ситуации, в Kaspersky Security Center можно запретить установку приложения на устройство, управляемое другим Сервером администрирования (см. раздел "Установка приложений с помощью мастера удаленной установки" на стр. [363](#)).

Свойство **Под управлением другого Сервера администрирования** можно также использовать как критерий для следующих операций:

- Поиск устройств (на стр. [938](#))
- Выборки устройств (на стр. [622](#))
- Правила перемещения устройств
- Правила автоматического назначения тегов (см. раздел "Автоматическое назначение тегов устройствам" на стр. [771](#))

В Kaspersky Security Center используется эвристический подход для определения, какой Сервер администрирования управляет клиентским устройством: тот, на котором вы работаете, или другой.

Двухэтапная проверка

В этом разделе описывается использование двухэтапной проверки для снижения риска несанкционированного доступа к Консоли администрирования или Kaspersky Security Center Web Console.

В этом разделе

Сценарий: настройка двухэтапной проверки для всех пользователей	733
О двухэтапной проверке	735
Включение двухэтапной проверки для вашей учетной записи	737
Включение двухэтапной проверки для всех пользователей	738
Выключение двухэтапной проверки для учетной записи пользователя	739
Выключение обязательной двухэтапной проверки для всех пользователей	740
Исключение учетных записей из двухэтапной проверки.	741
Изменение имени издателя кода безопасности	741
Настройка двухэтапной проверки для вашей учетной записи	742

Сценарий: настройка двухэтапной проверки для всех пользователей

В этом сценарии описывается, как включить двухэтапную проверку для всех пользователей и как исключить учетные записи пользователей из двухэтапной проверки. Если вы не включили двухэтапную проверку для своей учетной записи, прежде чем включить ее для других пользователей, приложение сначала откроет окно включения двухэтапной проверки для вашей учетной записи. В этом сценарии также описано, как включить двухэтапную проверку для вашей учетной записи.

Если вы включили двухэтапную проверку для своей учетной записи, вы можете перейти к включению двухэтапной проверки для всех пользователей.

Предварительные требования

Прежде чем начать:

- Убедитесь, что ваша учетная запись имеет право Изменение списков управления доступом объектов (см. раздел "Права доступа к функциям приложения" на стр. [810](#)) в функциональной области **Общий функционал: Права пользователей** для изменения параметров безопасности учетных записей других пользователей.
- Убедитесь, что другие пользователи Сервера администрирования установили на свои устройства приложение для аутентификации.

Этапы

Включение двухэтапной проверки для всех пользователей состоит из следующих этапов:

а. Установка приложения для аутентификации на устройство

Вы можете установить любое приложение проверки подлинности, которое поддерживает алгоритм формирования одноразового пароля на основе времени (TOTP), такие как:

- Google Authenticator.
- Microsoft Authenticator.
- Bitrix24 OTP.

- Яндекс ключ.
- Avanpost Authenticator.
- Aladdin 2FA.

Чтобы проверить, поддерживает ли Kaspersky Security Center приложение для аутентификации, которое вы хотите использовать, включите двухфакторную проверку для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением для аутентификации. В случае успеха Kaspersky Security Center поддерживает выбранное приложение проверки подлинности.

Категорически не рекомендуется устанавливать приложение для аутентификации на том же устройстве, с которого выполняется подключение к Серверу администрирования.

b. Синхронизация времени приложения для аутентификации и время устройства, на котором установлен Сервер администрирования

Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени. Иначе возможны сбои при аутентификации и активации двухэтапной проверки.

c. Включение двухэтапной проверки и получение секретного ключа для своей учетной записи

Инструкции:

- Для Консоли администрирования на основе MMC: Включение двухэтапной проверки для вашей учетной записи (на стр. [737](#)).
- Для Kaspersky Security Center Web Console: Включение двухэтапной проверки для вашей учетной записи.

После включения двухэтапной проверки для своей учетной записи вы можете включить двухэтапную проверку для всех пользователей.

d. Включение двухэтапной проверки для всех пользователей

Пользователи с включенной двухэтапной проверкой должны использовать ее для входа на Сервер администрирования.

Инструкции:

- Для Консоли администрирования на основе MMC: Включение двухэтапной проверки для всех пользователей (на стр. [738](#)).
- Для Kaspersky Security Center Web Console: Включение двухэтапной проверки для всех пользователей.

e. Изменение имени издателя кода безопасности

Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности для лучшего распознавания разных Серверов администрирования.

Инструкции:

- Для Консоли администрирования на основе MMC: Изменение имени издателя кода безопасности (на стр. [741](#)).
- Для Kaspersky Security Center Web Console: Изменение имени издателя кода безопасности.

f. Исключение учетных записей пользователей, для которых не требуется включать двухэтапную проверку

При необходимости исключите учетные записи пользователей из двухэтапной проверки. Пользователям с исключенными учетными записями не нужно использовать двухэтапную проверку для входа на Сервер администрирования.

Инструкции:

- Для Консоли администрирования на основе MMC: Исключение учетных записей из двухэтапной проверки (см. раздел "Исключение учетных записей из двухэтапной проверки." на стр. [741](#)).
- Для Kaspersky Security Center Web Console: Исключение учетных записей из двухэтапной проверки.

g. Настройка двухэтапной проверки для вашей учетной записи

Если пользователи не исключены из двухэтапной проверки и двухэтапная проверка еще не настроена для их учетных записей, им необходимо настроить ее в окне, открываемом при входе в Kaspersky Security Center. Иначе они не смогут получить доступ к Серверу администрирования в соответствии со своими правами.

Инструкции:

- Для Консоли администрирования на основе MMC: Настройка двухэтапной проверки для вашей учетной записи (на стр. [742](#)).
- Для Kaspersky Security Center Web Console: Настройка двухэтапной проверки для вашей учетной записи.

Результаты

После выполнения этого сценария:

- Двухэтапная проверка для вашей учетной записи включена.
- Двухэтапная проверка включена для всех учетных записей пользователей Сервера администрирования, кроме исключенных учетных записей пользователей.

См. также:

О двухэтапной проверке	735
Включение двухэтапной проверки для вашей учетной записи	737
Включение двухэтапной проверки для всех пользователей	738
Исключение учетных записей из двухэтапной проверки.	741

О двухэтапной проверке

Если для учетной записи включена двухэтапная проверка, для входа в Консоль администрирования или Kaspersky Security Center Web Console, помимо имени пользователя и пароля, требуется одноразовый код безопасности. Если доменная аутентификация включена, пользователю достаточно ввести одноразовый код безопасности.

Чтобы использовать двухэтапную проверку, установите на мобильное устройство или компьютер приложение для аутентификации, которое генерирует одноразовые коды безопасности. Вы можете

использовать любое приложение проверки подлинности, которое поддерживает алгоритм формирования одноразового пароля на основе времени (TOTP), такие как:

- Google Authenticator.
- Microsoft Authenticator.
- Bitrix24 OTP.
- Яндекс ключ.
- Avanpost Authenticator.
- Aladdin 2FA.

Чтобы проверить, поддерживает ли Kaspersky Security Center приложение для аутентификации, которое вы хотите использовать, включите двухфакторную проверку для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением для аутентификации. В случае успеха Kaspersky Security Center поддерживает выбранное приложение проверки подлинности.

Настоятельно рекомендуется сохранить секретный ключ или QR-код и хранить его в надежном месте. Это поможет вам восстановить доступ к Kaspersky Security Center Web Console в случае потери доступа к мобильному устройству.

Чтобы обезопасить использование Kaspersky Security Center, вы можете включить двухэтапную проверку для своей учетной записи и включить двухэтапную проверку для всех пользователей.

Вы можете исключить учетные записи из двухэтапной проверки. Это может быть необходимо для служебных учетных записей, которые не могут получить защитный код для аутентификации.

Правила и ограничения

Чтобы иметь возможность активировать двухэтапную проверку для всех пользователей и деактивировать двухэтапную проверку для отдельных пользователей:

- Убедитесь, что вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общий функционал: Права пользователей**.
- Включите двухэтапную проверку для вашей учетной записи.

Чтобы выключить двухэтапную проверку для всех пользователей:

- Убедитесь, что вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общий функционал: Права пользователей**.
- Войдите в Kaspersky Security Center Web Console с помощью двухэтапной проверки.

Если для учетной записи на Сервере администрирования Kaspersky Security Center версии 13 или выше включена двухэтапная проверка, то пользователь не сможет войти в приложение Kaspersky Security Center Web Console версий 12, 12.1 или 12.2.

Перевыпуск секретного ключа

Любой пользователь может повторно выпустить секретный ключ, используемый для двухэтапной проверки. Когда пользователь входит на Сервер администрирования с перевыпущенным секретным ключом, новый секретный ключ сохраняется для учетной записи пользователя. Если пользователь неправильно вводит новый секретный ключ, новый секретный ключ не сохраняется, а текущий секретный ключ остается действительным.

Код безопасности имеет идентификатор, называемый также *имя издателя*. Имя издателя кода безопасности используется в качестве идентификатора Сервера администрирования в приложении для аутентификации. Имя издателя кода безопасности имеет значение по умолчанию, такое же, как имя Сервера администрирования. Вы можете изменить имя издателя кода безопасности. Если вы изменили имя издателя кода безопасности, необходимо выпустить новый секретный ключ и передать его приложению для аутентификации.

См. также:

Исключение учетных записей из двухэтапной проверки. [741](#)

Включение двухэтапной проверки для вашей учетной записи

Перед тем как включить двухэтапную проверку для своей учетной записи, убедитесь, что на мобильном устройстве установлено приложение для аутентификации. Убедитесь, что время, установленное в приложении для аутентификации, синхронизировано со временем Сервера администрирования.

► Чтобы включить двухэтапную проверку для учетной записи:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** перейдите в раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. В разделе **Двухэтапная проверка** нажмите на кнопку **Настроить**.

Если для вашей учетной записи уже включена двухэтапная проверка, при нажатии на кнопку **Настроить** сбрасывается секретный ключ, чтобы можно было перенастроить двухэтапную проверку.

В открывшемся окне свойств двухэтапной проверки отображается секретный ключ.

4. Введите секретный ключ в приложение для аутентификации, чтобы получить одноразовый код безопасности. Вы можете указать секретный ключ в приложении для аутентификации вручную или отсканировать QR-код с помощью приложения для аутентификации на мобильном устройстве.
5. Укажите код безопасности, сгенерированный приложением для аутентификации, а затем нажмите на кнопку **ОК**, чтобы закрыть окно свойств двухэтапной проверки.
6. Нажмите на кнопку **Применить**.
7. Нажмите на кнопку **ОК**.

Двухэтапная проверка для вашей учетной записи включена.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей[733](#)

Включение двухэтапной проверки для всех пользователей

Вы можете включить двухэтапную проверку для всех пользователей Сервера администрирования, если у вашей учетной записи есть право Изменение списков управления доступом объектов (см. раздел "Права доступа к функциям приложения" на стр. [810](#)) в функциональной области **Общий функционал: Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки.

► Чтобы включить двухэтапную проверку для всех пользователей:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. Нажмите на кнопку **Установить как обязательную**, чтобы включить двухэтапную проверку для всех пользователей.
4. Если вы не включили двухэтапную проверку для своей учетной записи (см. раздел "Включение двухэтапной проверки для вашей учетной записи" на стр. [737](#)), приложение откроет окно включения двухэтапной проверки для вашей учетной записи.
 - a. Введите секретный ключ в приложение для аутентификации, чтобы получить одноразовый код безопасности. Введите секретный ключ вручную в приложении для аутентификации или отсканируйте QR-код с помощью приложения для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.
 - b. Укажите код безопасности, сгенерированный приложением для аутентификации, а затем нажмите на кнопку **ОК**, чтобы закрыть окно свойств двухэтапной проверки.
5. В разделе **Двухэтапная проверка** нажмите на кнопку **Применить** и нажмите на кнопку **ОК**.

Двухэтапная проверка для всех пользователей включена. Пользователям Сервера администрирования, включая пользователей, которые были добавлены после включения этого параметра, необходимо настроить двухэтапную проверку для своих учетных записей, за исключением пользователей, учетные записи которых исключены (см. раздел "Исключение учетных записей из двухэтапной проверки." на стр. [741](#)) из двухэтапной проверки.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей[733](#)

Включение двухэтапной проверки для вашей учетной записи[737](#)

Исключение учетных записей из двухэтапной проверки.[741](#)

Выключение двухэтапной проверки для учетной записи пользователя

► Чтобы выключить двухэтапную проверку для вашей учетной записи:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. В разделе **Двухэтапная проверка** нажмите на кнопку **Выключить**.
4. Нажмите на кнопку **Применить**.
5. Нажмите на кнопку **ОК**.

Двухэтапная проверка для вашей учетной записи выключена.

Вы можете выключить двухэтапную проверку для других учетных записей пользователей. Эта защита используется, например, если пользователь потеряет или сломает мобильное устройство.

Вы можете выключить двухэтапную проверку для другой учетной записи пользователя, только если у вашей учетной записи есть право Изменение списков управления доступом объектов (см. раздел "Права доступа к функциям приложения" на стр. 810) в функциональной области **Общий функционал: Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки. Следуя приведенным ниже инструкциям, вы также можете выключить двухэтапную проверку для своей учетной записи.

► Чтобы выключить двухэтапную проверку для учетной записи любого пользователя:

1. В дереве консоли откройте папку **Учетные записи пользователей**.
Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В рабочей области папки нажмите на учетную запись пользователя, для которой вы хотите выключить двухэтапную проверку.
Для всех учетных записей пользователей, для которых включена двухэтапная проверка, в столбце **Требуется 2FA** установите значение **Да**.
3. В окне **Свойства: <Имя пользователя>** выберите раздел **Двухэтапная проверка**.
4. В разделе **Двухэтапная проверка** выберите следующие параметры:
 - Если вы хотите выключить двухэтапную проверку для всех пользователей, нажмите на кнопку **Выключить**.
 - Если вы хотите исключить эту учетную запись пользователя из двухэтапной проверки, выберите параметр **Пользователь может пройти аутентификацию, используя только имя пользователя и пароль**.
5. Нажмите на кнопку **Применить**.
6. Нажмите на кнопку **ОК**.

Двухэтапная проверка учетной записи пользователя выключена.

Если вы хотите восстановить доступ пользователя, который не может войти в Консоль администрирования с помощью двухэтапной проверки, выключите двухэтапную проверку для этой учетной записи пользователя и выберите параметр **Пользователь может пройти аутентификацию, используя только имя пользователя и пароль** в разделе **Двухэтапная проверка**, как описано выше. После этого войдите в Консоль администрирования под учетной записью пользователя, для которого вы выключили двухэтапную проверку, и снова включите проверку (см. раздел "Включение двухэтапной проверки для вашей учетной записи" на стр. [737](#)).

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей [733](#)

Выключение обязательной двухэтапной проверки для всех пользователей

Вы можете выключить обязательную двухэтапную проверку для всех пользователей Сервера администрирования, если у вас есть право Изменение списков управления доступом объектов (см. раздел "Права доступа к функциям приложения" на стр. [810](#)) в функциональной области **Общий функционал: Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки.

► Чтобы выключить двухэтапную проверку для всех пользователей:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. Нажмите на кнопку **Установить как необязательную**, чтобы выключить двухэтапную проверку для всех пользователей.
4. Нажмите на кнопку **Применить** в разделе **Двухэтапная проверка**.
5. Нажмите на кнопку **ОК** в разделе **Двухэтапная проверка**.

Двухэтапная проверка для всех пользователей выключена. Выключение двухэтапной проверки для всех пользователей не применяется к конкретным учетным записям, для которых двухэтапная проверка ранее была включена отдельно.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей [733](#)

Исключение учетных записей из двухэтапной проверки.

Вы можете исключить учетную запись из двухэтапной проверки, если у вашей учетной записи есть право Изменение списков управления доступом объектов (см. раздел "Права доступа к функциям приложения" на стр. [810](#)) в функциональной области **Общий функционал: Права пользователей**.

Если учетная запись пользователя исключена из двухэтапной проверки, этот пользователь может войти в Консоль администрирования или Kaspersky Security Center Web Console без использования двухэтапной проверки.

Исключение учетных записей из двухэтапной проверки может быть необходимо для служебных учетных записей, которые не могут передать код безопасности во время аутентификации.

► Чтобы исключить учетную запись пользователя из двухэтапной проверки:

1. Если вы хотите исключить учетную запись Active Directory, выполните опрос Active Directory (на стр. [328](#)), чтобы обновить список пользователей Сервера администрирования.
2. В дереве консоли откройте папку **Учетные записи пользователей**.
Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
3. В рабочей области папки нажмите на учетную запись пользователя, которую вы хотите исключить из двухэтапной проверки.
4. В окне **Свойства: <Имя пользователя>** выберите раздел **Двухэтапная проверка**.
5. В открывшемся разделе выберите параметр **Пользователь может пройти аутентификацию, используя только имя пользователя и пароль**.
6. В разделе **Двухэтапная проверка** нажмите на кнопку **Применить** и нажмите на кнопку **ОК**.

Эта учетная запись пользователя исключена из двухэтапной проверки. Вы можете проверить исключенные учетные записи в списке учетных записей пользователей (см. раздел "Работа с учетными записями пользователей" на стр. [803](#)).

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей[733](#)

Изменение имени издателя кода безопасности

У вас может быть несколько идентификаторов (также их называют издателями) для разных Серверов администрирования. Вы можете изменить имя издателя кода безопасности, например, Сервер администрирования уже использует аналогичное имя издателя кода безопасности для другого Сервера администрирования. По умолчанию имя издателя кода безопасности совпадает с именем Сервера администрирования.

После изменения имени издателя кода безопасности необходимо повторно выпустить новый секретный ключ и передать его приложению для аутентификации.

► *Чтобы указать новое имя издателя кода безопасности:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. Укажите новое имя издателя кода безопасности в поле **Кем выдан код безопасности**.
4. Нажмите на кнопку **Применить** в разделе **Двухэтапная проверка**.
5. Нажмите на кнопку **ОК** в разделе **Двухэтапная проверка**.

Для Сервера администрирования указано новое имя издателя кода безопасности.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей [733](#)

Настройка двухэтапной проверки для вашей учетной записи

При первом входе в Kaspersky Security Center после включения двухэтапной проверки открывается окно настройки двухэтапной проверки для вашей учетной записи.

Перед тем как настроить двухэтапную проверку для своей учетной записи, убедитесь, что на мобильном устройстве установлено приложение для аутентификации. Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени.

► *Чтобы настроить двухэтапную проверку для учетной записи:*

1. Сгенерируйте одноразовый код безопасности с помощью приложения для аутентификации на мобильном устройстве. Для этого выполните одно из следующих действий:
 - Введите секретный ключ в приложение для аутентификации вручную.
 - Отсканируйте QR-код с помощью приложения для аутентификации.
 Код безопасности отобразится на мобильном устройстве.
2. В окне **Установить двухэтапную проверку** укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **ОК**.

Двухэтапная проверка для вашей учетной записи настроена. У вас есть доступ к Серверу администрирования в соответствии со своими правами.

Управление группами администрирования

Этот раздел содержит информацию о работе с группами администрирования.

Вы можете выполнять с группами администрирования следующие действия:

- добавлять в состав группы администрирования произвольное количество вложенных групп любых уровней иерархии;
- добавлять в состав групп администрирования устройства;
- изменять иерархию групп администрирования путем перемещения отдельных устройств и целых групп в другие группы;
- удалять из состава групп администрирования вложенные группы и устройства;
- добавлять в состав групп администрирования подчиненные и виртуальные Серверы администрирования;
- переносить устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера;
- определять, какие приложения "Лаборатории Касперского" будут автоматически устанавливаться на устройства, включаемые в состав группы.

Эти действия можно выполнять, только если у вас есть права **Изменение** (см. раздел "**Назначение прав пользователям или группам пользователей**" на стр. [838](#)) в области **Управление группами администрирования**, для групп, которыми вы хотите управлять (или для Сервера администрирования, к которому относятся эти группы).

В этом разделе

Создание групп администрирования	743
Перемещение групп администрирования.....	745
Удаление групп администрирования	745
Автоматическое создание структуры групп администрирования.....	746
Автоматическая установка приложений на устройства группы администрирования	747

Создание групп администрирования

Иерархия групп администрирования формируется в главном окне приложения Kaspersky Security Center в папке **Управляемые устройства**. Группы администрирования отображаются в виде папок в дереве консоли (см. рис. ниже).

Сразу после установки Kaspersky Security Center папка **Управляемые устройства** содержит только пустую папку **Серверы администрирования**.

Наличие или отсутствие папки **Серверы администрирования** в дереве консоли определяется параметрами пользовательского интерфейса. Для включения отображения этой папки нужно перейти в меню **Вид → Настройка интерфейса** и в открывшемся окне **Настройка интерфейса** установить флажок **Отображать подчиненные Серверы администрирования**.

При создании иерархии групп администрирования в состав папки **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы. В папку **Серверы администрирования** можно добавлять подчиненные и виртуальные Серверы администрирования.

Каждая созданная группа, как и папка **Управляемые устройства**, сначала содержит только пустую папку **Серверы администрирования** для работы с подчиненными и виртуальными Серверами администрирования этой группы. Информация о политиках и задачах этой группы, а также информация об устройствах, входящих в эту группу, отображается на вкладках с соответствующими именами в рабочей области этой группы.

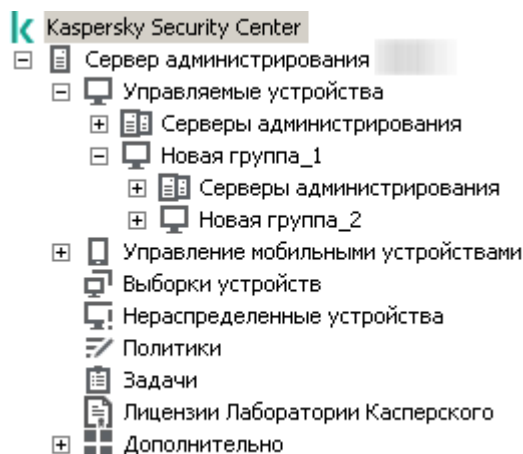


Рисунок 5. Просмотр иерархии групп администрирования

► Чтобы создать группу администрирования:

1. В дереве консоли откройте папку **Управляемые устройства**.
2. Если вы хотите создать подгруппу существующей группы администрирования, в папке **Управляемые устройства** выберите вложенную папку, соответствующую группе, в состав которой должна входить новая группа администрирования.

Если вы создаете новую группу администрирования верхнего уровня иерархии, этот шаг можно пропустить.

3. Запустите процесс создания группы администрирования одним из следующих способов:
 - с помощью команды контекстного меню **Создать** → **Группу**;
 - по кнопке **Новая группа**, расположенной в рабочей области главного окна приложения на вкладке **Устройства**.

4. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем.

Приложение позволяет создавать структуру групп администрирования на основе структуры Active Directory или структуры доменной сети. Также вы можете создавать структуру групп из текстового файла.

► Чтобы создать структуру групп администрирования:

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В контекстном меню папки **Управляемые устройства** выберите пункт **Все задачи** → **Новая структура групп**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Перемещение групп администрирования

Вы можете перемещать вложенные группы администрирования внутри иерархии групп.

Группа администрирования перемещается вместе со всеми вложенными группами, подчиненными Серверами администрирования, устройствами, групповыми политиками и задачами. К ней будут применены все параметры, соответствующие ее новому положению в иерархии групп администрирования.

Имя группы должно быть уникальным в пределах одного уровня иерархии. Если в папке, в которую вы перемещаете группу администрирования, уже существует группа с аналогичным названием, перед перемещением название группы следует изменить. Если вы предварительно не изменили название перемещаемой группы, к ее названию при перемещении автоматически добавляется окончание вида (<порядковый номер>), например: (1), (2).

Невозможно изменить название группы **Управляемые устройства**, поскольку она является встроенным элементом Консоли администрирования.

► Чтобы переместить группу в другую папку дерева консоли:

1. Выберите перемещаемую группу в дереве консоли.
2. Выполните одно из следующих действий:
 - Переместите группу с помощью контекстного меню:
 1. В контекстном меню группы выберите пункт **Вырезать**;
 2. В контекстном меню группы администрирования, в которую нужно переместить выбранную группу, выберите пункт **Вставить**.
 - Переместите группу с помощью главного меню приложения:
 - a. Выберите пункт главного меню **Действие** → **Вырезать**.
 - b. Выберите в дереве консоли группу администрирования, в которую нужно переместить выбранную группу.
 - c. Выберите пункт главного меню **Действие** → **Вставить**.
 - Переместите группу в другую группу в дереве консоли с помощью мыши.

Удаление групп администрирования

Вы можете удалить группу администрирования, если она не содержит подчиненных Серверов администрирования, вложенных групп и клиентских устройств и если для нее не сформированы задачи и политики.

Перед удалением группы администрирования требуется удалить из ее состава подчиненные Серверы администрирования, вложенные группы и клиентские устройства.

► Чтобы удалить группу:

1. В дереве консоли выберите группу администрирования.
2. Выполните одно из следующих действий:
 - в контекстном меню группы выберите пункт **Удалить**;

- в главном меню приложения выберите пункт **Действие** → **Удалить**;
- Нажмите на кнопку **DELETE**.

Автоматическое создание структуры групп администрирования

Kaspersky Security Center позволяет автоматически сформировать структуру групп администрирования с помощью мастера создания структуры групп.

Мастер создает структуру групп администрирования на основе следующих данных:

- структуры доменов и рабочих групп сети Windows;
- структуры групп Active Directory;
- содержимого текстового файла, созданного администратором вручную.

При формировании текстового файла требуется соблюдать следующие правила:

- Имя каждой новой группы должно начинаться с новой строки; разделитель должен начинаться с разрыва строки. Пустые строки игнорируются.

Пример:

Офис 1

Офис 2

Офис 3

В группе назначения будут созданы три группы первого уровня иерархии.

- Имя вложенной группы следует указывать через косую черту (/).

Пример:

Офис 1/Подразделение 1/Отдел 1/Группа 1

В группе назначения будут созданы четыре вложенные друг в друга подгруппы.

- Чтобы создать несколько вложенных групп одного уровня иерархии, следует указать "полный путь к группе".

Пример:

Офис 1/Подразделение 1/Отдел 1

Офис 1/Подразделение 2/Отдел 1

Офис 1/Подразделение 1/Отдел 1

Офис 1/Подразделение 1/Отдел 1

В группе назначения будет создана одна группа первого уровня иерархии "Офис 1", в состав которой будут входить четыре вложенные группы одного уровня иерархии: В состав каждой из этих групп будет входить группа "Отдел 1".

Создание структуры групп администрирования с помощью мастера не нарушает целостности сети: новые группы добавляются, а не замещают существующие. Клиентское устройство не может быть включено в

состав группы администрирования повторно, поскольку при перемещении устройства в группу администрирования оно удаляется из группы **Нераспределенные устройства**.

Если при создании структуры групп администрирования устройство по каким-либо причинам не было включено в состав группы **Нераспределенные устройства** (было выключено, отключено от сети), оно не будет автоматически перенесено в группу администрирования. Вы можете добавить устройства в группы администрирования вручную после завершения работы мастера.

► *Чтобы запустить автоматическое создание структуры групп администрирования:*

1. Выберите в дереве консоли папку **Управляемые устройства**.
2. В контекстном меню папки **Управляемые устройства** выберите пункт **Все задачи** → **Новая структура групп**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Автоматическая установка приложений на устройства группы администрирования

Вы можете указать, какие инсталляционные пакеты нужно использовать для автоматической удаленной установки приложений "Лаборатории Касперского" на вновь включенные в состав группы клиентские устройства.

► *Чтобы настроить автоматическую установку приложений на новые устройства в группе администрирования:*

1. Выберите в дереве консоли нужную вам группу администрирования.
2. Откройте окно свойств этой группы администрирования.
3. В панели **Разделы** в разделе **Автоматическая установка** выберите инсталляционные пакеты, которые следует устанавливать на новые устройства.
4. Нажмите на кнопку **ОК**.

Групповые задачи созданы. Эти задачи будут запускаться на клиентских устройствах сразу после их добавления в группу администрирования.

Если для автоматической установки указано несколько инсталляционных пакетов одного приложения, задача установки будет создана только для последней версии приложения.

Управление клиентскими устройствами

Этот раздел содержит информацию о работе с клиентскими устройствами.

В этом разделе

Подключение клиентских устройств к Серверу администрирования	748
Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover ..	750
Туннелирование соединения клиентского устройства с Сервером администрирования	751
Удаленное подключение к рабочему столу клиентского устройства	752
Подключение к устройствам с помощью совместного доступа к рабочему столу Windows	755
Настройка перезагрузки клиентского устройства	755
Аудит действий на удаленном клиентском устройстве	756
Проверка соединения клиентского устройства с Сервером администрирования	756
Идентификация клиентских устройств на Сервере администрирования	761
Перемещение устройств в состав группы администрирования	761
Смена Сервера администрирования для клиентских устройств	762
Кластеры и массивы серверов	763
Удаленное включение, выключение и перезагрузка клиентских устройств	763
Об использовании постоянного соединения между управляемым устройством и Сервером администрирования	764
О принудительной синхронизации	764
О расписании соединений	765
Отправка сообщения пользователям устройств	765
Работа с приложением Kaspersky Security для виртуальных сред	765
Настройка переключения статусов устройств	766
Назначение тегов устройствам и просмотр назначенных тегов	770
Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center	773
Устройства с защитой на уровне UEFI	781
Параметры управляемого устройства	782
Общие параметры политик	788
Параметры политики Агента администрирования	789

Подключение клиентских устройств к Серверу администрирования

Подключение клиентского устройства к Серверу администрирования осуществляет Агент администрирования, установленный на клиентском устройстве.

При подключении клиентского устройства к Серверу администрирования выполняются следующие операции:

- Автоматическая синхронизация данных:

- синхронизация списка приложений, установленных на клиентском устройстве;
- синхронизация политик, параметров приложений, задач и параметров задач.
- Получение Сервером текущей информации о состоянии приложений, выполнении задач и статистики работы приложений.
- Доставка на Сервер информации о событиях, которые требуется обработать.

Автоматическая синхронизация данных производится периодически, в соответствии с параметрами Агента администрирования (например, один раз в 15 минут). Вы можете вручную задать интервал между соединениями.

Информация о событии доставляется на Сервер администрирования сразу после того, как событие произошло.

Если Сервер администрирования является удаленным, то есть находится вне сети организации, клиентские устройства подключаются к нему через интернет.

Для подключения устройств к Серверу администрирования через интернет должны быть выполнены следующие условия:

- Удаленный Сервер администрирования должен иметь внешний IP-адрес, и на нем должен быть открыт входящий порт 13000 (для подключения от Агентов администрирования). Рекомендуется также открыть порт UDP 13000 (для приема уведомлений о выключении устройств).
- На устройствах должны быть установлены Агенты администрирования.
- При установке Агента администрирования на устройства должен быть указан внешний IP-адрес удаленного Сервера администрирования. Если для установки используется инсталляционный пакет, внешний IP-адрес требуется указать вручную в свойствах инсталляционного пакета в разделе **Параметры**.
- Для управления приложениями и задачами устройства с помощью удаленного Сервера администрирования требуется установить флажок **Не разрывать соединение с Сервером администрирования** в окне свойств этого устройства в разделе **Общие**. После установки флажка необходимо дождаться синхронизации Сервера администрирования с удаленным устройством. Непрерывное соединение с Сервером администрирования могут поддерживать не более 300 клиентских устройств одновременно.

Для ускорения выполнения задач, поступающих от удаленного Сервера администрирования, можно открыть на устройстве порт 15000. В этом случае для запуска задачи Сервер администрирования посылает специальный пакет Агенту администрирования по порту 15000, не дожидаясь синхронизации с устройством.

Kaspersky Security Center позволяет настроить соединение клиентского устройства с Сервером администрирования таким образом, чтобы соединение не завершалось по окончании выполнения операций. Непрерывное соединение необходимо в том случае, если требуется постоянный контроль состояния приложений, а Сервер администрирования не может инициировать соединение с клиентским устройством (например, соединение защищено сетевым экраном, запрещено открывать порты на клиентском устройстве, неизвестен IP-адрес клиентского устройства). Установить неразрывное соединение клиентского устройства с Сервером администрирования можно в окне свойств устройства, в разделе **Общие**.

Рекомендуется устанавливать непрерывное соединение с наиболее важными устройствами. Общее количество соединений, поддерживаемых Сервером администрирования одновременно, ограничено (до 300).

При синхронизации вручную используется вспомогательный способ подключения, при котором соединение инициирует Сервер администрирования. Перед подключением на клиентском устройстве требуется открыть UDP-порт. Сервер администрирования посылает на UDP-порт клиентского устройства запрос на соединение. В ответ на него производится проверка сертификата Сервера администрирования. Если сертификат Сервера совпадает с копией сертификата на клиентском устройстве, соединение осуществляется.

Запуск процесса синхронизации вручную используется также для получения текущей информации о состоянии приложений, выполнении задач и статистике работы приложений.

Подключение клиентского устройства к Серверу администрирования вручную. Утилита `klmover`

Если вам требуется подключить клиентское устройство к Серверу администрирования вручную, вы можете воспользоваться утилитой `klmover` на клиентском устройстве.

При установке на клиентское устройство Агента администрирования утилита автоматически копируется в папку установки Агента администрирования.

- Чтобы подключить клиентское устройство к Серверу администрирования вручную с помощью утилиты `klmover`,

на устройстве запустите утилиту `klmover` из командной строки.

При запуске из командной строки утилита `klmover` в зависимости от используемых ключей выполняет следующие действия:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает результаты выполнения операции в файл журнала событий или выводит их на экран.

Синтаксис командной строки утилиты:

```
klmover [-logfile <имя файла>] [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>] [-silent] [-dupfix] [-virtserv] [-cloningmode]
```

Для запуска утилиты требуются права администратора.

Описания ключей:

- `-logfile <имя файла>` – записать результаты выполнения утилиты в файл журнала.
По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, результаты и сообщения об ошибках выводятся на экран.
- `-address <адрес сервера>` – адрес Сервера администрирования для подключения.

В качестве адреса можно указать IP-адрес, NetBIOS- или DNS-имя устройства.

- `-pn <номер порта>` – номер порта, по которому будет осуществляться незашифрованное подключение к Серверу администрирования.

По умолчанию установлен порт 14000.

- `-ps <номер SSL-порта>` – номер SSL-порта, по которому осуществляется зашифрованное подключение к Серверу администрирования с использованием протокола SSL.

По умолчанию установлен порт 13000.

- `-nossl` – использовать незашифрованное подключение к Серверу администрирования.

Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному SSL-протоколу.

- `-cert <путь к файлу сертификата>` – использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования.

Если ключ не используется, Агент администрирования получает сертификат при первом подключении к Серверу администрирования.

- `-silent` – запустить утилиту на выполнение в неинтерактивном режиме.

Использование ключа может быть полезно, например, при запуске утилиты из сценария входа при регистрации пользователя.

- `-dupfix` – ключ используется в случае, если установка Агента администрирования была выполнена не традиционным способом, с использованием дистрибутива, а, например, путем восстановления из образа диска.
- `-virtserv` – имя виртуального Сервера администрирования.
- `-cloningmode` – режим клонирования диска Агента администрирования.

Используйте один из следующих параметров для настройки режима клонирования диска:

- `-cloningmode` – запрос состояния режима клонирования диска.
- `-cloningmode 1` – включить режим клонирования диска.
- `-cloningmode 0` – выключить режим клонирования диска.

Например, чтобы подключить Агент администрирования к Серверу администрирования, выполните следующую команду:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Туннелирование соединения клиентского устройства с Сервером администрирования

Kaspersky Security Center позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

В частности, туннелирование используется для подключения к удаленному рабочему столу: как для подключения к существующей сессии, так и для создания новой удаленной сессии.

Также туннелирование может быть использовано при помощи механизма внешних инструментов. В

частности, администратор может запускать таким образом утилиту putty, VNC-клиент и прочие инструменты.

Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

- Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
- Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт сетевым экраном.

► *Чтобы произвести туннелирование соединения клиентского устройства с Сервером администрирования:*

1. В дереве консоли выберите папку группы, в которую входит клиентское устройство.
2. На вкладке **Устройства** выберите устройство.
3. В контекстном меню устройства выберите пункт **Все задачи** → **Туннелирование соединения**.
4. Создайте туннель в открывшемся окне **Туннелирование соединения**.

Удаленное подключение к рабочему столу клиентского устройства

Администратор может получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве.

Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа. После подключения к устройству администратор получает полный доступ к информации на этом устройстве и может управлять приложениями, установленными на нем.

В этом разделе описывается, как установить соединение с клиентским устройством с операционной системой Windows (см. раздел "Подключение к клиентским устройствам с операционной системой Windows" см. стр. [752](#)) и клиентским устройством с операционной системой macOS (см. раздел "Подключение к клиентским устройствам с операционной системой macOS" см. стр. [754](#)) через Агент администрирования.

См. также:

Подключение к клиентским устройствам с операционной системой Windows	752
Подключение к клиентским устройствам с операционной системой macOS	754
Варианты лицензирования Kaspersky Security Center	354

Подключение к клиентским устройствам с операционной системой Windows

Удаленное подключение к клиентскому устройству с операционной системой Windows можно осуществить двумя способами:

- С помощью стандартного компонента Microsoft Windows "Подключение к удаленному рабочему столу".

Подключение к удаленному рабочему столу выполняется с помощью штатной утилиты Windows mstsc.exe в соответствии с параметрами работы этой утилиты.

- С помощью технологии совместного доступа к рабочему столу Windows.

Подключение к клиентскому устройству с операционной системой Windows с помощью подключения к удаленному рабочему столу

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. После подключения администратора к сеансу пользователь устройства будет отключен от сеанса без предварительного уведомления.

► Чтобы подключиться к рабочему столу клиентского устройства с помощью компонента "Подключение к удаленному рабочему столу":

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи** → **Подключиться к устройству** → **Новая сессия RDP**.

В результате будет запущена штатная утилита Windows mstsc.exe для подключения к удаленному рабочему столу.

3. Следуйте указаниям в открывающихся окнах утилиты.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

Подключение к клиентскому устройству с операционной системой Windows с помощью совместного доступа к рабочему столу Windows

При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит запрос от администратора на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky Security Center.

Администратор может подключиться к существующему сеансу на клиентском устройстве без отключения пользователя, работающего в этом сеансе. В этом случае у администратора и пользователя сеанса на устройстве есть совместный доступ к рабочему столу.

Администратор может настроить аудит действий на удаленном клиентском устройстве. В ходе аудита приложение сохраняет информацию о файлах на клиентском устройстве, которые открывал и/или изменял администратор (см. раздел "Аудит действий на удаленном клиентском устройстве" на стр. [756](#)).

Для подключения к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows требуется выполнение следующих условий:

- На рабочем месте администратора установлена операционная система Microsoft Windows Vista или более поздняя версия. Тип операционной системы устройства, на котором установлен Сервер администрирования, не является ограничением для подключения с помощью совместного доступа к рабочему столу Windows.

Чтобы проверить, включена ли функция совместного доступа к рабочему столу Windows в вашей версии Windows, убедитесь, что ключ CLSID{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} включен в реестре Windows.

- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.
- Kaspersky Security Center использует лицензию на Системное администрирование.

► *Чтобы подключиться к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows:*

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи** → **Подключиться к устройству** → **Совместный доступ к рабочему столу Windows**.
3. В открывшемся окне **Выбор сессии рабочего стола** выберите сеанс на клиентском устройстве, к которому требуется подключиться.

В случае успешного подключения к клиентскому устройству рабочий стол этого устройства будет доступен в окне **Kaspersky Remote Desktop Session Viewer**.

4. Для начала взаимодействия с устройством в главном меню окна **Kaspersky Remote Desktop Session Viewer** выберите пункт **Действия** → **Интерактивный режим**.

Для работы утилиты **Kaspersky Remote Desktop Session Viewer** требуется коммерческая лицензия (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. 354).

Подключение к клиентским устройствам с операционной системой macOS

Администратор может использовать систему Virtual Network Computing (VNC) для подключения к устройствам с операционной системой macOS.

Подключение к удаленному рабочему столу осуществляется с помощью VNC-клиента, установленного на устройстве Сервера администрирования. VNC-клиент переключает управление клавиатурой и мышью с клиентского устройства на администратора.

Когда администратор подключается к удаленному рабочему столу, пользователь не получает уведомлений или запросов на подключение от администратора. Администратор подключается к существующему сеансу на клиентском устройстве без отключения пользователя, работающего в этом сеансе.

Для подключения к рабочему столу клиентского устройства с операционной системой macOS с помощью VNC-клиента требуется выполнение следующих условий:

- VNC-клиент установлен на устройстве Сервера администрирования.
- На клиентском устройстве разрешены удаленный вход и удаленное управление.
- Пользователь разрешил администратору доступ к клиентскому устройству в параметры **Обмен** в операционной системе macOS.

► *Чтобы подключиться к рабочему столу клиентского устройства с помощью системы Virtual Network Computing:*

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи** → **Туннелирование соединения**.
3. В открывшемся окне **Туннелирование соединения** выполните одно из следующих действий:
 - a. В разделе **1. Сетевой порт** укажите номер порта устройства, к которому требуется подключиться.

По умолчанию номер порта – 5900.

- b. В разделе **2. Туннелирование** нажмите на кнопку **Создать туннель**.
- c. В разделе **3. Сетевые атрибуты** нажмите на кнопку **Копировать**.
4. Откройте VNC-клиент и вставьте скопированные сетевые атрибуты в текстовое поле. Нажмите на клавишу **ENTER**.
5. В появившемся окне просмотрите параметры сертификата. Если вы согласны использовать сертификат, нажмите на кнопку **Да**.
6. В окне **Аутентификация** укажите учетные данные клиентского устройства и нажмите на кнопку **ОК**.

Подключение к устройствам с помощью совместного доступа к рабочему столу Windows

► *Чтобы подключиться к устройству с помощью совместного доступа к рабочему столу Windows:*

1. В дереве консоли на вкладке **Устройства** выберите папку **Управляемые устройства**.
В рабочей области папки отображается список устройств.
2. В контекстном меню устройства, к которому вы хотите подключиться, выберите пункт **Подключиться к устройству** → **Совместный доступ к рабочему столу Windows**.
Откроется окно **Выбор сессии рабочего стола**.
3. В окне **Выбор сессии рабочего стола** выберите сессию рабочего стола, которая будет использоваться для подключения к устройству.
4. Нажмите на кнопку **ОК**.
Будет выполнено подключение к устройству.

Настройка перезагрузки клиентского устройства

В ходе работы, установки или удаления Kaspersky Security Center может потребоваться перезагрузка клиентского устройства. Вы можете настроить параметры перезагрузки только для устройств под управлением Windows.

► *Чтобы настроить перезагрузку клиентского устройства:*

1. В дереве консоли выберите группу администрирования, для которой нужно настроить перезагрузку.
2. В рабочей области группы выберите вкладку **Политики**.
3. В списке политик выберите политику Агента администрирования Kaspersky Security Center и в контекстном меню политики выберите пункт **Свойства**.
4. В окне свойств политики выберите раздел **Управление перезагрузкой**.
5. Выберите действие, которое нужно выполнять, если потребуется перезагрузка устройства:
 - Выберите **Не перезагружать операционную систему**, чтобы запретить автоматическую перезагрузку.
 - Выберите **При необходимости перезагрузить операционную систему автоматически**, чтобы разрешить автоматическую перезагрузку.
 - Выберите **Запрашивать у пользователя**, чтобы включить запрос на перезагрузку у пользователя.

Вы можете указать периодичность запроса на перезагрузку, включить принудительную перезагрузку и принудительное закрытие приложений в заблокированных сессиях на устройстве, установив соответствующие флажки и интервалы.

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно свойств политики.

В результате перезагрузка операционной системы устройства будет настроена.

Аудит действий на удаленном клиентском устройстве

Приложение позволяет выполнять аудит действий администратора на удаленных клиентских устройствах под управлением Windows. В ходе аудита приложение сохраняет информацию о файлах на устройстве, которые открывал и/или изменял администратор. Аудит действий администратора доступен при выполнении следующих условий:

- лицензия на Системное администрирование уже используется;
- у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

► Чтобы включить аудит действий на удаленном клиентском устройстве:

1. В дереве консоли выберите группу администрирования, для которой нужно настроить аудит действий администратора.
2. В рабочей области группы выберите вкладку **Политики**.
3. Выберите политику Агента администрирования Kaspersky Security Center и в контекстном меню политики выберите пункт **Свойства**.
4. В окне свойств политики выберите раздел **Совместный доступ к рабочему столу Windows**.
5. Установите флажок **Включить аудит**.
6. В списке **Маски файлов, чтение которых нужно отслеживать** и **Маски файлов, изменение которых нужно отслеживать** добавьте маски файлов, для которых приложение будет контролировать действия во время аудита.

По умолчанию приложение отслеживает действия с файлами с расширениями .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt, and .pdf.

7. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно свойств политики.

В результате аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу будет настроен.

Записи о действиях администратора на удаленном устройстве сохраняются:

- в журнале событий на удаленном устройстве;
- в файле с расширением syslog, который находится в папке Агента администрирования на удаленном устройстве (например, C:\ProgramData\KasperskyLab\adminkit\1103\logs);
- в базе событий Kaspersky Security Center.

Проверка соединения клиентского устройства с Сервером администрирования

Kaspersky Security Center позволяет проверять соединение клиентского устройства с Сервером администрирования автоматически или вручную.

Автоматическая проверка соединения осуществляется на Сервере администрирования. Проверка

соединения вручную осуществляется на устройстве.

Автоматическая проверка соединения клиентского устройства с Сервером администрирования

► Чтобы запустить автоматическую проверку соединения клиентского устройства с Сервером администрирования:

1. В дереве консоли выберите группу администрирования, в которую входит устройство.
2. В рабочей области группы администрирования на вкладке **Устройства** выберите устройство.
3. В контекстном меню устройства выберите пункт **Проверить доступность устройства**.

В результате открывается окно, содержащее информацию о доступности устройства.

Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита klnagchk

Вы можете проверять соединение и получать подробную информацию о параметрах подключения клиентского устройства к Серверу администрирования с помощью утилиты klnagchk. Утилита klnagchk находится в папке установки Агента администрирования.

При запуске из командной строки утилита klnagchk в зависимости от используемых ключей выполняет следующие действия:

- Выводит на экран или заносит в файл журнала событий значения параметров подключения Агента администрирования, установленного на устройстве, к Серверу администрирования.
- Записывает в файл журнала событий статистику Агента администрирования (с момента его последнего запуска) и результаты выполнения утилиты либо выводит информацию на экран.
- Пытается установить соединение Агента администрирования с Сервером администрирования. Если соединение установить не удалось, утилита посылает ICMP-пакет для проверки статуса устройства, на котором установлен Сервер администрирования.

► Чтобы проверить соединение клиентского устройства с Сервером администрирования с помощью утилиты klnagchk,

на устройстве с установленным Агентом администрирования запустите утилиту klnagchk из командной строки под учетной записью локального администратора.

Синтаксис командной строки утилиты:

```
klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>]  
[-restart] [-sendhb]
```

Описания ключей:

- `-logfile <имя файла>` – записывает значения параметров подключения Агента администрирования к Серверу и результаты выполнения утилиты в файл журнала. По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, параметры, результаты и сообщения об ошибках выводятся на экран.
- `-sp` – выводит пароль для аутентификации пользователя на прокси-сервере.

Ключ используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.

- `-savecert <имя файла>` – сохраняет сертификат для аутентификации доступа к Серверу администрирования в указанном файле.
- `-restart` – запускает Агент администрирования после завершения работы утилиты.
- `-sendhb` – запускает синхронизацию Агента администрирования с Сервером администрирования.

После запуска утилита `klmchk` обращается к конфигурационным файлам Агента администрирования и отображает параметры подключения. Эти параметры задаются при установке Агента администрирования и в параметрах политики Агента администрирования (см. раздел "Параметры политики Агента администрирования" см. стр. [789](#)):

- `Current device` – имя клиентского устройства в сети Windows.
- `Network Agent version` – номер версии Агента администрирования (с патчами), установленного на устройстве.
- `Administration Server address` – адрес Сервера администрирования.
- `Use SSL` – параметр, указывающий, используется ли защищенное соединение при подключении к Серверу администрирования.

Возможные значения:

- 0 – защищенный канал не используется.
- 1 – используется защищенный канал.
- `Compress traffic` – параметр, указывающий, сжимается ли трафик между клиентским устройством и Сервером администрирования.
- `Numbers of the Administration Server SSL ports` – номера допустимых портов для подключения к Серверу администрирования при использовании защищенного канала.
- `Numbers of the Administration Server ports` – номера портов, допустимых для подключения к Серверу администрирования при использовании обычного соединения.
- `Use proxy server` – параметр, указывающий, используется ли прокси-сервер.

Возможные значения:

- 0 – прокси-сервер не используется.
- 1 – прокси-сервер используется.
- `Address` – адрес и порт прокси-сервера, разделенные двоеточием. Этот параметр отображается, только если используется прокси-сервер.
- `User name` – имя пользователя для доступа к прокси-серверу. Этот параметр отображается, только если используется прокси-сервер.
- `Password` – пароль для доступа к прокси-серверу. Этот параметр отображается, только если используется прокси-сервер. Чтобы показать пароль прокси-сервера, вам нужно использовать в команде ключ `sp`.
- `Administration Server certificate` – параметр, указывающий, есть ли у клиентского устройства сертификат Сервера администрирования. Сертификат может не существовать, например, если Агент администрирования ни разу не подключился к Серверу администрирования.

Возможные значения:

- `not installed` – на клиентском устройстве отсутствует сертификат Сервера администрирования.
- `available` – клиентское устройство имеет сертификат Сервера администрирования.
- `Open UDP port` – параметр, указывающий, использует ли Агент администрирования UDP-порт для получения запросов на синхронизацию от Сервера администрирования.

Возможные значения:

- `0` – UDP-порт закрыт для приема запросов на синхронизацию от Сервера администрирования.
- `1` – UDP-порт открыт для приема запросов на синхронизацию от Сервера администрирования.
- `Numbers of UDP ports` – номера UDP-портов, которые может использовать Агент администрирования.
- `Location name` – сетевое местоположение устройства.
- `State of network location` – параметр, указывающий, можно ли переключить клиентское устройство с одного профиля соединений Сервера администрирования на другой.

Возможные значения:

- `Enabled` – профиль соединений к Серверу администрирования можно переключить для клиентского устройства.
- `Disabled` – профиль соединений к Серверу администрирования переключить для клиентского устройства невозможно.
- `Profile to use` – профиль соединений к Серверу администрирования.
- `Condition` – IP-адрес и маска подсети сети, к которой подключено клиентское устройство.
- `Synchronization interval (min)` – стандартный интервал синхронизации.
- `Connection timeout (in seconds)` – время ожидания соединения.
- `Send / receive timeout (in seconds)` – время ожидания соединения для операций чтения-записи.
- `Device ID` – идентификатор устройства в сети. `Device ID` уникален для клиентских устройств, управляемых определенным Сервером администрирования.
- `Locations of connection gateways` – параметры подключения клиентского устройства к Серверу администрирования с помощью шлюза соединения.
- `Location of distribution points` – параметры подключения клиентского устройства к Серверу администрирования с помощью точки распространения.
- `Connection with server` – параметр, указывающий, имеет ли шлюз соединения постоянное соединение с Сервером администрирования. Параметр отображается только в том случае, если клиентское устройство выступает в роли шлюза соединения.

Возможные значения:

- `active` – шлюз соединения имеет постоянное соединение с Сервером администрирования.
- `inactive` – шлюз соединения не имеет постоянного соединения с Сервером администрирования.

- `Connection with server through connection gateway` – параметр, указывающий, правильно ли установлено соединение с Сервером администрирования с помощью шлюза соединения. Параметр отображается только в том случае, если клиентское устройство выступает в роли шлюза соединения.

Возможные значения:

- `active` – соединение с Сервером администрирования с помощью шлюза соединения установлено правильно.
- `inactive` – соединение с Сервером администрирования с помощью шлюза соединения установлено некорректно.

Также вывод утилиты `klmagchk` может содержать одну из следующих строк:

- `Administration Server is installed on this device` – на устройстве Сервера администрирования запущена утилита `klmagchk`.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` – утилита `klmagchk` запущена на устройстве, на котором установлен Агент администрирования, выполняющий роль шлюза соединения (см. раздел "Сценарий: подключение автономных устройств через шлюз соединения" см. стр. [297](#)). Настроенный шлюз соединения ожидает соединения от Сервера администрирования, но Сервер администрирования не перечисляет устройство среди управляемых устройств. Вам потребуется убедиться, что Сервер администрирования инициировал соединение со шлюзом соединения (см. раздел "Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения" см. стр. [693](#)).
- `This device is a connection gateway` – утилита `klmagchk` запускается на устройстве, которое выполняет роль шлюза соединения (см. раздел "Шлюз соединения" см. стр. [54](#)).
- `Acts as a distribution point` – утилита `klmagchk` запускается на устройстве, которое выполняет роль точки распространения (см. раздел "Назначение управляемого устройства точкой распространения" на стр. [688](#)).

Утилита `klmagchk` проверяет состояние службы Агента администрирования. Если служба не запущена, утилита останавливается. Если служба запущена, утилита отображает следующую статистику подключений:

- `Total number of synchronization requests` – количество попыток подключения клиентского устройства к Серверу администрирования.
- `The number of successful synchronization request` – количество успешных попыток подключения клиентского устройства к Серверу администрирования.
- `Total number of synchronizations` – количество попыток синхронизации параметров клиентского устройства с параметрами Сервера администрирования.
- `The number of successful synchronizations` – количество успешных попыток синхронизации параметров клиентского устройства с Сервером администрирования.
- `Date/time of the last request for synchronization` – дата и время последнего подключения.

При анализе соединения между Сервером администрирования и Агентом администрирования необходимо использовать параметры `Total number of synchronization requests` и `The number of successful synchronization request`. Параметры клиентского устройства синхронизируются с параметрами Сервера администрирования только в случае изменения параметров Сервера администрирования (например, при добавлении новых задач или изменении параметров политики). Иначе

значения параметров `Total number of synchronizations` и `The number of successful synchronization request` не изменяются.

Подробнее об устранении проблем с подключением Агента администрирования к Серверу администрирования см. Kaspersky Security Center FAQ <https://support.kaspersky.com/KSC/FAQ/en-US/273885.htm>.

О проверке времени соединения устройства с Сервером администрирования

При выключении устройства Агент администрирования уведомляет Сервер администрирования о выключении. В Консоли администрирования такое устройство отображается как выключенное. Однако Агенту удастся уведомить Сервер администрирования не во всех случаях. Поэтому Сервер администрирования для каждого устройства периодически анализирует атрибут **Соединение с Сервером администрирования** (значение атрибута отображается в Консоли администрирования в свойствах устройства в разделе **Общие**) и сопоставляет его с периодом синхронизации из действующих параметров Агента администрирования. Если устройство не выходило на связь более чем три периода синхронизации, то такое устройство отмечается как выключенное.

Идентификация клиентских устройств на Сервере администрирования

Идентификация клиентских устройств осуществляется на основании их имен. Имя устройства является уникальным среди всех имен устройств, подключенных к Серверу администрирования.

Имя устройства передается на Сервер администрирования либо при опросе сети Windows и обнаружении в ней нового устройства, либо при первом подключении к Серверу администрирования установленного на устройство Агента администрирования. По умолчанию имя совпадает с именем устройства в сети Windows (NetBIOS-имя). Если на Сервере администрирования уже зарегистрировано устройство с таким именем, то к имени нового устройства будет добавлено окончание с порядковым номером, например: **<Имя>-1**, **<Имя>-2**. Под этим именем устройство включается в состав группы администрирования.

Перемещение устройств в состав группы администрирования

Устройства можно перемещать из одной группы администрирования в другую только при наличии прав **Изменение** (см. раздел "**Назначение прав пользователям или группам пользователей**" на стр. [838](#)) в области **Управление группами администрирования** как для исходных, так и для целевых групп администрирования (или для Сервера администрирования, к которым принадлежат эти группы).

► *Чтобы включить одно или несколько устройств в состав выбранной группы администрирования:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В папке **Управляемые устройства** выберите вложенную папку, соответствующую группе, в состав которой будут включены клиентские устройства.

Если вы хотите включить устройства в состав группы **Управляемые устройства**, этот шаг можно пропустить.

3. В рабочей области выбранной группы администрирования на вкладке **Устройства** запустите процесс включения устройств в группу одним из следующих способов:
 - Добавьте устройства в группу по кнопке **Переместить устройства в группу** в блоке работы со списком устройств.
 - В контекстном меню списка устройств выберите **Создать** → **Устройство**.

В результате запустится мастер перемещения устройств. Следуя его указаниям, определите способ перемещения устройств в группу и сформируйте список устройств, включаемых в состав группы.

Если вы формируете список устройств вручную, в качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя. Вручную в список устройств могут быть перемещены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

Для импорта списка устройств из файла требуется указать файл в формате TXT с перечнем адресов добавляемых устройств. Каждый адрес должен располагаться в отдельной строке.

После завершения работы мастера выбранные устройства включаются в состав группы администрирования и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

Можно переместить устройство в выбранную группу администрирования, перетащив его мышью из папки **Нераспределенные устройства** в папку группы администрирования.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи *Смена Сервера администрирования*.

► *Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу смены Сервера администрирования одним из следующих способов:
 - Если требуется сменить Сервер администрирования для устройств, входящих в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание задачи" на стр. [416](#)).
 - Если требуется сменить Сервер администрирования для устройств, входящих в разные группы администрирования или не входящих в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. [418](#)).

Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне **Выбор типа задачи** мастера создания задачи выберите узел **Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу *Смена Сервера администрирования*.

3. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Если Сервер администрирования поддерживает управление шифрованием и защитой данных, то при создании задачи *Смена Сервера администрирования* отображается предупреждение. Предупреждение содержит информацию о том, что при наличии на устройствах зашифрованных данных после переключения устройств под управлением другого Сервера пользователям будет предоставлен доступ только к тем зашифрованным данным, с которыми они работали ранее. В остальных случаях доступ к зашифрованным данным предоставлен не будет. Подробное описание сценариев, в которых доступ к зашифрованным данным не будет предоставлен, приведено в справке Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/help/KESWin/12.6/en-US/128089.htm>.

Кластеры и массивы серверов

Kaspersky Security Center поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что приложение, установленное на клиентском устройстве, является частью массива сервера, то клиентское устройство становится узлом кластера. Кластер будет добавлен как отдельный объект в папке **Управляемые устройства** в дереве консоли со



значками серверов ().

Можно выделить несколько типичных свойств кластера:

- Кластер и любой из его узлов всегда располагаются в одной группе администрирования.
- Если администратор попытается переместить какой-либо узел кластера, то узел вернется в исходное местоположение.
- Если администратор попытается переместить кластер в другую группу, то все его узлы также переместятся вместе с ним.

Удаленное включение, выключение и перезагрузка клиентских устройств

Kaspersky Security Center позволяет удаленно управлять клиентскими устройствами, включать, выключать и перезагружать их.

► *Чтобы удаленно управлять клиентскими устройствами:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу управления устройствами одним из следующих способов:
 - Если требуется включить, выключить или перезагрузить устройства, входящие в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание задачи" на стр. [416](#)).
 - Если требуется включить, выключить или перезагрузить устройства, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. [418](#)).

Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне **Выбор типа задачи** мастера создания задачи выберите узел **Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Управление устройствами**.

3. Запустите созданную задачу.

После завершения работы задачи команда (включение, выключение или перезагрузка) будет выполнена на выбранных устройствах.

Об использовании постоянного соединения между управляемым устройством и Сервером администрирования

По умолчанию в Kaspersky Security Center нет постоянных соединений между управляемыми устройствами и Сервером администрирования. Агенты администрирования на управляемых устройствах периодически устанавливают соединение и синхронизируются с Сервером администрирования. Интервал между этими сеансами синхронизации определяется в политике Агента администрирования и по умолчанию составляет 15 минут. Если необходима досрочная синхронизация (например, для ускорения применения политики), то Сервер администрирования посылает Агенту администрирования подписанный сетевой пакет на порт UDP 15000. Сервер администрирования может отправить этот пакет по IPv4-сети или IPv6-сети. Если подключение по UDP от Сервера администрирования к управляемому устройству по какой-то причине невозможно, то синхронизация произойдет при очередном периодическом подключении Агента администрирования к Серверу в течение периода синхронизации.

Однако некоторые операции невозможно выполнить без подключения Агента администрирования к Серверу администрирования. Эти операции включают запуск и остановку локальных задач, получение статистики для управляемого приложения и создание туннеля. Чтобы эти операции стали возможными, необходимо включить на управляемом устройстве (см. раздел "Параметры управляемого устройства" на стр. [782](#)) параметр **Не разрывать соединение с Сервером администрирования**.

См. также:

Информация об ограничениях Kaspersky Security Center[151](#)

О принудительной синхронизации

Несмотря на то, что Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору нужно точно знать, что в текущий момент для определенного устройства синхронизация выполнена.

В контекстном меню управляемых устройств в Консоли администрирования в пункте меню **Все задачи** имеется команда **Синхронизировать принудительно**. Когда Kaspersky Security Center выполняет эту команду, Сервер администрирования пытается подключиться к устройству. Если эта попытка успешна, будет выполнена принудительная синхронизация. В противном случае принудительная синхронизация произойдет только после очередного выхода Агента администрирования на связь с Сервером.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства[405](#)

О расписании соединений

В окне свойств политики Агента администрирования в разделе **Подключения** во вложенном разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования.

Подключаться при необходимости. Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

Подключаться в указанные периоды. Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Отправка сообщения пользователям устройств

► *Чтобы отправить сообщение пользователям устройств:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. Создайте задачу отправки сообщения пользователям устройств одним из следующих способов:
 - Если требуется отправить сообщение пользователям устройств, входящих в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание задачи" на стр. [416](#)).
 - Если требуется отправить сообщение пользователям устройств, входящих в разные группы администрирования или не принадлежащих ни одной группе администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. [418](#)).

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. В окне Тип задачи мастера создания задачи выберите узел **Сервер администрирования Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Сообщение для пользователя**. Отправка сообщений пользователю с помощью задачи доступна только для устройств под управлением операционной системы Windows. Также вы можете отправить сообщение из контекстного меню пользователя из рабочей области папки **Управление учетными записями пользователей** (см. раздел "Рассылка сообщений пользователям" на стр. [842](#)).
4. Запустите созданную задачу.

После завершения работы задачи созданное сообщение будет отправлено пользователям выбранных устройств. Отправка сообщений пользователю с помощью задачи доступна только для устройств под управлением операционной системы Windows. Также вы можете отправить сообщение из контекстного меню пользователя из рабочей области папки **Учетные записи пользователей** (см. раздел "Рассылка сообщений пользователям" на стр. [842](#)).

Работа с приложением Kaspersky Security для виртуальных сред

Kaspersky Security Center поддерживает возможность подключения виртуальных машин к Серверу администрирования. Защита виртуальных машин осуществляется с помощью программы Kaspersky Security для виртуальных сред. Подробнее см. в документации к этому приложению.

Настройка переключения статусов устройств

Kaspersky Security Center позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*.

► Чтобы изменить статус устройства на *Критический*:

- Откройте окно свойств одним из следующих способов:
 - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
 - В контекстном меню группы администрирования выберите пункт **Свойства**.
- В открывшемся окне Свойства в панели **Разделы** выберите раздел **Статус устройства**.
- В блоке **Установить статус "Критический"** установите флажок для условия из списка.
- Для выбранного условия установите необходимое вам значение.
Не для всех условий можно задать значения.
- Нажмите на кнопку **ОК**.

► Чтобы изменить статус устройства на *Предупреждение*:

- Откройте окно свойств одним из следующих способов:
 - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
 - В контекстном меню группы администрирования выберите пункт **Свойства**.
- В открывшемся окне Свойства в панели **Разделы** выберите раздел **Статус устройства**.
- В блоке **Установить статус "Предупреждение"** установите флажок для условия из списка.
- Для выбранного условия установите необходимое вам значение.
Не для всех условий можно задать значения.
- Нажмите на кнопку **ОК**.

Разным значениям одного условия могут соответствовать разные статусы. Например, при соблюдении условия **Базы устарели** со значением *Более 7 дней* клиентскому устройству присваивается статус *Предупреждение*, а со значением *Более 14 дней* – статус *Критический*.

В таблице приведены условия для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения

Таблица 70. Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	- Флажок установлен. - Флажок снят.

Условие	Описание условия	Доступные значения
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вирусов, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но задача поиска вирусов не выполнялась больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня
Обнаружены активные угрозы	Количество необработанных объектов в папке Необработанные файлы превышает указанное значение.	Более чем 0 штук

Условие	Описание условия	Доступные значения
Требуется перезагрузка	Устройство видимо в сети, но приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Флажок снят. • Флажок установлен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи Поиск уязвимостей и требуемых обновлений на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если нельзя закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Флажок снят. • Флажок установлен.
Срок действия лицензии скоро истечет	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней

Условие	Описание условия	Доступные значения
Давно не выполнялась проверка обновлений Центра обновления Windows	Не выполнялась задача Синхронизация обновлений Windows Update больше указанного времени.	Более 1 дня
Указанный статус шифрования данных	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Флажок снят. • Флажок установлен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором.	• Флажок снят. • Флажок установлен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	• Флажок снят. • Флажок установлен.

Условие	Описание условия	Доступные значения
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы <i>Критический</i> или <i>Предупреждение</i> меняются на статус <i>ОК</i> , когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	- Флажок снят. - Флажок установлен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве выключено больше указанного времени.	Более чем 0 минут
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	- Флажок снят. - Флажок установлен.

См. также:

Настройка общих параметров Сервера администрирования [716](#)

Назначение тегов устройствам и просмотр назначенных тегов

Kaspersky Security Center позволяет назначать теги устройствам. *Тег* представляет собой идентификатор устройства, который можно использовать для группировки, описания, поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств, при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Ручное назначение тегов устройству выполняется в свойствах устройства и может потребоваться, когда необходимо отметить отдельное

устройство. Автоматическое назначение тегов выполняется Сервером администрирования в соответствии с заданными правилами назначения тегов.

В свойствах Сервера администрирования вы можете настроить автоматическое назначение тегов устройствам, управляемым этим Сервером администрирования. Автоматическое назначение тегов устройствам происходит при выполнении определенных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве приложениям и другим свойствам устройства. Например, вы можете настроить правило, в соответствии с которым устройствам, работающим под управлением операционной системы Windows, назначается тег *Win*. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать устройства, работающие под управлением операционной системы Windows, и назначить им задачу.

Вы также можете использовать теги в качестве условия для активации профиля политики на управляемом устройстве, чтобы определенные профили политик применялись только на устройствах, имеющих определенные теги. Например, если в группе администрирования *Пользователи* появляется устройство с тегом *Курьер* и по тегу *Курьер* настроена активация соответствующего профиля политики, то к этому устройству будет применяться не сама политика, созданная для группы *Пользователи*, а ее профиль. Профиль политики может разрешить на этом устройстве запуск отдельных приложений, которые запрещено запускать в рамках политики.

Вы можете создать несколько правил назначения тегов. Одному устройству может быть назначено несколько тегов, в случае если вы создали несколько правил назначения тегов и условия этих правил выполняются одновременно. Вы можете просмотреть список всех назначенных тегов в свойствах устройства. Каждое правило назначения тегов можно включить или выключить. Если правило включено, оно применяется к устройствам, управляемым Сервером администрирования. Если правило не нужно, но может понадобиться в дальнейшем, то нет необходимости его удалять; достаточно снять флажок **Включить правило**. При этом правило выключается и не выполняется до тех пор, пока флажок **Включить правило** не будет установлен. Отключение правила без удаления может потребоваться, если это правило необходимо временно исключить из списка правил назначения тегов, а потом опять включить.

В этом разделе

Автоматическое назначение тегов устройствам.....	771
Просмотр и настройка тегов, назначенных устройству.....	773

Автоматическое назначение тегов устройствам

Вы можете создавать и изменять правила автоматического назначения тегов в окне свойств Сервера администрирования.

► Чтобы автоматически назначить теги устройствам:

1. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется задать правила назначения тегов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Правила назначения тегов**.
4. В разделе **Правила назначения тегов** нажмите на кнопку **Добавить**.

Откроется окно **Новое правило**.

5. В окне **Новое правило** настройте общие свойства правила:

- Укажите имя правила.

Имя правила не может превышать 255 символов и содержать специальные символы (" * < > ? \ : |).

- Включите или выключите правило с помощью флажка **Включить правило**.

По умолчанию флажок **Включить правило** установлен.

- В поле **Тег** введите название тега.

Название тега не может превышать 255 символов и содержать специальные символы (" * < > ? \ : |).

6. В разделе **Условия** нажмите на кнопку **Добавить**, чтобы добавить новое условие, или нажмите на кнопку **Свойства**, чтобы изменить существующее условие.

Откроется окно мастера создания условия для правила автоматического назначения тегов.

7. В окне **Условие назначения тега** установите флажки для тех условий, которые должны влиять на назначения тега. Можно выбрать несколько условий.

8. В зависимости от того, какие условия назначения тега вы выбрали, мастер покажет окна для настройки соответствующих условий. Настройте срабатывание правила по следующим условиям:

- **Использование или отношение устройства к определенной сети** – сетевые свойства устройства (например, имя устройства в сети Windows, принадлежность устройства к домену, к IP-диапазону).

Если для базы данных, которую вы используете для Kaspersky Security Center, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

- **Использование Active Directory** – нахождение устройства в подразделении Active Directory и членство устройства в группе Active Directory.
- **Определенные приложения** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.
- **Виртуальные машины** – принадлежность устройства к разным типам виртуальных машин.
- **Установлено приложение из реестра приложений** – наличие на устройстве приложений различных производителей.

9. После настройки условия введите название условия и завершите работу мастера.

При необходимости можно задать несколько условий для одного правила. В этом случае тег будет назначен устройствам, если для них выполняется хотя бы одно из условий. Добавленные условия отображаются в окне свойств правила.

10. Нажмите на кнопку **ОК** в окне **Новое правило** и на кнопку **ОК** в окне свойств Сервера администрирования.

Созданные правила выполняются на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

Просмотр и настройка тегов, назначенных устройству

Вы можете просмотреть список всех тегов, назначенных устройству, а также перейти к настройке правил автоматического назначения тегов в окне свойств устройства.

► *Чтобы просмотреть и настроить назначенные устройству теги:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В рабочей области папки **Управляемые устройства** выберите устройство, для которого вы хотите посмотреть назначенные теги.
3. В контекстном меню мобильного устройства выберите пункт **Свойства**.
4. В окне свойств устройства выберите раздел **Теги**.

Отобразится список тегов, назначенных выбранному устройству, а также способ назначения тега: вручную или по правилу.

5. При необходимости выполните одно из следующих действий:
 - Чтобы перейти к настройке правил назначения тегов, перейдите по ссылке **Настроить правила автоматического назначения тегов** (только для устройств с операционной системой Windows).
 - Чтобы переименовать тег, выделите тег и нажмите на кнопку **Переименовать**.
 - Чтобы удалить тег, выделите тег и нажмите на кнопку **Удалить**.
 - Чтобы добавить тег вручную, введите тег в поле в нижней части раздела **Теги** и нажмите на кнопку **Добавить**.
6. Нажмите на кнопку **Применить**, если вы делали изменения в разделе **Теги**, чтобы ваши изменения вступили в силу.
7. Нажмите на кнопку **ОК**.

Если вы удалили или переименовали тег в свойствах устройства, это изменение не распространится на правила назначения тегов, заданные в свойствах Сервера администрирования. Изменение будет применено только к тому устройству, в свойства которого вы внесли изменение.

Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center

Утилита удаленной диагностики Kaspersky Security Center (далее – утилита удаленной диагностики) предназначена для удаленного выполнения на клиентских устройствах следующих операций:

- включения и выключения трассировки, изменения уровня трассировки, загрузки файла трассировки;
- загрузки системной информации и параметров приложения;
- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуска и остановки приложений.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также специалист Службы технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал

событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

Утилита удаленной диагностики автоматически устанавливается на устройство совместно с Консолью администрирования.

В этом разделе

Подключение утилиты удаленной диагностики к клиентскому устройству	774
Создание файла дампа для приложения	776
Включение и выключение трассировки, загрузка файла трассировки	777
Загрузка параметров приложений	779
Загрузка журналов событий	780
Загрузка нескольких диагностических информационных элементов	780
Запуск диагностики и загрузка ее результатов	780
Запуск, остановка и перезапуск приложений	781

Подключение утилиты удаленной диагностики к клиентскому устройству

► Чтобы подключить утилиту удаленной диагностики к клиентскому устройству:

1. В дереве консоли выберите любую группу администрирования.
2. В рабочей области на вкладке **Устройства** в контекстном меню любого устройства выберите пункт **Внешние инструменты** → **Удаленная диагностика**.
В результате открывается главное окно утилиты удаленной диагностики.
3. В первом поле главного окна утилиты удаленной диагностики определите, какими средствами требуется подключиться к устройству:
 - **Доступ средствами сети Microsoft Windows.**
 - **Доступ средствами Сервера администрирования.**
4. Если в первом поле главного окна утилиты вы выбрали вариант **Доступ средствами сети Microsoft Windows**:
 - В поле **Устройство** укажите адрес устройства, к которому требуется подключиться.
В качестве адреса устройства можно использовать IP-адрес, NetBIOS- или DNS-имя.
По умолчанию указан адрес устройства, из контекстного меню которого запущена утилита.
 - Укажите учетную запись для подключения к устройству:
 - **Подключиться от имени текущего пользователя** (выбрано по умолчанию). Подключитесь под учетной записью текущего пользователя.
 - **При подключении использовать предоставленное имя пользователя и пароль.** Подключитесь под указанной учетной записью. Укажите **Имя пользователя** и **Пароль** нужной учетной записи.

Подключение к устройству возможно только под учетной записью локального администратора устройства.

5. Если в первом поле главного окна утилиты вы выбрали вариант **Доступ средствами Сервера администрирования**:
 - В поле **Сервер администрирования** укажите адрес Сервера администрирования, с которого следует подключиться к устройству.

В качестве адреса Сервера можно использовать IP-адрес, NetBIOS- или DNS-имя.

По умолчанию указан адрес Сервера, с которого запущена утилита.
 - Если требуется, установите флажки **Использовать SSL**, **Сжимать трафик** и **Устройство принадлежит подчиненному Серверу администрирования**.

Если установлен флажок **Устройство принадлежит подчиненному Серверу администрирования**, в поле **Устройство принадлежит подчиненному Серверу администрирования** вы можете выбрать подчиненный Сервер администрирования, под управлением которого находится устройство, нажав на кнопку **Обзор**.
6. Для подключения к устройству нажмите на кнопку **Войти**.

Вам нужно авторизовываться с помощью двухэтапной проверки (см. раздел "О двухэтапной проверке" на стр. [735](#)), если двухэтапная проверка для вашей учетной записи включена.

В результате откроется окно удаленной диагностики устройства (см. рис. ниже). В левой части окна расположены ссылки для выполнения операций по диагностике устройства. В правой части окна

расположено дерево объектов устройства, с которыми может работать утилита. В нижней части окна отображается процесс выполнения операций утилиты.

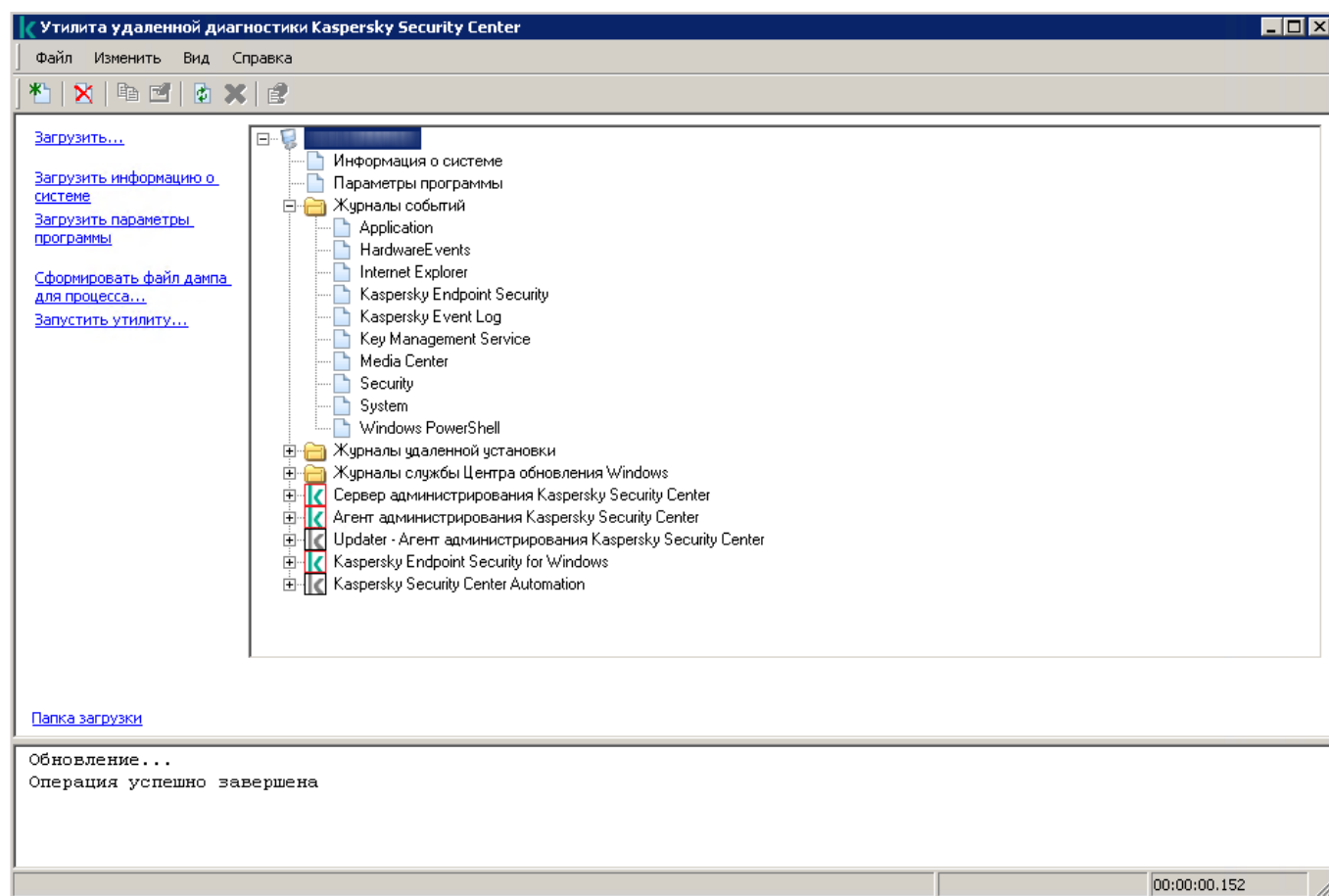


Рисунок 6. Утилита удаленной диагностики. Окно удаленной диагностики клиентского компьютера

Утилита удаленной диагностики сохраняет загруженные с устройств файлы на рабочем столе устройства, с которого она запущена.

См. также:

О двухэтапной проверке [735](#)

Создание файла дампа для приложения

Файл дампа приложения позволяет просматривать параметры приложения, работающего на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для приложения.

Получение файлов дампа с клиентских устройств с операционной системой Linux не поддерживается.

Чтобы получить файлы дампа с помощью удаленной диагностики, используется утилита kldumper. Эта утилита предназначена для получения файлов дампа процессов приложений "Лаборатории Касперского" по запросу специалистов Службы технической поддержки. Подробную информацию о требованиях к использованию утилиты kldumper приведена в Базе знаний Kaspersky Security Center.

► *Чтобы создать файл дампа для приложения:*

1. В рабочей области папки **Управляемые устройства** на вкладке **Устройства** в контекстном меню нужного устройства выберите пункт **Внешние инструменты** → **Удаленная диагностика**.

Откроется окно **Утилита удаленной диагностики Kaspersky Security Center**.

2. Подключите утилиту удаленной диагностики к клиентскому устройству (см. раздел "Подключение утилиты удаленной диагностики к клиентскому устройству" см. стр. [774](#)).

В результате откроется окно удаленной диагностики устройства.

3. В правой части окна перейдите по ссылке **Сформировать файл дампа для процесса**.
4. В открывшемся окне **Формирование дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.
5. Нажмите на кнопку **ОК**.

Архив с файлом дампа для указанного приложения загружен.

Если указанное приложение не запущено на клиентском устройстве, папка "result" в загруженном архиве будет пустой.

Если указанное приложение запущено, но загрузка завершается с ошибкой или папка "result" в загруженном архиве пуста, см. Базу знаний Kaspersky Security Center.

Включение и выключение трассировки, загрузка файла трассировки

► *Чтобы включить трассировку на удаленном устройстве:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному устройству (см. раздел "Подключение утилиты удаленной диагностики к клиентскому устройству" см. стр. [774](#)).
2. В дереве объектов устройства выберите приложение, для которого требуется включить трассировку.

Включение и выключение трассировки у приложений с самозащитой возможно только при подключении к устройству средствами Сервера администрирования.

Если вы хотите включить трассировку для Агента администрирования, вы также можете сделать это при создании задачи Установка требуемых обновлений и закрытие уязвимостей (см. раздел "Закрытие уязвимостей в приложениях" на стр. [541](#)). В этом случае Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики.

3. Чтобы включить трассировку:
 - a. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Включить трассировку**.
 - b. В открывшемся окне **Выбор уровня трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости специалист Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:

- **Уровень трассировки**

Уровень трассировки определяет состав информации, которую содержит файл трассировки.

- **Трассировка на основе ротации** (доступно только для Kaspersky Endpoint Security)

Приложение перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

a. Нажмите на кнопку **ОК**.

1. Для Kaspersky Endpoint Security специалисты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

Чтобы включить трассировку xperf:

- a. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Включить трассировку Xperf**.
- b. В открывшемся окне **Выбор уровня трассировки**, в зависимости от запроса специалиста Службы технической поддержки, выберите один из следующих уровней трассировки:

- **Легкий уровень**

Файл трассировки этого типа содержит минимальный объем информации о системе.

По умолчанию выбран этот вариант.

- **Детальный уровень**

Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит информацию об оборудовании, операционной системе, список запущенных и завершенных процессов и приложений, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

- c. Выберите один из уровней трассировки:

- **Базовый тип**

Приложение получает данные трассировки во время работы приложения Kaspersky Endpoint Security.

По умолчанию выбран этот вариант.

- **Тип перезагрузки**

Приложение получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

- d. Также вам могут предложить включить параметр **Трассировка на основе ротации**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.

- e. Нажмите на кнопку **ОК**.

В некоторых случаях для включения трассировки приложения безопасности требуется перезапустить это приложение и его задачу.

Утилита удаленной диагностики позволяет получать трассировку для выбранного приложения.

► *Чтобы загрузить файл трассировки приложения:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (см. стр. [774](#))".
2. В узле приложения в папке **Файлы трассировки** выберите требуемый файл.
3. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Загрузить весь файл**.

Для файлов большого объема есть возможность загрузить только последние части трассировки.

Вы можете удалить выделенный файл трассировки. Удаление файла возможно после выключения трассировки.

Выбранный файл загружается в местоположение, указанное в нижней части окна.

► *Чтобы выключить трассировку на удаленном устройстве:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (см. стр. [774](#))".
2. В дереве объектов устройства выберите приложение, для которого требуется выключить трассировку.

Включение и выключение трассировки у приложений с самозащитой возможно только при подключении к устройству средствами Сервера администрирования.

3. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Выключить трассировку**.

Утилита удаленной диагностики выключит трассировку для выбранного приложения.

Загрузка параметров приложений

► *Чтобы загрузить с удаленного устройства параметры приложений:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (см. стр. [774](#))".
2. В дереве объектов окна утилиты удаленной диагностики выберите верхний узел с именем устройства.
3. В левой части окна утилиты удаленной диагностики выберите требуемое действие из следующих параметров:

- **Загрузить информацию о системе**
- **Загрузить параметры приложения**
- **Сформировать файл дампа для процесса**

В окне, открывшемся по этой ссылке, укажите исполняемый файл приложения, для которого нужно сформировать файл дампа.

- **Запустить утилиту**

В окне, открывшемся по этой ссылке, укажите исполняемый файл утилиты, которую вы хотите запустить, и параметры ее запуска.

В результате выбранная утилита будет загружена на устройство и запущена на нем.

Загрузка журналов событий

► *Чтобы загрузить с удаленного устройства журнал событий:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (см. стр. [774](#))".
2. В папке **Журналы событий системы** в дереве объектов устройства выберите соответствующий журнал событий.
3. Чтобы загрузить журнал событий, перейдите по ссылке **Загрузить журнал событий <Имя журнала событий>** в левой части окна утилиты удаленной диагностики.

Выбранный журнал событий загружается в местоположение, указанное в нижней части окна.

Загрузка нескольких диагностических информационных элементов

Утилита удаленной диагностики Kaspersky Security Center позволяет загружать несколько элементов диагностической информации, включая журналы событий, системную информацию, файлы трассировки и файлы дампа.

► *Чтобы загрузить с удаленного устройства диагностическую информацию:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (см. стр. [774](#))".
2. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Загрузить**.
3. Установите флажки напротив объектов, которые вы хотите загрузить.
4. Нажмите на кнопку **Запустить**.

Каждый выбранный объект загружается в месторасположение, указанное в нижней панели.

Запуск диагностики и загрузка ее результатов

► *Чтобы запустить диагностику приложения на удаленном устройстве и загрузить ее результаты:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (см. стр. [774](#))".
2. В дереве объектов устройства выберите необходимое приложение.
3. Чтобы запустить диагностику, перейдите по ссылке **Выполнить диагностику** в левой части окна утилиты удаленной диагностики.

В результате в узле выбранного приложения в дереве объектов появится отчет диагностики.

4. Выберите сформированный отчет диагностики в дереве объектов и скачайте его по ссылке **Папка загрузки**.

Выбранный отчет загружается в местоположение, указанное в нижней части окна.

Запуск, остановка и перезапуск приложений

Запуск, остановка и перезапуск приложений возможны только при подключении к устройству средствами Сервера администрирования.

► Чтобы запустить, остановить или перезапустить приложение:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (см. стр. [774](#))".
2. В дереве объектов устройства выберите необходимое приложение.
3. Выберите действие в левой части окна утилиты удаленной диагностики:
 - **Остановить приложение.**
 - **Перезапустить приложение.**
 - **Запустить приложение.**

В зависимости от выбранного вами действия приложение запустится, остановится или перезапустится.

Устройства с защитой на уровне UEFI

Устройство с защитой на уровне UEFI – это устройство со встроенным на уровне BIOS решением или приложением "Лаборатории Касперского" для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска приложения безопасности. Kaspersky Security Center поддерживает управление такими устройствами.

► Чтобы изменить параметры подключения устройств с защитой на уровне UEFI:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Параметры подключения к Серверу → Дополнительные порты**.
4. В разделе **Дополнительные порты** измените необходимые вам параметры:
 - **Открыть порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

Если флажок установлен, то устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

По умолчанию флажок установлен.
 - **Порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию используется порт 13294.
5. Нажмите на кнопку **ОК**.

Параметры управляемого устройства

► Чтобы просмотреть параметры управляемого устройства:

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки выберите устройство.
3. В контекстном меню устройства выберите пункт **Свойства**.

Откроется окно свойств устройства с выбранным разделом **Общие**.

Общие

Раздел **Общие** содержит общую информацию о клиентском устройстве. Информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского устройства с Сервером администрирования:

- **Название**
В поле можно просмотреть и изменить имя клиентского устройства в группе администрирования.
- **Описание**
В поле можно ввести дополнительное описание клиентского устройства.
- **Windows-домен**
Windows-домен или рабочая группа, в которую входит устройство.
- **NetBIOS-имя**
Имя клиентского устройства в сети Windows.
- **DNS-имя**
Имя DNS-домена устройства.
- **IP-адрес**
IP-адрес устройства.
- **Группа**
Группа администрирования, в состав которой входит клиентское устройство.
- **Последнее обновление**
Дата последнего обновления баз или приложений на устройстве.
- **Последнее появление в сети**
Дата и время, когда устройство последний раз было видимо в сети.
- **Соединение с Сервером администрирования**
Дата и время последнего соединения Агента администрирования, установленного на клиентском устройстве, с Сервером администрирования.
- **Не разрывать соединение с Сервером администрирования**
Если флажок установлен, поддерживается непрерывное соединение между Сервером администрирования и клиентским устройством.
Если флажок снят, клиентское устройство подключается к Серверу администрирования для синхронизации данных или передачи информации.

По умолчанию флажок установлен, если на устройстве установлен Сервер администрирования.

Если на устройстве установлен только Агент администрирования, по умолчанию флажок снят.

Защита

В разделе **Защита** представлена информация о состоянии антивирусной защиты на клиентском устройстве:

- **Статус устройства**

Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на устройстве и активности устройства в сети.

- **Все проблемы**

Эта таблица содержит полный список проблем, обнаруженных управляемыми приложениями, установленных на клиентском устройстве. Каждая проблема имеет статус, который управляемое приложение предлагает вам назначить устройству из-за этой проблемы.

- **Постоянная защита**

Статус текущего состояния постоянной защиты клиентского устройства.

- **Последняя проверка по требованию**

Дата и время последнего поиска вирусов на клиентском устройстве.

- **Всего обнаружено угроз**

Общее количество обнаруженных на клиентском устройстве вирусов (счетчик обнаруженных вирусов) со времени установки приложения защиты (первой проверки устройства), либо со времени последнего обнуления значения этой величины.

- **Активные угрозы**

Количество необработанных файлов на клиентском устройстве.

В поле не учитывается количество необработанных файлов для мобильных устройств.

- **Статус шифрования дисков**

Текущее состояние шифрования файлов на локальных дисках устройства.

Приложения

В разделе **Приложения** отображается список приложений "Лаборатории Касперского", установленных на клиентском устройстве:

- **События**

При нажатии на кнопку можно просмотреть список событий, произошедших на клиентском устройстве при работе приложения, а также результаты выполнения задач для этого приложения.

- **Статистика**

При нажатии на кнопку можно просмотреть текущую статистическую информацию о работе приложения.

- **Свойства**

При нажатии на кнопку можно получить информацию о приложении и выполнить настройку приложения.

Задачи

В разделе **Задачи** можно управлять задачами клиентского устройства: просматривать список существующих, создавать новые, удалять, запускать и останавливать задачи, изменять их параметры, просматривать результаты выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером администрирования. Информация о статусе задач запрашивается Сервером администрирования с клиентского устройства. В случае отсутствия связи статус не отображается.

События

В разделе **События** отображаются события, зарегистрированные на Сервере администрирования для выбранного клиентского устройства.

Теги

В разделе **Теги** можно управлять списком ключевых слов, на основании которых выполняется поиск клиентского устройства: просматривать список существующих тегов, назначать теги из списка, настраивать правила автоматического назначения тегов, добавлять новые и переименовывать старые теги, удалять теги.

Информация о системе

В разделе **Общая информация о системе** представлена информация о приложении, установленной на клиентском устройстве.

Реестр приложений

В разделе **Реестр приложений** можно просмотреть реестр установленных на клиентском устройстве приложений и обновлений для них, а также настроить отображение реестра приложений.

Информация об установленных приложениях предоставляется в том случае, если установленный на клиентском устройстве Агент администрирования передает необходимую информацию на Сервер администрирования. Параметры передачи информации на Сервер администрирования можно настроить в окне свойств Агента администрирования или его политики в разделе **Хранилища**.

Агент администрирования предоставляет информацию о приложениях на основе данных системного реестра.

- **Показывать только несовместимые приложения безопасности**

Если флажок установлен, в списке приложений отображаются только те приложения безопасности, которые несовместимы с приложениями "Лаборатории Касперского".

По умолчанию флажок снят.

- **Показывать обновления**

Если флажок установлен, в списке приложений отображаются не только приложения, но и установленные для них пакеты обновлений.

По умолчанию флажок снят.

- **Экспортировать в файл**

Нажмите эту кнопку, чтобы экспортировать список приложений, установленных на устройстве, в файл формата CSV или TXT.

- **История**

Нажмите эту кнопку, чтобы просмотреть события, относящиеся к установке приложений на устройство. Отобразится следующая информация:

- дата и время, когда приложение было установлено на устройство;
- название приложения;
- Версия приложения.

- **Свойства**

Нажмите эту кнопку, чтобы просмотреть свойства приложения, выбранного в списке приложений, установленных на устройстве. Отобразится следующая информация:

- название приложения;
- версия приложения;
- поставщик приложения.

Исполняемые файлы

В разделе **Исполняемые файлы** отображаются исполняемые файлы, обнаруженные на клиентском устройстве.

Реестр оборудования

В этом разделе можно просмотреть информацию об оборудовании, установленном на клиентском устройстве.

Сеансы

В разделе **Сеансы** представлена информация о владельце клиентского устройства, а также об учетных записях пользователей, которые работали с выбранным клиентским устройством.

Информация о доменных пользователях формируется на основе данных Active Directory. Информация о локальных пользователях предоставляется Диспетчером учетных записей безопасности (Security Account Manager), установленным на клиентском устройстве.

- **Владелец устройства**

В поле **Владелец устройства** отображается имя пользователя, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с клиентским устройством.

По кнопкам **Назначить** и **Свойства** можно выбрать владельца устройства и просмотреть информацию о пользователе, назначенном владельцем устройства.

По кнопке с красным крестом можно удалить текущего владельца устройства.

В списке содержатся учетные записи пользователей, которые работают с клиентским устройством.

- **Имя**

Имя устройства в сети.

- **Имя участника**

Имя пользователя (доменное или локальное), который выполнил вход в систему на этом устройстве.

- **Учетная запись**

Учетная запись пользователя, который выполнил вход в систему на этом устройстве.

- **Электронная почта**

Адрес электронной почты пользователя.

- **Телефон**

Номер телефона пользователя.

Проблемы безопасности

В разделе **Инциденты** можно просматривать, редактировать и создавать инциденты для клиентского устройства. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором. Например, если пользователь постоянно переносит на устройство вредоносные приложения с личного съемного диска, администратор может создать по этому поводу инцидент. В тексте инцидента администратор может кратко описать ситуацию и рекомендуемые действия, например, административные меры в отношении пользователя, а также добавить ссылку на пользователя.

Инцидент, для которого выполнены необходимые действия, называется обработанным. Наличие необработанных инцидентов может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

В разделе содержится список инцидентов, созданных для устройства. Инциденты классифицируются по уровню важности и типу. Тип инцидента определяется приложением "Лаборатории Касперского", которое создает инцидент. Обработанные инциденты можно отметить в списке, установив флажок в графе **Обработан**.

Уязвимости в приложениях

В разделе **Уязвимости в приложениях** можно просмотреть список с информацией об уязвимостях сторонних приложений, установленных на клиентских устройствах. С помощью строки поиска над списком вы можете искать в списке уязвимости по имени уязвимости.

- **Экспортировать в файл**

По кнопке **Экспортировать в файл** вы можете сохранить список уязвимостей в файле. По умолчанию приложение экспортирует список уязвимостей в файл формата CSV.

- **Показывать только те уязвимости, которые можно закрыть**

Если флажок установлен, в разделе отображаются уязвимости, которые можно закрыть патчем.

Если флажок снят, в разделе отображаются и уязвимости, которые можно закрыть патчем, и уязвимости, для которых патч отсутствует.

По умолчанию флажок установлен.

- **Свойства**

Выберите уязвимость в приложениях в списке и нажмите на кнопку **Свойства**,

чтобы просмотреть свойства выбранной уязвимости в приложениях в отдельном окне. В окне свойств можно выполнить следующие действия:

- Пропустить уязвимость в приложениях на этом управляемом устройстве (в Консоли администрирования (см. раздел "Игнорирование уязвимостей в приложениях" на стр. [565](#)) или в Kaspersky Security Center Web Console (см. раздел "Параметры управляемого устройства" на стр. [782](#))).
- Просмотреть список рекомендуемых исправлений для уязвимости.
- Вручную указать обновления программного обеспечения для закрытия уязвимости (в Консоли администрирования (см. раздел "Пользовательские исправления для уязвимостей в приложениях сторонних производителей" на стр. [566](#)) или в Kaspersky Security Center Web Console).
- Просмотреть экземпляр уязвимости.
- Просмотреть список существующих задач для закрытия уязвимости и создать задачи для закрытия уязвимости.

Неустановленные обновления

В этом разделе можно просмотреть список обнаруженных на устройстве обновлений программного обеспечения, которые не были установлены.

- **Показывать установленные обновления**

Если флажок установлен, в списке обновлений отображаются и не установленные обновления, и обновления, которые уже установлены на клиентском устройстве.

По умолчанию флажок снят.

Активные политики

В этом разделе отображается список политик для приложений "Лаборатории Касперского", активных на устройстве в настоящее время.

- **Экспортировать в файл**

По кнопке **Экспортировать в файл** вы можете сохранить список активных политик в файле. По умолчанию приложение экспортирует список политик в файл формата CSV.

Действующие профили политик

- **Действующие профили политик**

В списке можно просмотреть информацию о действующих профилях политики, которые активны на клиентских устройствах. С помощью строки поиска над списком вы можете искать в списке действующие профили политик по имени политики или по имени профиля политики.

- **Экспортировать в файл**

Точки распространения

В этом разделе представлен список агентов обновлений, с которыми взаимодействует устройство.

- **Экспортировать в файл**

По кнопке **Экспортировать в файл** вы можете сохранить в файле список агентов обновлений, с которыми взаимодействует устройство. По умолчанию приложение экспортирует список устройств в файл формата CSV.

- **Свойства**

По кнопке **Свойства** вы можете посмотреть и настроить параметры агента обновлений, с которым взаимодействует устройство.

См. также:

Настройка общих параметров Сервера администрирования [716](#)

Общие параметры политик

Общие

В разделе **Общие** можно изменить состояние политики и настроить наследование параметров политики.

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:

- **Активная политика**

Если выбран этот вариант, политика становится активной.

По умолчанию выбран этот вариант.

- **Политика для автономных пользователей**

Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации. Политика для автономных пользователей доступна только для Антивируса Касперского для Windows Workstations версии 6.0 MP3 и выше.

- **Неактивная политика**

Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

- В блоке **Наследование параметров** можно настроить параметры наследования политики:

- **Наследовать параметры родительской политики**

Если флажок установлен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

По умолчанию флажок установлен.

- **Обеспечить принудительное наследование параметров для дочерних политик**

Если флажок установлен, после применения изменений в политике будут выполнены следующие действия:

- значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
 - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически установлен флажок **Наследовать параметры политики верхнего уровня**.

Когда флажок установлен, значения параметров дочерних политик недоступны для изменения.

По умолчанию флажок снят.

Настройка событий

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на вкладках:

- **Отказ функционирования.**
- **Предупреждение.**
- **Информационное сообщение.**

В списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). По кнопке **Свойства** можно настроить параметры регистрации и уведомления о событиях, выбранных в списке.

Для выбора нескольких типов событий используйте клавиши **SHIFT** или **CTRL**, для выбора всех типов используйте кнопку **Выбрать все**.

См. также:

Контроль возникновения вирусных эпидемий [718](#)

Параметры политики Агента администрирования

► *Чтобы настроить параметры политики Агента администрирования:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки выберите политику Агента администрирования.
3. В контекстном меню политики выберите пункт **Свойства**.

Откроется окно свойств политики Агента администрирования.

Общие

В разделе **Общие** можно изменить состояние политики и настроить наследование параметров политики.

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
 - **Активная политика**
Если выбран этот вариант, политика становится активной.
По умолчанию выбран этот вариант.
 - **Политика для автономных пользователей**
Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации. Политика для автономных пользователей доступна только для Антивируса Касперского для Windows Workstations версии 6.0 MP3 и выше.
 - **Неактивная политика**
Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
 - **Наследовать параметры родительской политики**
Если флажок установлен, значения параметров политики наследуются из политики

для группы верхнего уровня иерархии и недоступны для изменения.

По умолчанию флажок установлен.

- **Обеспечить принудительное наследование параметров для дочерних политик**

Если флажок установлен, после применения изменений в политике будут выполнены следующие действия:

- значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
- в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически установлен флажок **Наследовать параметры политики верхнего уровня**.

Когда флажок установлен, значения параметров дочерних политик недоступны для изменения.

По умолчанию флажок снят.

Настройка событий

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на вкладках:

- **Отказ функционирования.**
- **Предупреждение.**
- **Информационное сообщение.**

В списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). По кнопке **Свойства** можно настроить параметры регистрации и уведомления о событиях, выбранных в списке.

Для выбора нескольких типов событий используйте клавиши **SHIFT** или **CTRL**, для выбора всех типов используйте кнопку **Выбрать все**.

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Распространять файлы только через точки распространения**

Если флажок установлен, клиентские устройства получают обновления только через агенты обновлений, а не напрямую с серверов обновлений.

Если флажок снят, клиентские устройства могут получать обновления из разных источников: напрямую с серверов обновлений, от главного Сервера администрирования, из локальной или сетевой папки.

По умолчанию флажок снят.

- **Максимальный размер очереди событий (МБ)**

В поле можно указать максимальное место на диске, которое может занимать очередь событий.

По умолчанию указано значение 2 МБ.

- **Приложение может получать расширенные данные политики на устройстве**

Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в приложение безопасности (например, Kaspersky Endpoint Security для Windows). Передаваемая информация

отображается в интерфейсе приложения безопасности.

Агент администрирования передает следующую информацию:

- время доставки политики на управляемое устройство;
- имя активной политики и политики для автономных пользователей в момент доставки политики на управляемое устройство;
- имя и полный путь группы администрирования, которой принадлежит управляемое устройство на момент доставки политики на управляемое устройство;
- список активных профилей политики.

Вы можете использовать эту информацию, чтобы обеспечить применение правильной политики к устройству и в целях устранения неполадок. По умолчанию параметр выключен.

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

Если этот параметр включен, после того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

По умолчанию параметр выключен.

- **Использовать пароль деинсталляции**

Если флажок установлен, при нажатии на кнопку **Изменить** можно указать пароль для задачи удаленной деинсталляции Агента администрирования.

По умолчанию флажок снят.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, параметры недоступны для изменения.

- **Информация об обновлениях Центра обновления Windows**

Если флажок установлен, на Сервер администрирования отправляется информация об обновлениях Microsoft Windows, которые необходимо установить на клиентских устройствах.

По умолчанию флажок установлен.

- **Информация об уязвимостях в приложениях и соответствующих обновлениях**

Если флажок установлен, на Сервер администрирования отправляется информация об уязвимостях программного обеспечения, обнаруженных на клиентских устройствах.

По умолчанию флажок установлен.

- **Информация о реестре оборудования**

Если флажок установлен, на Сервер администрирования отправляется информация об оборудовании, обнаруженном в результате опроса сети.

По умолчанию флажок установлен.

- **Информация об установленных приложениях**

Если флажок установлен, на Сервер администрирования отправляется информация о приложениях, установленных на клиентских устройствах.

По умолчанию флажок установлен.

- **Включить информацию о патчах**

Информация о патчах приложений, установленных на клиентских устройствах, отправляется на Сервер администрирования. Включение этого параметра может увеличить нагрузку на Сервер администрирования и СУБД, а также вызвать увеличение объема базы данных.

По умолчанию параметр включен. Доступен только для Windows.

Обновления и уязвимости в приложениях

В разделе **Обновления и уязвимости в приложениях** можно настроить поиск и распространение обновлений Windows, а также включить проверку исполняемых файлов на наличие уязвимостей:

- **Использовать Сервер администрирования в роли WSUS-сервера**

Если флажок установлен, обновления Windows загружаются на Сервер администрирования. Загруженные обновления Сервер администрирования централизованно предоставляет службам Windows Update на клиентских устройствах с помощью Агентов администрирования.

Если флажок снят, Сервер администрирования не используется для загрузки обновлений Windows. В этом случае клиентские устройства получают обновления Windows самостоятельно.

По умолчанию флажок снят.

- С помощью параметра **Разрешить пользователям управлять установкой обновлений Центра обновления Windows** вы можете ограничить обновления Windows, которые пользователи могут устанавливать на своих устройствах вручную, с помощью Центра обновления Windows.

Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, то новый параметр, который вы выбрали под **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

Выберите параметр из раскрывающегося списка:

- **Устанавливать все применимые обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

Выберите этот вариант, если вы не хотите влиять на установку обновлений.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Устанавливать только одобренные обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Запретить устанавливать обновления Центра обновления Windows**

Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

- В блоке параметров **Режим поиска обновлений Windows Update** можно выбрать режим поиска обновлений:

- **Активный**

Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от агента обновлений Windows.

По умолчанию выбран этот вариант.

- **Пассивный**

Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при последней синхронизации агента обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.

- **Выключен**

Если выбран этот вариант, Сервер администрирования не запрашивает информацию об обновлениях.

- **Проверять исполняемые файлы на наличие уязвимостей при запуске**

Если флажок установлен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

По умолчанию флажок установлен.

Управление перезагрузкой

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если в ходе работы, установки или удаления приложения требуется перезагрузка операционной системы:

- **Не перезагружать операционную систему**

Перезагрузка операционной системы не выполняется.

Этот вариант выбран по умолчанию.

- **При необходимости перезагрузить операционную систему автоматически**

При необходимости перезагрузка операционной системы выполняется автоматически.

- **Запрашивать у пользователя**

Приложение запрашивает у пользователя разрешение перезагрузить операционную систему.

- **Повторять запрос периодически через (мин)**

Если флажок установлен, приложение запрашивает у пользователя разрешение на перезагрузку операционной системы с периодичностью, указанной в поле рядом с флажком. По умолчанию периодичность повторных запросов составляет 5 минут.

Если флажок снят, приложение не запрашивает разрешение на перезагрузку повторно.

По умолчанию флажок установлен.

- **Принудительно перезагружать через (мин)**

Если флажок установлен, после запроса у пользователя операционная система перезагружается принудительно по истечении времени, указанного в поле рядом с флажком.

Если флажок снят, принудительная перезагрузка не выполняется.

По умолчанию флажок снят.

- **Время ожидания перед принудительным закрытием приложения в заблокированных сессиях через (мин)**

Принудительное завершение работы приложений, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

Если флажок установлен, работа приложений на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

Если флажок снят, работа приложений на заблокированном устройстве не прекращается.

По умолчанию флажок снят.

Совместный доступ к рабочему столу Windows

В разделе **Общий доступ к рабочему столу** можно включить и настроить аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу:

- **Включить аудит**

Если флажок установлен, аудит действий администратора на удаленном устройстве включен. Записи о действиях администратора на удаленном устройстве

сохраняются:

- в журнале событий на удаленном устройстве;
- в файле с расширением syslog, который находится в папке установки Агента администрирования на удаленном устройстве;
- в базе событий Kaspersky Security Center.

Аудит действий администратора доступен при выполнении следующих условий:

- есть в наличии действующая лицензия на Системное администрирование;
- у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

Если флажок снят, аудит действий администратора на удаленном устройстве выключен.

По умолчанию флажок снят.

- **Маски файлов, чтение которых нужно отслеживать**

В списке содержатся маски файлов. Когда аудит включен, приложение отслеживает чтение администратором файлов, соответствующих маскам, и сохраняет информацию о чтении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Маски файлов, изменение которых нужно отслеживать**

В списке содержатся маски файлов на удаленном устройстве. Когда аудит включен, приложение отслеживает изменение администратором файлов, соответствующих маскам, и сохраняет информацию об изменении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Управление патчами и обновлениями

В разделе **Управление патчами и обновлениями** можно настроить получение и распространение обновлений и установку патчей на управляемые устройства.

- **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**

Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Автоматическая установка патчей со статусом *Не определено* доступна для версий Kaspersky Security Center Service Pack 2 и выше.

Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того как администратор изменит их статус на *Одобен*.

По умолчанию флажок установлен.

- **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**

Если флажок установлен, включена офлайн-модель получения обновлений. В этом случае, когда Сервер администрирования получает обновления, он оповещает Агенты администрирования о том, какие обновления потребуются для приложения на клиентских устройствах. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загружает все обновления, обновления становятся доступными для приложений на клиентском устройстве.

Когда управляемое приложение на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемого приложения, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемому приложению обновления из локального кеша. Соединение с Сервером администрирования при этом может отсутствовать, но оно и не требуется для обновления.

Если флажок снят, офлайн-модель получения обновлений выключена. Обновления распределяются по расписанию задачи обновления.

По умолчанию флажок установлен.

Подключения

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**
- **Профили соединений** (только для Windows и macOS)
- **Расписание соединений**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер. Доступны следующие параметры:

- В блоке **Подключение к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования.
- **Сжимать сетевой трафик**

Если флажок установлен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

Нагрузка на центральный процессор клиентского компьютера может возрасти.

По умолчанию флажок установлен.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

Если флажок установлен, UDP-порт, необходимый для работы Агента администрирования, будет добавлен в список исключений сетевого экрана Microsoft Windows.

По умолчанию флажок установлен.

- **Использовать SSL**

Если флажок установлен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

По умолчанию флажок установлен.

- **Использовать шлюз соединения точки распространения (при наличии) в параметрах подключения по умолчанию**

Если флажок установлен, то используется шлюз соединений агента обновлений, параметры которого заданы в свойствах группы администрирования.

По умолчанию флажок установлен.

- **Использовать UDP-порт**

Чтобы управляемое устройство подключалось к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **Номер UDP-порта**

В поле можно ввести номер UDP-порта. По умолчанию используется порт 15000.

Используется десятичная форма записи.

Если клиентское устройство работает под управлением операционной системы Windows XP Service Pack 2, встроенный межсетевой экран блокирует UDP-порт с номером 15000. Этот порт требуется открыть вручную.

- **Использовать точку распространения для принудительного подключения к Серверу администрирования**

В разделе **Профили соединений** можно задать параметры сетевого местоположения, настроить профили подключения к Серверу администрирования, включить автономный режим, когда Сервер администрирования недоступен. Параметры раздела **Профили соединений** доступны только для устройств под управлением Windows и macOS:

- **Параметры сетевого местоположения**

Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети.

- **Профили подключения к Серверу администрирования**

В этом разделе можно просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

- подключении клиентского устройства к другой локальной сети;
- отключении устройства от локальной сети организации;
- изменении адреса шлюза соединения или изменении адреса DNS-сервера.
- **Включить автономный режим, когда Сервер администрирования недоступен**

Если флажок установлен, при подключении через этот профиль приложения, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных

пользователей (см. раздел "О переключении Агента администрирования на другой Сервер администрирования" на стр. [307](#)). В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

Если флажок снят, приложения будут использовать активные политики.

По умолчанию флажок снят.

В разделе **Менеджер соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

Этот вариант выбран по умолчанию.

- **Подключаться в указанные периоды**

Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Точки распространения

Раздел **Точки распространения** включает четыре вложенных раздела:

- **Опросы сети**
- **Параметры подключения к интернету**
- **Прокси-сервер KSN**
- **Обновления**

В подразделе **Опросы сети** вы можете настроить автоматический опрос сети. Вы можете включить три типа опроса, то есть опрос сети, опрос IP-диапазонов и опрос Active Directory:

- **Разрешить опрос сети**

Если флажок установлен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить период быстрого опроса** и **Настроить период полного опроса**.

Если флажок снят, Сервер администрирования не выполняет опрос сети.

Периодичность опроса сети для версий Агента администрирования версий ниже 10.2 можно настроить в полях **Период запроса информации с доменов, мин** и **Период опроса компьютерной сети, мин**. Поля доступны, если флажок установлен.

По умолчанию флажок установлен.

- **Разрешить опрос IP-диапазона**

Если флажок установлен, Сервер администрирования автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

Если флажок снят, Сервер администрирования не выполняет опрос IP-диапазонов.

Периодичность опроса IP-диапазонов для версий Агента администрирования

версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если флажок установлен.

По умолчанию флажок снят.

- **Использовать опрос Zeroconf (только для платформ Linux; указанные вручную IP-диапазоны игнорируются)**
- **Разрешить опрос Active Directory**

Если флажок установлен, Сервер администрирования автоматически выполняет опрос Active Directory в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

Если флажок снят, Сервер администрирования не выполняет опрос Active Directory.

Периодичность опроса Active Directory для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если флажок установлен.

По умолчанию флажок установлен.

В разделе **Параметры подключения к интернету** можно настроить параметры доступа к сети интернет:

- **Использовать прокси-сервер**

Если флажок установлен, в полях ввода можно настроить параметры подключения к прокси-серверу.

По умолчанию флажок снят.

- **Адрес прокси-сервера**

Адрес прокси-сервера.

- **Номер порта**

Номер порта, по которому будет выполняться подключение.

- **Не использовать прокси-сервер для локальных адресов**

Если флажок установлен, то при подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

По умолчанию флажок снят.

- **Аутентификация на прокси-сервере**

Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

По умолчанию флажок снят.

- **Имя пользователя**

Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

В разделе **Прокси-сервер KSN** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств:

- **Включить прокси-сервер KSN на стороне точки распространения**

Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены (см. раздел "Настройка доступа к KPSN" на стр. [874](#)) в окне свойств Сервера администрирования.

Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Пересылать KSN запрос Серверу администрирования**

Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

По умолчанию параметр включен.

- **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к KPSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения.

Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к KPSN.

- **TCP-порт**

Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **Использовать UDP-порт**

Чтобы управляемое устройство подключалось к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

В подразделе **Обновления** вы можете указать, должен ли Агент администрирования загружать файлы различий (см. раздел "Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"" см. стр. [467](#)), включив или выключив параметр **Загрузить файлы различий**. По умолчанию параметр включен.

История ревизий

В этом разделе можно посмотреть историю ревизий Агента администрирования (см. раздел "Работа с ревизиями объектов" на стр. [852](#)). Вы можете сравнивать ревизии, просматривать ревизии, сохранять ревизии в файл, добавлять и изменять описания ревизий.

Сравнение возможностей Агента администрирования по операционным системам

В таблице ниже показано, какие параметры политики Агента администрирования можно использовать для настройки Агента администрирования для конкретной операционной системы.

Таблица 71. Параметры политики Агента администрирования: сравнение по операционным системам

Раздел Политики	Windows	Mac	Linux
Общие	✓	✓	✓
Настройка событий	✓	✓	✓
Параметры	✓	✓	Доступны следующие параметры: • Распространять файлы только через точки распространения • Максимальный размер очереди событий (МБ) • Приложение может получать расширенные данные политики на устройстве
Хранилища	✓	—	Доступны следующие параметры: • Информация об установленных приложениях • Информация о реестре оборудования
Обновления и уязвимости в приложениях	✓	—	—
Управление перезагрузкой	✓	—	—
Совместный доступ к рабочему столу Windows	✓	—	—
Управление патчами и обновлениями	✓	—	—

Раздел Политики	Windows	Mac	Linux
Подключения → Сеть	✓	✓	✓ Кроме параметра Открывать порты Агента администрирования в брандмауэре Microsoft Windows.
Подключения → Профили соединений	✓	✓	—
Подключения → Расписание соединений	✓	✓	✓
Точки распространения → Опросы сети	✓	—	✓ Доступны следующие параметры: • Zeroconf • IP-диапазоны
Точки распространения → Параметры подключения к интернету	✓	✓	✓
Точки распространения → Прокси-сервер KSN	✓	—	✓
Точки распространения → Обновления	✓	—	✓
История ревизий	✓	✓	✓

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Управление учетными записями пользователей

Этот раздел содержит информацию об учетных записях и ролях пользователей, которые поддерживает приложение. В разделе приведены инструкции по созданию учетных записей и ролей пользователей Kaspersky Security Center.

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами учетных записей. Приложение поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих пользователей при опросе сети организации.
- Учетные записи внутренних пользователей (см. раздел "Работа с внутренними пользователями" на стр. [720](#)). Применяются для работы с виртуальными Серверами администрирования. Учетные записи внутренних пользователей создаются (см. раздел "Добавление учетной записи внутреннего пользователя" на стр. [804](#)) и используются только внутри Kaspersky Security Center.

В этом разделе

Работа с учетными записями пользователей	803
Добавление учетной записи внутреннего пользователя	804
Изменение учетной записи внутреннего пользователя	806
Изменение количества попыток ввода пароля	807
Настройка проверки уникальности имени внутреннего пользователя	807
Добавление группы безопасности	808
Добавление пользователя в группу	809
Настройка прав. Пользовательские роли	809
Назначение пользователя владельцем устройства	841
Рассылка сообщений пользователям	842
Просмотр списка мобильных устройств пользователя	842
Установка сертификата пользователю	842
Просмотр списка сертификатов, выписанных пользователю	843
Об администраторе виртуального Сервера	843

Работа с учетными записями пользователей

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами учетных записей. Приложение поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих пользователей при опросе сети организации.
- Учетные записи внутренних пользователей (см. раздел "Работа с внутренними пользователями" на стр. [720](#)). Применяются для работы с виртуальными Серверами администрирования. Учетные

записи внутренних пользователей создаются (см. раздел "Добавление учетной записи внутреннего пользователя" на стр. [804](#)) и используются только внутри Kaspersky Security Center.

Вы можете просмотреть список учетных записей пользователей одним из следующих способов:

- В дереве консоли перейдите в раздел **Дополнительно** → **Учетные записи пользователей**.
- В дереве консоли перейдите в папку **Управляемые устройства** → вкладка **Устройства** → ссылка <название устройства> → раздел **Сеансы**.

В разделе **Сеансы** отображаются учетные записи пользователей с активными сеансами на устройствах под управлением Windows.

Список учетных записей пользователей отображается правильно, если выполнены следующие требования:

- Используется Агент администрирования той же версии, что и Сервер администрирования, или выше.
- Опрос Active Directory включен (см. раздел "Опрос Active Directory" на стр. [328](#)) для отображения учетных записей пользователей домена.
- На управляемых устройствах под управлением Windows работает служба **Сервера (LanmanServer)**.

Вы можете выполнять с учетными записями пользователей и группами учетных записей следующие действия:

- настраивать права доступа пользователей к функциям приложения с помощью ролей (см. раздел "Настройка прав. Пользовательские роли" на стр. [809](#));
- рассылать сообщения пользователям с помощью электронной почты и SMS (см. раздел "Рассылка сообщений пользователям" на стр. [842](#));
- просматривать список мобильных устройств пользователя (см. раздел "Просмотр списка мобильных устройств пользователя" на стр. [842](#));
- выписывать и устанавливать сертификаты на мобильные устройства пользователя (см. раздел "Установка сертификата пользователю" на стр. [842](#));
- просматривать список сертификатов, выписанных пользователю (см. раздел "Просмотр списка сертификатов, выписанных пользователю" на стр. [843](#));
- выключать двухэтапную проверку (см. раздел "Выключение двухэтапной проверки для учетной записи пользователя" на стр. [739](#)) для учетной записи пользователя.

Добавление учетной записи внутреннего пользователя

► Чтобы добавить новую учетную запись пользователя Kaspersky Security Center:

1. В дереве консоли откройте папку **Учетные записи пользователей**.
Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В рабочей области нажмите на кнопку **Добавить пользователя**.
3. В открывшемся окне **Новый пользователь** укажите параметры нового пользователя:

- Имя пользователя ().

Пожалуйста, будьте внимательны при вводе имени пользователя. Вы не сможете его изменить после сохранения изменений.

- **Описание**
- **Полное имя**
- **Основная электронная почта**
- **Основной телефон**
- **Пароль** для подключения пользователя к Kaspersky Security Center.

Пароль должен соответствовать следующим правилам:

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп списка ниже:
 - верхний регистр (A-Z);
 - нижний регистр (A-Z) (a-z);
 - числа (0-9);
 - специальные символы (@ # \$ % ^ & * - _ ! + = [] { } | : ' , . ? / \ ` ~ " () ;)
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля (см. стр. 807)".
Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. В списке учетных записей пользователей значок



заблокированной учетной записи затемнен (недоступен). Вы можете разблокировать учетную запись, только сменив пароль.

- При необходимости установите флажок **Отключить учетную запись**, чтобы запретить пользователю подключаться к приложению. Например, можно отключить учетную запись, если вы хотите создать учетную запись заранее, но активировать ее позже.
- Установите флажок **Запрашивать пароль при изменении параметров учетной записи**, если вы хотите включить дополнительную защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, то для изменения параметров учетной записи пользователя требуется авторизация пользователя с правом Изменение списков управления доступом объектов (см. раздел "Права доступа к функциям приложения" на стр. 810) в области **Общий функционал: Права пользователей**.

4. Нажмите на кнопку **ОК**.

Созданная учетная запись пользователя отобразится в рабочей области папки **Учетные записи пользователей**.

Изменение учетной записи внутреннего пользователя

► Чтобы изменить учетную запись внутреннего пользователя Kaspersky Security Center:

1. В дереве консоли откройте папку **Учетные записи пользователей**.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В рабочей области дважды щелкните учетную запись внутреннего пользователя, которую требуется изменить.
3. В открывшемся окне **Свойства: <имя пользователя>** измените параметры учетной записи пользователя:

- **Описание**
- **Полное имя**
- **Основная электронная почта**
- **Основной телефон**
- **Пароль** для подключения пользователя к Kaspersky Security Center.

Пароль должен соответствовать следующим правилам:

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп списка ниже:
 - верхний регистр (A-Z);
 - нижний регистр (A-Z) (a-z);
 - числа (0-9);
 - специальные символы (@ # \$ % ^ & * - _ ! + = [] { } | : ' , . ? / \ ` ~ " () ;)
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля (см. стр. 807)".

Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. В списке учетных записей пользователей значок



заблокированной учетной записи затемнен (недоступен). Вы можете разблокировать учетную запись, только сменив пароль.

- При необходимости установите флажок **Отключить учетную запись**, чтобы запретить пользователю подключаться к приложению. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.
- Выберите параметр **Запрашивать пароль при изменении параметров учетной записи**, если вы хотите включить дополнительную защиту учетной записи пользователя от

несанкционированного изменения. Если этот параметр включен, то для изменения параметров учетной записи пользователя требуется авторизация пользователя с правом Изменение списков управления доступом объектов (см. раздел "Права доступа к функциям приложения" на стр. [810](#)) в области **Общий функционал: Права пользователей**.

4. Нажмите на кнопку **ОК**.

Измененная учетная запись пользователя отобразится в рабочей области папки **Учетные записи пользователей**.

Изменение количества попыток ввода пароля

Пользователь Kaspersky Security Center может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить количество попыток ввода пароля, следуя инструкции ниже.

► *Чтобы изменить количество попыток ввода пароля, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите к следующему разделу:
 - для 32-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
 - для 64-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
3. Если параметр SrvSpIPpcLogonAttempts отсутствует в разделе реестра, создайте его. Тип значения параметра – DWORD.
Этот параметр не создается по умолчанию при установке Kaspersky Security Center.
4. Укажите требуемое количество попыток в качестве значения параметра SrvSpIPpcLogonAttempts.
5. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
6. Перезапустите службу Сервера администрирования.

Максимальное количество попыток ввода пароля изменено.

Настройка проверки уникальности имени внутреннего пользователя

Вы можете настроить проверку уникальности имени внутреннего пользователя Kaspersky Security Center при его добавлении в приложение. Проверка на уникальность имени внутреннего пользователя может выполняться только на виртуальном Сервере или главном Сервере, для которого создается учетная запись пользователя, или на всех виртуальных Серверах и главном Сервере. По умолчанию проверка на уникальность имени внутреннего пользователя выполняется на всех виртуальных Серверах и на главном Сервере администрирования.

► *Чтобы включить проверку уникальности имени внутреннего пользователя в рамках виртуального Сервера или главного Сервера:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
 - для 32-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\core\independent\KLLIM
 - для 64-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\core\independent\KLLIM
3. Для ключа LP_InterUserUniqVsScope (DWORD) установите значение 00000001.
По умолчанию для этого ключа указано значение 0.
4. Перезапустите службу Сервера администрирования.

В результате проверка уникальности имени будет выполнена только на том виртуальном Сервере, на котором был создан внутренний пользователь, или на главном Сервере, если пользователь был создан на главном Сервере.

► *Чтобы включить проверку уникальности имени внутреннего пользователя на всех виртуальных Серверах и главном Сервере:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
 - для 64-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\core\independent\KLLIM
 - для 32-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\core\independent\KLLIM
3. Для ключа LP_InterUserUniqVsScope (DWORD) установите значение 00000000.
По умолчанию для этого ключа указано значение 0.
4. Перезапустите службу Сервера администрирования.

В результате проверка уникальности имени будет выполнена на всех виртуальных Серверах и на главном Сервере администрирования.

Добавление группы безопасности

Вы можете добавлять группы безопасности (группы пользователей), гибко настраивать состав групп и доступ группы безопасности к разным функциям приложения. Группам безопасности можно давать названия, соответствующие их назначению. Например, название может соответствовать расположению пользователей в офисе или названию структурного подразделения компании, к которому относятся пользователи.

Один пользователь может входить в состав нескольких групп безопасности. Учетная запись пользователя под управлением виртуального Сервера администрирования может входить только в группы безопасности этого виртуального Сервера и иметь права доступа только в рамках этого виртуального Сервера.

► *Чтобы добавить группу безопасности:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. Нажмите на кнопку **Добавить группу безопасности**.

Откроется окно **Добавить группу безопасности**.

3. В окне **Добавить группу безопасности** в разделе **Общие** укажите имя группы.

Имя группы не может превышать 255 символов и не может содержать символы *, <, >, ?, \, :, |. Имя группы должно быть уникальным.

Вы можете ввести описание группы в поле ввода **Описание**. Заполнение поля **Описание** не является обязательным.

4. Нажмите на кнопку **ОК**.

Добавленная группа безопасности отобразится в папке **Учетные записи пользователей** в дереве консоли. Вы можете добавить пользователей (см. раздел "Добавление пользователя в группу" на стр. [809](#)) в созданную группу.

Добавление пользователя в группу

► *Чтобы добавить пользователя в группу:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В списке учетных записей пользователей и групп выберите группу, в которую нужно добавить пользователя.

3. В окне свойств группы выберите раздел **Пользователи группы**, затем нажмите на кнопку **Добавить**.

В результате откроется окно со списком пользователей.

4. В списке выберите пользователя или пользователей, которых нужно включить в состав группы.

5. Нажмите на кнопку **ОК**.

Пользователь добавлен в группу и отображается в списке пользователей группы.

Настройка прав. Пользовательские роли

Вы можете гибко настраивать доступ к различным функциям приложения администраторам, пользователям и группам пользователей. Вы можете предоставить пользователям права доступа к функциям приложения одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

Пользовательская роль представляет собой специально созданный и предопределенный набор прав доступа к функциям приложения. Роль может быть предоставлена пользователю или группе пользователей. Применение ролей упрощает и сокращает рутинные действия по настройке прав доступа пользователей к приложению. Права доступа в роли настраивают в соответствии с типовыми задачами и служебными обязанностями пользователей. Например, роль пользователя может иметь права только на чтение и отправку информационных команд на мобильные устройства других пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В приложении можно создавать неограниченное количество ролей.

Вы можете настроить доступ к различным функциям приложения для следующих объектов:

- Серверы администрирования.
- Группы администрирования.
- Виртуальные Серверы администрирования.

В этом разделе

Права доступа к функциям приложения	810
Предопределенные роли пользователей	832
Добавление роли пользователя	837
Назначение роли пользователю или группе безопасности	838
Назначение прав пользователям или группам пользователей	838
Распространение пользовательских ролей на подчиненные Серверы администрирования	840

Права доступа к функциям приложения

В таблице ниже приведены функции Kaspersky Security Center с правами доступа для управления задачами, отчетами, параметрами и для выполнения действий пользователя.

Для выполнения действий пользователя, перечисленных в таблице, у пользователя должно быть право, указанное рядом с действием.

Права на **Чтение**, **Запись** и **Выполнение** применимы к любой задаче, отчету или параметрам. В дополнение к этим правам у пользователя должно быть право **Выполнение операций с выборками устройств** для управления задачами, отчетами или изменения параметров выборок устройств.

Все задачи, отчеты, параметры и инсталляционные пакеты, отсутствующие в таблице, относятся к области **Общие функции: Базовая функциональность**.

Таблица 72. Права доступа к функциям приложения

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Управление группами администрирования	Запись.	- Добавление устройства в группу администрирования: Запись. - Удаление устройства из состава группы администрирования: Запись. - Добавление группы администрирования в другую группу администрирования: Запись. - Удаление группы администрирования из другой группы администрирования: Запись.	Отсутствует.	Отсутствует.	Отсутствует.
Общие функции: Доступ к объектам независимо от их списков ACL	Чтение.	Получение доступа на чтение ко всем объектам: Чтение.	Отсутствует.	Отсутствует.	Отсутствует.

Общие функции: Базовая функциональность	• Чтение. • Запись. • Выполнение. • Выполнение действий над выборками и устройств.	• Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: Запись, Выполнение действий над выборками и устройств. • Получение мобильного протокола пользователя сертификата (LWNGT): Чтение. • Установка мобильного протокола пользователя сертификата (LWNGT): Запись. • Получить список сетей, определенных NLA: Чтение. • Добавить, изменить или удалить список сетей, определенных NLA: Запись. • Просмотр списка контроля	• Загрузка обновлений в хранилище Сервера администрирования. • Рассылка отчетов. • Распространение инсталляционных пакетов. • Установка приложений на подчиненные Серверы администрирования.	• Отчет о состоянии защиты. • Отчет об угрозах. • Отчет о наиболее зараженных устройствах. • Отчет о статусе антивирусных баз. • Отчет об ошибках. • Отчет о сетевых атаках. • Сводный отчет о приложениях для защиты почтовых систем. • Сводный отчет о приложениях для защиты периметра. • Сводный отчет о типах установленных приложений. • Отчет о пользователях зараженных устройств. • Отчет об инцидентах. • Отчет о событиях.	Отсутствует.

		доступа групп: Чтение. Просмотрите журнал событий Kaspersky Event Log: Чтение.		- Отчет о работе точек распространения. - Отчет о подчиненных Серверах администрирования. - Отчет о событиях Контроля устройств. - Отчет об уязвимостях. - Отчет о запрещенных приложениях. - Отчет о работе Веб-Контроля. - Отчет о статусе шифрования управляемых устройств. - Отчет о статусе шифрования запоминающих устройств. - Отчет об ошибках шифрования файлов. - Отчет о блокировании доступа к зашифрованным файлам.	

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
				• Отчет о правах доступа к зашифрованным устройствам. • Отчет об эффективных правах пользователя. • Отчет о правах.	
Общие функции: Удаленные объекты	• Чтение. • Запись.	• Просмотр удаленных объектов в корзине: Чтение. • Удаление объектов из корзины: Запись.	Отсутствует.	Отсутствует.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Обработка событий	- Удаление событий. - Изменение параметра в уведомлении о событиях. - Изменение параметра в записи событий в журнал событий. - Запись.	- Изменение параметра в регистрации и событий: Изменение параметра в записи событий в журнал событий. - Изменение параметра в уведомлении о событиях: Изменение параметра в уведомлении о событиях. - Удаление событий: Удаление событий.	Отсутствует.	Отсутствует.	Параметры: - Параметры вирусной атаки: количество обнаружений вирусов, необходимое для создания события вирусной атаки. - Параметры вирусной атаки: период для оценки обнаружения вирусов. - Максимальное количество событий, хранящихся в базе данных. - Период хранения событий удаленных устройств.

Общие функции: Операции с Сервером администрирования	• Чтение. • Запись. • Выполнение. • Изменение списков ACL объекта. • Выполнение действий над выборкам и устройств.	• Изменение портов Сервера администрирования для подключения Агента администрирования: Запись. • Изменение портов прокси-сервера активации, запущенного на Сервере администрирования: Запись. • Изменение портов прокси-сервера активации для мобильных устройств, запускаемых на Сервере администрирования: Запись. • Изменение портов Веб-сервера для распространения автономных пакетов: Запись. • Изменение портов Веб-сервера для распространения iOS	• Резервное копирование данных Сервера администрирования. • Обслуживание базы данных.	Отсутствует.	Отсутствует.

		MDM-профилей: Запись. • Изменение SSL-портов Сервера администрирования для подключения с помощью Kaspersky Security Center Web Console: Запись. • Изменение портов Сервера администрирования для подключения мобильных устройств: Запись. • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования: Запись. • Укажите максимальное количество событий, которое может отправлять Сервер администрирования: Запись.			

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
		Изменение периода, в течение которого Сервер администрирования может отправлять события: Запись.			

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Развертывание приложений "Лаборатории Касперского"	- Управление патчами "Лаборатории Касперского". - Чтение. - Запись. - Выполнение. - Выполнение действий над выборками устройств.	Одобрить или отклонить установку патча: Управление патчами "Лаборатории Касперского".	Отсутствует.	- Отчет об использовании лицензионных ключей виртуальным Сервером администрирования. - Отчет о версиях приложений "Лаборатории Касперского". - Отчет о несовместимых приложениях. - Отчет о версиях обновлений модулей приложений "Лаборатории Касперского". - Отчет о развертывании защиты.	Инсталляционный пакет: "Приложения Лаборатории Касперского"

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Управление лицензионными ключами	• Экспорт файл ключа. • Запись.	• Экспорт файл ключа: Экспорт файл ключа. • Изменение параметра в лицензионного ключа Сервера администрирования: Запись.	Отсутствует.	Отсутствует.	Отсутствует.
Общие функции: Управление отчетами	• Чтение. • Запись.	• Создание отчетов для объектов независимо от их списков ACL: Запись. • Выполнять отчеты независимо от их списков ACLs: Чтение.	Отсутствует.	Отсутствует.	Отсутствует.
Общие функции: Иерархия Серверов администрирования	Настройка иерархии Серверов администрирования	Добавление, обновление или удаление подчиненных Серверов администрирования: Настройка иерархии Серверов администрирования.	Отсутствует.	Отсутствует.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Права пользователя	Изменение списков ACL объекта.	- Изменение свойств Безопасности любого объекта: Изменение списков ACL объекта. - Управление ролями пользователей: Изменение списков ACL объекта. - Управление внутренними пользователями: Изменение списков ACL объекта. - Управление группами безопасности: Изменение списков ACL объекта. - Управление псевдонимами: Изменение списков ACL объекта.	Отсутствует.	Отсутствует.	Отсутствует.

Общие функции: Виртуальные Серверы администрирования	• Управление виртуальными Серверами и администрирования. • Чтение. • Запись. • Выполнение. • Выполнение действий над выборками и устройств.	• Получение списка виртуальных Серверов администрирования: Чтение. • Получение информации о виртуальном Сервере администрирования: Чтение. • Создание, обновление или удаление виртуального Сервера администрирования: Управление виртуальными Серверами и администрирования. • Перемещение виртуального Сервера администрирования в другую группу: Управление виртуальными Серверами и администрирования. • Установка прав доступа к виртуальному Серверу администр	Отсутствует.	Отчет о результатах установки обновлений стороннего ПО.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
		ирования: Управление виртуальными Серверами и администрирования.			
Общие функции: Управление ключами шифрования	• Чтение. • Запись.	• Экспорт ключей шифрования: Чтение. • Импорт ключей шифрования: Запись.	Отсутствует.	Отсутствует.	Отсутствует.

Управление мобильным и устройствам и: Общие	• Подключение новых устройств. • Отправка только информационных команд на мобильные устройства. • Отправка команд на мобильные устройства. • Управление сертификатами • Чтение. • Запись.	• Получение восстановленных данных службы управления ключами: Чтение. • Удаление сертификатов пользователей: Управление сертификатами. • Получение публичной части сертификата пользователя: Чтение. • Проверка, включены ли инфраструктура открытых ключей: Чтение. • Проверка учетной записи инфраструктуры открытых ключей: Чтение. • Получение шаблонов инфраструктуры открытых ключей: Чтение. • Получение шаблонов инфраструктуры открытых ключей с	Отсутствует.	Отсутствует.	Отсутствует.

		помощью расширенного использования ключа (EКУ) сертификата: Чтение. • Проверка, не отозваны ли сертификат инфраструктуры открытых ключей: Чтение. • Обновление параметров выпуска сертификатов пользователя: Управление сертификатами. • Получение параметров выпуска сертификатов пользователя: Чтение. • Получение пакетов по названию и версиям приложений: Чтение. • Установка или отмена сертификатов пользователя: Управление сертификатами.			

Функциональная область	Право	Действие пользователя: право, необходимо для выполнения действия	Задача	Отчет	Другое
		- Обновление сертификата пользователя: Управление сертификатами. - Установка тега для сертификата пользователя: Управление сертификатами. - Запуск генерации инсталляционного пакета, содержащего iOS MDM-профиль; отмена генерации инсталляционного пакета, содержащего iOS MDM-профиль: Подключение новых устройств.			

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Управление системой: Подключения	- Запуск RDP-сессий. - Подключение к существующим RDP-сессиям. - Туннелирование. - Сохранение файлов с устройств на рабочем месте администратора. - Чтение. - Запись. - Выполнение. - Выполнение действий над выборками и устройств.	- Создание сеанса совместного доступа к рабочему столу: Право на создание сеанса совместного доступа к рабочему столу. - Создание RDP-сессии: Подключение к существующим RDP-сессиям. - Создание туннеля: Туннелирование. - Сохранение списка сетей: Сохранение файлов с устройств на рабочем месте администратора.	Отсутствует.	Отчет о пользователях устройства.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Управление системой: Инвентаризация оборудования	- Чтение. - Запись. - Выполнение. - Выполнение действий над выборками и устройств.	- Получение или экспорт объектов инвентаризации оборудования: Чтение. - Добавление, установка или удаление объектов инвентаризации оборудования: Запись.	Отсутствует.	- Отчет о реестре оборудования. - Отчет об изменении конфигурации. - Отчет об оборудовании.	Отсутствует.
Управление системой: Управление доступом в сеть	- Чтение. - Запись.	- Просмотр параметра в Cisco: Чтение. - Изменение параметра в Cisco: Запись.	Отсутствует.	Отсутствует.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимо для выполнения действия	Задача	Отчет	Другое
Управление системой: Развертывание операционной системы	- Развертывание PXE-серверов. - Чтение. - Запись. - Выполнение. - Выполнение действий над выборками и устройств.	- Развертывание PXE-серверов: Развертывание PXE-серверов. - Просмотр списка PXE-серверов: Чтение. - Запуск или остановка процесс установки на PXE-клиентах: Выполнение. - Управление драйверами для среды WinPE и образов операционной системы: Запись.	Создание инсталляционного пакета на основе образа ОС эталонного устройства.	Отсутствует.	Инсталляционный пакет: Образ операционной системы.

Функциональная область	Право	Действие пользователя: право, необходимо для выполнения действия	Задача	Отчет	Другое
Управление системой: Системное администрирование	• Чтение. • Запись. • Выполнение. • Выполнение действий над выборками и устройств.	• Просмотр свойства патчей сторонних производителей: Чтение. • Изменение свойства патчей сторонних производителей: Запись.	• Выполнение синхронизации обновлений Центра обновлений Windows. • Установка обновлений Центра обновлений Windows. • Закрывание уязвимостей. • Установка требуемых обновлений и закрытия уязвимостей.	Отчет об обновлениях ПО.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Управление системой: Удаленная установка	• Чтение. • Запись. • Выполнение. • Выполнение действий над выборками и устройств.	• Просмотр Системного администрирования стороннего производителя на основе свойств инсталляционного пакета: Чтение. • Изменение Системного администрирования на основе свойств инсталляционного пакета: Запись.	Отсутствует.	Отсутствует.	Инсталляционные пакеты: • Пользовательское приложение. • Пакет VAPM.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Управление системой: Инвентаризация приложений	• Чтение. • Запись. • Выполнение. • Выполнение действий над выборками и устройств.	Отсутствует.	Отсутствует.	• Отчет об установленных приложениях. • Отчет об истории реестра приложений. • Отчет о состоянии групп лицензионных приложений. • Отчет о лицензионных ключах сторонних приложений.	Отсутствует.

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center, предоставляют им набор прав доступа к функциям приложения (см. раздел "Права доступа к функциям приложения" на стр. [810](#)).

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права. Некоторые из предопределенных ролей пользователей, доступных в Kaspersky Security Center, могут быть связаны с определенными должностями, например, **Аудитор**, **Специалист по безопасности**, **Контролер** (эти роли присутствуют в Kaspersky Security Center начиная с версии 11). Права доступа этих ролей предварительно настраиваются в соответствии со стандартными задачами и обязанностями соответствующих должностей. В таблице ниже показано как роли могут быть связаны с определенными должностями.

Таблица 73. Примеры ролей для определенных должностей

Роль	Комментарий
Аудитор	Разрешено выполнение любых операций со всеми типами отчетов, а также всех операций просмотра, включая просмотр удаленных объектов (предоставлены права Чтение и Запись для области Удаленные объекты). Другие операции не разрешены. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.
Контролер	Разрешен просмотр всех операций, не разрешены другие операции. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Специалист по безопасности	Разрешены всех операции просмотра, разрешено управление отчетами; предоставлены ограниченные права в области Управление системой: Подключения . Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.

В таблице ниже приведены права для каждой предопределенной роли пользователя.

Таблица 74. Права предопределенных ролей пользователей

Роль	Описание
Администратор Сервера администрирования	Разрешает все операции в следующих функциональных областях: Общие функции: - Базовая функциональность. - Обработка событий. - Иерархия Серверов администрирования. - Виртуальные Серверы администрирования. Управление системой: - Подключения. - Инвентаризация оборудования. - Инвентаризация приложений. Предоставляет права на Чтение и Запись в области Общие функции: Управление ключами шифрования.

Роль	Описание
Оператор Сервера администрирования	Предоставляет права на Чтение и Выполнение во всех следующих функциональных областях: • Общие функции: • Базовая функциональность. • Виртуальные Серверы администрирования. • Управление системой: • Подключения. • Инвентаризация оборудования. • Инвентаризация приложений.
Аудитор	Разрешает все операции в функциональной области Общий функционал: • Доступ к объектам независимо от их списков ACL. • Удаленные объекты. • Управление отчетами. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.
Администратор установки приложений	Разрешает все операции в следующих функциональных областях: • Общие функции: • Базовая функциональность. • Развертывание приложений "Лаборатории Касперского". • Управление лицензионными ключами. • Управление системой: • Развертывание операционной системы. • Системное администрирование. • Удаленная установка. • Инвентаризация приложений. Предоставляет права на Чтение и Выполнение в области Общий функционал: Базовая функциональность.

Роль	Описание
Оператор установки приложений	Предоставляет права на Чтение и Выполнение во всех следующих функциональных областях: • Общие функции: • Базовая функциональность. • Развертывание приложений "Лаборатории Касперского" (также предоставляет права на Управление патчами "Лаборатории Касперского" в этой же области). • Виртуальные Серверы администрирования. • Управление системой: • Развертывание операционной системы. • Системное администрирование. • Удаленная установка. • Инвентаризация приложений.
Администратор Kaspersky Endpoint Security	Разрешает все операции в следующих функциональных областях: • Общие функции: Базовая функциональность. • Область Kaspersky Endpoint Security, включая все функции. Предоставляет права на Чтение и Запись в области Общие функции: Управление ключами шифрования.
Оператор Kaspersky Endpoint Security	Предоставляет права на Чтение и Выполнение во всех следующих функциональных областях: • Общие функции: Базовая функциональность. • Область Kaspersky Endpoint Security, включая все функции.
Главный администратор	Разрешает все операции в функциональных областях, за исключением следующих областей: Общие функции: • Доступ к объектам независимо от их списков ACL. • Управление отчетами. Предоставляет права на Чтение и Запись в области Общие функции: Управление ключами шифрования.

Роль	Описание
Главный оператор	Предоставляет права на Чтение и Выполнение (если применимо) во всех следующих функциональных областях: • Общие функции: • Базовая функциональность. • Удаленные объекты. • Операции с Сервером администрирования. • Развертывание приложений "Лаборатории Касперского" • Виртуальные Серверы администрирования. • Управление мобильными устройствами: Общие • Управление системой, включая все функции. • Область Kaspersky Endpoint Security, включая все функции.
Администратор управления мобильными устройствами	Разрешает все операции в следующих функциональных областях: • Общие функции: Базовая функциональность. • Управление мобильными устройствами: Общие.
Оператор управления мобильными устройствами	Предоставляет права на Чтение и Выполнение в области Общие функции: Базовая функциональность. Предоставляет права на Чтение и Отправление только информационных команд на мобильные устройства в функциональной области: Управление мобильными устройствами: Общие.
Специалист по безопасности	Разрешает все операции в следующих функциональных областях: Общие функции: • Доступ к объектам независимо от их списков ACL. • Управление отчетами. Предоставляет права на Чтение, Запись, Выполнение, Сохранение файлов с устройств на рабочем месте администратора и Выполнение операций с выборками устройств в области Управление системой: Подключения. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.
Пользователь Self Service Portal	Разрешает все операции в области Управление мобильными устройствами: Self Service Portal. Эта функция не поддерживается в версиях приложения Kaspersky Security Center 11 и выше.

Роль	Описание
Контролер	Предоставляет права на Чтение в области Общие функции: Доступ к объектам независимо от их списков ACL и Общие функции: функциональная область Управление отчетами . Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Администратор Системного администрирования	Разрешает все операции в области Общие функции: Базовая функциональность и Управление системой (включая все функции).
Оператор Системного администрирования	Предоставляет права на Чтение и Выполнение (если применимо) в области Общие функции: Базовая функциональность и Управление системой (включая все функции).

Добавление роли пользователя

► Чтобы добавить роль пользователя:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойства Сервера администрирования в панели **Разделы** перейдите в раздел **Роли пользователей** и нажмите на кнопку **Добавить**.

Раздел **Роли пользователей** доступен, если включен параметр **Отображать разделы с параметрами безопасности** (см. раздел "Настройка общих параметров Сервера администрирования" на стр. [716](#)).

4. В окне **Новая роль** настройте параметры роли:
 - В панели **Разделы** выберите раздел **Общие** и укажите имя роли.
Имя роли не может превышать 100 символов.
 - В разделе **Права** настройте набор прав, установив флажки **Разрешить** и **Запретить** напротив функций приложения.

Если вы работаете на главном Сервере администрирования, вы можете включить параметр (см. раздел "Распространение пользовательских ролей на подчиненные Серверы администрирования" на стр. [840](#)) **Передать список ролей подчиненному Серверу администрирования**.

5. Нажмите на кнопку **ОК**.

Роль добавлена.

Роли пользователей, созданные для Сервера администрирования, отображаются в окне свойств Сервера в разделе **Роли пользователей**. Вы можете изменять и удалять роли пользователей, а также назначать

роли группам безопасности или отдельным пользователям (см. раздел "Назначение роли пользователю или группе безопасности" на стр. [838](#)).

Назначение роли пользователю или группе безопасности

► Чтобы назначить роль пользователю или группе пользователей:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Безопасность**.

Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности** (см. раздел "Настройка общих параметров Сервера администрирования" на стр. [716](#)).

4. В поле **Имена групп или пользователей** выберите пользователя или группу пользователей, которой нужно присвоить роль.

Если пользователь или группа отсутствует в поле, добавьте их по кнопке **Добавить**.

При добавлении пользователя по кнопке **Добавить** можно выбрать тип аутентификации пользователя (Microsoft Windows или Kaspersky Security Center). Аутентификация Kaspersky Security Center используется для выбора учетных записей внутренних пользователей, которые используются для работы с виртуальными Серверами администрирования.

5. Перейдите на вкладку **Роли** и нажмите на кнопку **Добавить**.
Откроется окно **Роли пользователей**. В окне отображаются созданные роли пользователей.
6. В окне **Роли пользователей** выберите роль для группы безопасности.
7. Нажмите на кнопку **ОК**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе безопасности. Назначенные роли отображаются на вкладке **Роли** в разделе **Безопасность** окна свойств Сервера администрирования.

Назначение прав пользователям или группам пользователей

Вы можете назначить права пользователям или группам пользователей, чтобы использовать различные возможности Сервера администрирования и приложений "Лаборатории Касперского", для которых у вас есть плагины управления, например, Kaspersky Endpoint Security для Windows.

► Чтобы назначить права пользователю или группе пользователей:

1. В дереве консоли выполните одно из следующих действий:
 - Раскройте узел **Сервер администрирования** и выберите подпапку с именем требуемого Сервера администрирования.
 - Выберите группу администрирования.

2. В контекстном меню Сервера администрирования или группы администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервера администрирования (или окне свойств группы администрирования) в панели **Разделы** выберите раздел **Безопасность**.

Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности** (см. раздел "**Настройка общих параметров Сервера администрирования**" на стр. [716](#)).

4. В разделе **Безопасность** в списке **Имена групп или пользователей** выберите пользователя или группу пользователей.
5. В списке прав в нижней части окна, на вкладке **Права** настройте права для пользователей или групп:
 - a. Нажмите на значок плюс (+), чтобы раскрыть узел в списке, и назначьте права.
 - b. Установите флажки **Разрешить** и **Запретить** рядом с требуемыми правами.

Пример 1: Раскройте узел **Доступ к объектам независимо от их списков ACL** или узел **Удаленные объекты**, и выберите **Чтение**.

Пример 2: Раскройте узел **Базовая функциональность** и выберите **Запись**.

6. После того как вы настроили набор прав, нажмите на кнопку **Применить**.

Набор прав для пользователя или группа пользователей настроен.

Права Сервера администрирования (или группы администрирования) разделены на следующие области:

- Общие функции:
 - Управление группами администрирования.
 - Доступ к объектам независимо от их списков ACL.
 - Базовая функциональность.
 - Удаленные объекты.
 - Обработка событий.
 - Операции с Сервером администрирования (только в окне свойств Сервера администрирования).
 - Развертывание приложений "Лаборатории Касперского".
 - Управление лицензионными ключами.
 - Управление отчетами.
 - Иерархия Серверов.
 - Права пользователей.
 - Виртуальные Серверы администрирования.
- Управление мобильными устройствами:
 - Общие.
- Управление системой:
 - Подключения.

- Инвентаризация оборудования.
- Управление доступом в сеть.
- Развертывание операционной системы.
- Управление уязвимостями и патчами.
- Удаленная установка.
- Инвентаризация приложений.

Если для права не выбрано ни **Разрешить**, ни **Запретить**, оно считается *неопределенным*: право отклоняется до тех пор, пока оно не будет явно отклонено или разрешено для пользователя.

Права пользователей являются суммой следующего:

- собственных прав пользователя;
- прав всех ролей, назначенных пользователю;
- прав всех групп безопасности, в которые входит пользователь;
- прав всех ролей, назначенных группам, в которые входит пользователь.

Если хотя бы в одном наборе прав есть запрещенное право (для права установлен флажок **Запретить**), тогда для пользователя это право запрещено, даже если в других наборах прав оно разрешено или не определено.

Распространение пользовательских ролей на подчиненные Серверы администрирования

По умолчанию списки пользовательских ролей главного и подчиненного Серверов администрирования являются независимыми. Вы можете настроить приложения для автоматического распространения ролей пользователей, созданных на главном Сервере администрирования, на все подчиненные Сервера администрирования. Роли пользователей также могут распространяться с подчиненного Сервера администрирования на собственные подчиненные Сервера администрирования.

► *Чтобы распространить роли пользователей с главного Сервера администрирования на подчиненные Серверы администрирования:*

1. Откройте главное окно приложения.
2. Выполните одно из следующих действий:
 - В дереве консоли в контекстном меню требуемого Сервера администрирования выберите пункт **Свойства**.
 - Если у вас есть активная политика Сервера администрирования, в рабочей области папки **Политики** в контекстном меню этой политики выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования или в окне свойств политики в панели **Разделы** перейдите в раздел **Роли пользователей**.

Раздел **Роли пользователей** доступен, если включен параметр **Отображать разделы с параметрами безопасности** (см. раздел "**Настройка общих параметров Сервера администрирования**" на стр. [716](#)).

4. Включите параметр **Передать список ролей подчиненному Серверу администрирования**.

5. Нажмите на кнопку **ОК**.

Приложение копирует роли пользователей главного Сервера администрирования на подчиненные Серверы администрирования.

Если параметр **Передать список ролей подчиненному Серверу администрирования** включен и роли пользователей распространены, такие роли не доступны для изменений или удаления на подчиненном Сервере администрирования. Когда вы создаете роль или изменяете существующую роль на главном Сервере администрирования, изменения автоматически копируются на подчиненные Серверы администрирования. Когда вы удаляете роль пользователя на главном Сервере администрирования, эта роль остается на подчиненном Сервере администрирования и может быть изменена или удалена.

Роли, которые распространяются на подчиненный Сервер администрирования с главного Сервера, отображаются с помощью значка замок (🔒). Вы не можете изменять эти роли на подчиненном Сервере администрирования.

Если роль создается на главном Сервере администрирования, а на подчиненном Сервере администрирования есть роль с таким же именем, новая роль копируется на подчиненный Сервер администрирования, и к ее имени в скобках добавляется номер, например, ~1, ~2 (номер может быть случайным).

Если отключить параметр **Передать список ролей подчиненному Серверу администрирования**, все роли пользователя останутся на подчиненных Серверах администрирования, но станут независимыми от ролей на главном Сервере администрирования. Когда роли на подчиненных Серверах администрирования становятся независимыми, их можно изменять или удалять.

Назначение пользователя владельцем устройства

Вы можете назначить пользователя владельцем устройства, чтобы "закрепить" устройство за этим пользователем. При необходимости выполнить какие-либо действия с устройством (например, обновить аппаратное обеспечение) администратор может проинформировать владельца устройства и согласовать действия с ним.

► *Чтобы назначить пользователя владельцем устройства:*

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки на вкладке **Устройства** выберите устройство, для которого нужно назначить владельца.
3. В контекстном меню устройства выберите пункт **Свойства**.
4. В окне свойств устройства выберите **Информация о системе** → **Сеансы**.
5. Нажмите на кнопку **Назначить** рядом с полем **Владелец устройства**.
6. В окне **Выбор пользователя** выберите пользователя, которого нужно назначить владельцем устройства и нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК**.

В результате владелец устройства будет назначен. По умолчанию поле **Владелец устройства** заполнено значением из Active Directory и обновляется при каждом опросе Active Directory (см. раздел "Опрос Active Directory" на стр. [328](#)). Вы можете просмотреть список владельцев устройств в отчете **Отчет о владельцах устройств**. Отчет можно создать с помощью мастера создания отчетов (см. раздел "Создание шаблона отчета" на стр. [602](#)).

Рассылка сообщений пользователям

► Чтобы отправить сообщение пользователю по электронной почте:

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.
Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В контекстном меню пользователя выберите **Уведомлять по электронной почте**.
3. Заполните необходимые поля в окне **Сообщение для пользователя** и нажмите на кнопку **ОК**.

В результате сообщение будет отправлено на электронную почту, указанную в свойствах пользователя.

► Чтобы отправить SMS-сообщение пользователю:

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.
2. В контекстном меню пользователя выберите **Отправить SMS-сообщение**.
3. Заполните необходимые поля в окне **Текст SMS** и нажмите на кнопку **ОК**.

В результате сообщение будет отправлено на мобильное устройство, номер которого указан в свойствах пользователя.

Просмотр списка мобильных устройств пользователя

► Чтобы просмотреть список мобильных устройств пользователя:

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.
Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В контекстном меню учетной записи пользователя выберите пункт **Свойства**.
3. В окне свойств учетной записи пользователя выберите раздел **Мобильные устройства**.

В разделе **Мобильные устройства** можно просмотреть список мобильных устройств пользователя и информацию о мобильных устройствах. По кнопке **Экспортировать в файл** можно сохранить список мобильных устройств в файле.

Установка сертификата пользователю

Вы можете установить пользователю сертификаты трех типов:

- общий сертификат, необходим для идентификации мобильного устройства пользователя;
- почтовый сертификат, необходим для настройки корпоративной почты на мобильном устройстве пользователя;
- VPN-сертификат, необходим для настройки виртуальной частной сети на мобильном устройстве пользователя.

► Чтобы выписать пользовательский сертификат и установить его:

1. В дереве консоли откройте папку **Учетные записи пользователей** и выберите учетную запись пользователя.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню учетной записи пользователя выберите пункт **Установить сертификат**.

Будет запущен мастер установки сертификата. Следуйте далее указаниям мастера.

В результате работы мастера установки сертификата сертификат будет создан и установлен пользователю. Список установленных сертификатов пользователя можно просмотреть и экспортировать в файл (см. раздел "Просмотр списка сертификатов, выписанных пользователю" на стр. [843](#)).

Просмотр списка сертификатов, выписанных пользователю

► *Чтобы просмотреть список всех сертификатов, выписанных пользователю:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.
Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В контекстном меню учетной записи пользователя выберите пункт **Свойства**.
3. В окне свойств учетной записи пользователя выберите раздел **Сертификаты**.

В разделе **Сертификаты** можно просмотреть список сертификатов пользователя и информацию о сертификатах. По кнопке **Экспортировать в файл** можно сохранить список сертификатов в файле.

Об администраторе виртуального Сервера

При необходимости можно создать несколько учетных записей администраторов виртуального Сервера.

Администратор виртуального Сервера администрирования является внутренним пользователем Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Удаленная установка операционных систем и приложений

Kaspersky Security Center позволяет централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку приложений "Лаборатории Касперского" или других производителей программного обеспечения.

Для создания образов операционных систем установите Windows ADK <https://go.microsoft.com/fwlink/?linkid=2165884> и средства дополнения Windows PE для Windows ADK <https://go.microsoft.com/fwlink/?linkid=2166133> на Сервере администрирования. Вы можете создать образ любой версии операционной системы Windows, отвечающей требованиям Kaspersky Security Center (см. раздел "Аппаратные и программные требования" на стр. [29](#)).

Kaspersky Security Center не поддерживает 64-разрядные версии Windows ADK и Windows PE.

Захват образов операционных систем

Kaspersky Security Center может выполнять захват образов операционных систем устройств и доставлять эти образы на Сервер администрирования. Такие образы операционных систем хранятся на Сервере администрирования в специальной папке. Снятие и создание образа операционной системы эталонного

устройства выполняется с помощью задачи создания инсталляционного пакета (см. раздел "Создание инсталляционных пакетов приложений" на стр. [850](#)).

Функциональность захвата образа операционной системы имеет следующие особенности:

- Образ операционной системы невозможно снимать с устройства, на котором установлен Сервер администрирования.
- Во время снятия образа операционной системы происходит обнуление параметров эталонного устройства утилитой sysprep.exe. В случае необходимости восстановления параметров эталонного устройства в мастере создания задачи снятия образа ОС необходимо установить флажок **Сохранять резервную копию состояния устройства**.
- В процессе снятия образа выполняется перезагрузка эталонного устройства.

Развертывание образов операционных систем на новых устройствах

Вы можете использовать полученные образы для развертывания на новых устройствах в сети, на которых еще не была установлена операционная система. Для этой цели используется технология Preboot eXecution Environment (PXE). Вы назначаете устройство в сети, которое будет использоваться в качестве PXE-сервера. Это устройство должно отвечать следующим требованиям:

- на устройстве должен быть установлен Агент администрирования;
- на устройстве не должен работать DHCP-сервер, так как PXE-сервер использует те же порты, что и DHCP;
- в сегменте сети, в который входит устройство, не должно быть других PXE-серверов.

Для развертывания операционной системы должны быть выполнены следующие условия:

- на устройстве должна быть установлена сетевая карта;
- устройство должно быть подключено к сети;
- при загрузке устройства в BIOS необходимо выбрать параметр загрузки по сети.

Развертывание операционной системы выполняется в следующей последовательности:

1. Клиентское устройство устанавливает соединение с PXE-сервером при загрузке клиентского устройства.
2. Клиентское устройство загружается в среде Windows Preinstallation Environment (WinPE).

Для включения устройства в среду WinPE может потребоваться настройка состава драйверов для среды WinPE.

3. Клиентское устройство регистрируется на Сервере администрирования.
4. Администратор назначает клиентскому устройству инсталляционный пакет с образом операционной системы.

Администратор может добавлять необходимые драйверы в инсталляционный пакет с образом операционной системы. Администратор также может указывать конфигурационный файл с параметрами операционной системы (файл ответов), которые должны применяться во время установки.

5. Выполняется развертывание операционной системы на клиентском устройстве.

Администратор может вручную указать MAC-адреса еще не подключившихся клиентских устройств и назначить им инсталляционный пакет с образом операционной системы. Когда указанные клиентские устройства подключаются к PXE-серверу, автоматически выполняется установка операционной системы на этих устройствах.

Развертывание образов операционных систем на устройствах с уже установленной операционной системой

Развертывание образов операционной системы на клиентских устройствах, на которых уже установлена рабочая операционная система, выполняется с помощью задачи удаленной установки для наборов устройств.

Обратите внимание, что выполняется чистая установка операционной системы. Все данные будут удалены.

Установка приложений "Лаборатории Касперского" и других производителей программного обеспечения

Администратор может создавать инсталляционные пакеты любых приложений, включая приложения, указанные пользователем, и устанавливать эти приложения на клиентские устройства с помощью задачи удаленной установки.

В этом разделе

Создание образов операционных систем	845
Установка образов операционных систем.....	846
Настройка адреса прокси-сервера KSN	847
Добавление драйверов для среды предустановки Windows (WinPE)	847
Добавление драйверов в инсталляционный пакет с образом операционной системы	848
Настройка параметров утилиты sysprep.exe.....	848
Развертывание операционных систем на новых устройствах в сети	849
Развертывание операционных систем на клиентских устройствах	850
Создание инсталляционных пакетов приложений	850
Выписка сертификата для инсталляционных пакетов приложений	851
Установка приложений на клиентские устройства.	852

Создание образов операционных систем

Создание образов операционных систем выполняется при помощи задачи снятия образа операционной системы эталонного устройства.

► *Чтобы создать задачу снятия образа операционной системы:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.
3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет с образом операционной системы**.

4. Следуйте далее указаниям мастера.

В результате работы мастера создается задача Сервера администрирования **Создание инсталляционного пакета на основе образа ОС эталонного устройства**. Задачу можно просмотреть в папке **Задачи**.

В результате выполнения задачи **Создание инсталляционного пакета на основе образа ОС эталонного устройства** создается инсталляционный пакет, который можно использовать для развертывания операционной системы на клиентских устройствах с помощью PXE-сервера или задачи удаленной установки. Просмотреть инсталляционный пакет можно в папке **Инсталляционные пакеты**.

Установка образов операционных систем

Kaspersky Security Center позволяет разворачивать на устройства сети организации wim-образы настольных и серверных версий операционных систем Windows.

Образ операционной системы, пригодный для развертывания средствами Kaspersky Security Center, может быть получен следующими способами:

- импортом из файла install.wim, который входит в состав дистрибутива Windows;
- захватом образа с эталонного устройства.

Поддерживаются два сценария развертывания образа операционной системы:

- развертывание на "чистое" устройство, то есть на устройство без установленной на нем операционной системы;
- развертывание на устройство, работающее под управлением операционной системы Windows.

Используйте Use Windows Preinstallation Environment (Windows PE) для захвата и развертывания образов операционной системы. В WinPE следует добавить все драйверы, необходимые для правильной работы всех устройств. Как правило, необходимо добавить драйверы сетевого адаптера и контроллера устройства хранения.

Для реализации сценариев развертывания и захвата образов должны быть выполнены следующие требования:

- На Сервер администрирования должен быть установлен Windows Automated Installation Kit (WAIK) <https://go.microsoft.com/fwlink/?linkid=2165884> версии 2.0 и выше или Windows ADK с надстройкой Windows PE для Windows ADK <https://go.microsoft.com/fwlink/?linkid=2166133>. Если предполагаются работы по установке или захвату образов на Windows XP, следует установить WAIK.
- В сети, в которой расположено устройство, должен присутствовать DHCP-сервер.
- Папка общего доступа Сервера администрирования должна быть доступна для чтения из сети, в которой находится устройство. Если папка общего доступа расположена на Сервере администрирования, то доступ нужен для учетной записи KIPxeUser (эта учетная запись создается автоматически на этапе работы инсталлятора Сервера администрирования). Если папка расположена вне Сервера администрирования, то доступ нужен для всех.

При выборе образа операционной системы для установки администратор должен явно указать архитектуру процессора устройства: x86 или x86-64.

Настройка адреса прокси-сервера KSN

По умолчанию доменное имя Сервера администрирования совпадает с адресом прокси-сервера KSN. При изменении доменного имени для Сервера администрирования необходимо указать правильный адрес прокси-сервера KSN, чтобы предотвратить потерю связи между устройствами и KSN.

► *Чтобы настроить адреса прокси-сервера KSN:*

1. В дереве консоли перейдите в раздел **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
2. В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Свойства**.
3. В открывшемся окне укажите новый адрес прокси-сервера KSN на вкладке **Общие**.
4. Нажмите на кнопку **Применить**.

С этого момента указанный адрес используется как адрес прокси-сервера KSN.

[См. также](#)

Kaspersky Security Network и Kaspersky Private Security Network[873](#)

Добавление драйверов для среды предустановки Windows (WinPE)

► *Чтобы добавить драйверы для среды предустановки Windows (WinPE):*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Развертывание образов устройств**.
2. В рабочей области папки **Развертывание образов устройств** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Настроить состав драйверов для среды предустановки Windows (WinPE)**.
Откроется окно **Драйверы для среды предустановки Windows**.
3. В окне **Драйверы для среды предустановки Windows** нажмите на кнопку **Добавить**.
Откроется окно **Выбор драйвера**.
4. В окне **Выбор драйвера** выберите драйвер из списка.
Если необходимый драйвер отсутствует в списке, нажмите на кнопку **Добавить** и в открывшемся окне **Добавление драйвера** укажите имя драйвера и папку дистрибутива драйвера.
Вы можете выбрать папку по кнопке **Обзор**.
В окне **Добавление драйвера** нажмите на кнопку **ОК**.
5. В окне **Выбор драйвера** нажмите на кнопку **ОК**.
Драйвер будет добавлен в хранилище Сервера администрирования. Добавленный в хранилище драйвер отображается в окне **Выбор драйвера**.
6. В окне **Драйверы для среды предустановки Windows** нажмите на кнопку **ОК**.
Драйвер будет добавлен в среду предустановки Windows (WinPE).

Добавление драйверов в инсталляционный пакет с образом операционной системы

► Чтобы добавить драйверы в инсталляционный пакет с образом операционной системы:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета с образом операционной системы выберите пункт **Свойства**.

Откроется окно свойств инсталляционного пакета.

3. В окне свойств инсталляционного пакета выберите раздел **Дополнительные драйверы**.
4. Нажмите на кнопку **Добавить**, расположенную в разделе **Дополнительные драйверы**.

Откроется окно **Выбор драйвера**.

5. В окне **Выбор драйвера** выберите драйверы, которые вы хотите добавить в инсталляционный пакет с образом операционной системы.

Новые драйверы можно добавить в хранилище Сервера администрирования при нажатии на кнопку **Добавить** в окне **Выбор драйвера**.

6. Нажмите на кнопку **ОК**.

Добавленные драйверы отображаются в разделе **Дополнительные драйверы** в окне свойств инсталляционного пакета с образом операционной системы.

Настройка параметров утилиты sysprep.exe

Утилита sysprep.exe используется для подготовки устройства к созданию с него образа операционной системы.

► Чтобы настроить параметры утилиты sysprep.exe:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета с образом операционной системы выберите пункт **Свойства**.

Откроется окно свойств инсталляционного пакета.

3. В окне свойств инсталляционного пакета выберите раздел **Параметры sysprep.exe**.
4. В разделе **Параметры sysprep.exe** укажите конфигурационный файл, который будет использоваться при развертывании операционной системы на клиентском устройстве:

- **Использовать конфигурационный файл по умолчанию.** Выберите этот вариант, чтобы использовать файл ответов, создаваемый по умолчанию во время снятия образа операционной системы.
- **Задать пользовательские значения основных параметров.** Выберите этот вариант, чтобы задать значения параметров с помощью пользовательского интерфейса.
- **Задать конфигурационный файл.** Выберите этот вариант, чтобы использовать собственный файл ответов.

5. Нажмите на кнопку **Применить**, чтобы внесенные изменения вступили в силу.

Развертывание операционных систем на новых устройствах в сети

- Чтобы развернуть операционную систему на новых устройствах, на которых еще не установлена операционная система:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Развертывание образов устройств**.

Убедитесь, что в окне **Настройка интерфейса** включен параметр **Отображать Системное администрирование** (см. раздел "Настройка интерфейса" на стр. [320](#)). Иначе папка **Удаленная установка** не отображается.

2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите значение **Управлять списком PXE-серверов в сети**.

Откроется окно **Свойства: Развертывание образов устройств** на разделе **PXE-серверы**.

3. В разделе **PXE-серверы** нажмите на кнопку **Добавить** и в открывшемся окне **PXE-серверы** выберите устройство, которое будет использоваться как PXE-сервер.

Добавленное устройство отобразится в разделе PXE-серверы. Созданные WinPE-файлы передаются на устройство с Сервера администрирования. Процесс передачи файлов обычно занимает 10 минут. После завершения передачи файлов отображаемое значение **Статус** меняется с **Начало работы** на **Готов**.

4. В разделе **PXE-серверы** выберите PXE-сервер и нажмите на кнопку **Свойства**.
5. В окне свойств выбранного PXE-сервера в разделе **Параметры подключения к PXE-серверу** выполните настройку параметров подключения Сервера администрирования к PXE-серверу.
6. Выполните загрузку клиентского устройства, на котором вы хотите развернуть операционную систему.
7. В среде BIOS клиентского устройства выберите вариант установки Network boot.

Клиентское устройство подключается к PXE-серверу и отображается в рабочей области папки **Развертывание образов устройств**.

8. В блоке **Действия** по ссылке **Назначить инсталляционный пакет** выберите инсталляционный пакет, который будет использоваться для установки операционной системы на выбранное устройство.

Используйте инструмент DiskPart на выбранном устройстве, чтобы проверить доступные диски. В командной строке Windows PE введите `diskpart`, чтобы открыть инструмент DiskPart. Введите `list disk`, чтобы просмотреть список дисков.

После добавления устройства и назначения для него инсталляционного пакета развертывание операционной системы на этом устройстве начинается автоматически.

9. Для отмены развертывания операционной системы на клиентском устройстве воспользуйтесь ссылкой **Отменить установку образов ОС** в блоке **Действия**.

- Чтобы добавить устройства по MAC-адресу, выполните одно из следующих действий:

- по ссылке **Добавить MAC-адрес устройства** в папке **Развертывание образов устройств** откройте окно **Новое устройство** и укажите MAC-адрес устройства, которое вы хотите добавить;
- по ссылке **Импортировать MAC-адреса устройств из файла** в папке **Развертывание образов устройств** выберите файл, содержащий список MAC-адресов всех устройств, на которых вы хотите развернуть операционную систему.

См. также:

Основной сценарий установки.....[56](#)

Развертывание операционных систем на клиентских устройствах

► Чтобы выполнить развертывание операционной системы на клиентских устройствах с уже установленной операционной системой:

1. В дереве консоли откройте папку **Удаленная установка** и перейдите по ссылке **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)**, чтобы запустить мастер развертывания защиты.
2. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет с образом операционной системы.
3. Следуйте далее указаниям мастера.

В результате работы мастера создается задача удаленной установки операционной системы на клиентских устройствах. Запустить или остановить задачу можно в папке **Задачи**.

Создание инсталляционных пакетов приложений

► Чтобы создать инсталляционный пакет приложения:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.
3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на одну из кнопок:
 - **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**. Выберите этот вариант, если вы хотите создать инсталляционный пакет для приложения "Лаборатории Касперского".
 - **Создать инсталляционный пакет для указанного исполняемого файла**. Выберите этот вариант, если вы хотите создать инсталляционный пакет для приложения с помощью исполняемого файла. Как правило, исполняемый файл является установочным файлом приложения.
 - Копировать всю папку в инсталляционный пакет
 - Указать параметры установки
 - **Выбрать приложение из базы "Лаборатории Касперского" для создания инсталляционного пакета**. Выберите этот вариант, если вы хотите выбрать приложение стороннего производителя из базы "Лаборатории Касперского", для которого требуется создать инсталляционный пакет. База данных создается автоматически при запуске задачи Загрузка обновлений в хранилище Сервера администрирования (см. раздел "Создание задачи для загрузки обновлений в хранилище Сервера администрирования" на стр. [469](#)); приложения отображаются в списке.

- **Создать инсталляционный пакет с образом операционной системы.** Выберите этот вариант, если вы хотите создать инсталляционный пакет с образом операционной системы эталонного устройства.

В результате работы мастера создается задача Сервера администрирования с именем **Создание инсталляционного пакета на основе образа ОС эталонного устройства**. В результате выполнения этой задачи создается инсталляционный пакет, который можно использовать для развертывания образа операционной системы с помощью PXE-сервера или задачи удаленной установки.

4. Следуйте далее указаниям мастера.

В результате работы мастера создается инсталляционный пакет, который можно использовать для установки приложения на клиентские устройства. Вы можете просмотреть инсталляционный пакет в папке **Инсталляционные пакеты** дерева консоли.

См. также:

Создание инсталляционного пакета.[372](#)

Выписка сертификата для инсталляционных пакетов приложений

► Чтобы выписать сертификат для инсталляционного пакета приложения:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.
2. В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Дополнительно**.
В результате откроется окно свойств папки **Инсталляционные пакеты**.
3. В окне свойств папки **Инсталляционные пакеты** выберите раздел **Подпись автономных пакетов**.
4. В разделе **Подпись автономных пакетов** нажмите на кнопку **Задать**.
Откроется окно **Сертификат**.
5. В поле **Тип сертификата** выберите открытый или закрытый тип сертификата:
 - Если выбрано значение **Контейнер PKCS#12**, укажите файл сертификата и пароль.
 - Если выбрано значение **X.509-сертификат**:
 - a. укажите файл закрытого ключа (файл с расширением `prk` или `pem`);
 - b. укажите пароль закрытого ключа;
 - c. укажите файл открытого ключа (файл с расширением `cer`).
6. Нажмите на кнопку **ОК**.

В результате будет выписан сертификат для инсталляционного пакета приложения.

Установка приложений на клиентские устройства.

► Чтобы установить приложение на клиентские устройства:

1. В дереве консоли откройте папку **Удаленная установка** и перейдите по ссылке **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)**, чтобы запустить мастер развертывания защиты.
2. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет приложения, которое вы хотите установить.
3. Следуйте далее указаниям мастера.

В результате работы мастера создается задача удаленной установки приложения на клиентских устройствах. Запустить или остановить задачу можно в папке **Задачи**.

Вы можете устанавливать Агент администрирования на клиентские устройства с операционными системами Windows, Linux и macOS с помощью мастера развертывания защиты. Чтобы управлять 64-разрядными приложениями безопасности с помощью Kaspersky Security Center на устройствах с операционными системами Linux, необходимо использовать 64-разрядный Агент администрирования для Linux. Требуемую версию Агента администрирования можно загрузить с веб-сайта Службы технической поддержки <https://support.kaspersky.com>. Перед выполнением удаленной установки Агента администрирования на устройство с операционной системой Linux необходимо подготовить устройство (см. раздел "Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux" на стр. [384](#)).

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов. Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия*. Каждая ревизия имеет номер.

Объекты приложения, которые поддерживают работу с ревизиями:

- свойства Сервера администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать объект с выбранной ревизией другого однотипного объекта (см. раздел "Сравнение ревизий объекта" на стр. [855](#));

- просматривать выбранную ревизию (см. раздел "Просмотр раздела История ревизий" на стр. [854](#));
- откатывать изменения объекта к выбранной ревизии (см. раздел "Откат изменений" на стр. [857](#));
- сохранять ревизии в файле формата TXT (см. раздел "Сохранение ревизии объекта в файле" на стр. [857](#)).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- номер ревизии объекта;
- дата и время изменения объекта;
- имя пользователя, изменившего объект;
- выполненное действие с объектом;
- описание ревизии изменения параметров объекта (см. раздел "Добавление описания ревизии" на стр. [858](#)).

В этом разделе

О ревизиях объектов	854
Просмотр раздела История ревизий.....	854
Сравнение ревизий объекта	855
Установка срока хранения ревизий объектов и информации об удаленных объектах	856
Просмотр ревизии объекта	856
Сохранение ревизии объекта в файле	857
Откат изменений	857
Добавление описания ревизии	858

О ревизиях объектов

Вы можете выполнять с ревизиями объектов следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать объект с выбранной ревизией другого однотипного объекта (см. раздел "Сравнение ревизий объекта" на стр. [855](#));
- просматривать выбранную ревизию (см. раздел "Просмотр раздела История ревизий" на стр. [854](#));
- откатывать изменения объекта к выбранной ревизии (см. раздел "Откат изменений" на стр. [857](#));
- сохранять ревизии в файле формата TXT (см. раздел "Сохранение ревизии объекта в файле" на стр. [857](#)).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- номер ревизии объекта;
- дата и время изменения объекта;
- имя пользователя, изменившего объект;
- выполненное действие с объектом;
- описание ревизии изменения параметров объекта (см. раздел "Добавление описания ревизии" на стр. [858](#)).

Просмотр раздела История ревизий

Вы можете сравнить ревизии объекта с текущей ревизией, сравнить ревизии, выбранные в списке, или сравнить ревизию объекта с ревизией другого однотипного объекта.

► Чтобы просмотреть раздел **История ревизий** объекта:

1. В дереве консоли выберите один из объектов:
 - узел **Сервер администрирования**;
 - папку **Политики**;
 - папку **Задачи**;
 - папку группы администрирования;
 - папку **Учетные записи пользователей**;
 - папку **Удаленные объекты**;
 - подпапку **Инсталляционные пакеты**, вложенную в папку **Удаленная установка**.
2. В зависимости от местоположения соответствующего объекта выполните одно из следующих действий:
 - Если объект находится в узле **Сервер администрирования** или в папке группы администрирования, выберите пункт **Свойства** в контекстном меню объекта.

- Если объект находится в папке **Политики, Задачи, Учетные записи пользователей, Удаленные объекты** или **Инсталляционные пакеты**, выберите папку и в соответствующей рабочей области выберите объект.

Откроется окно свойств объекта.

3. В панели **Разделы** выберите раздел **История ревизий**.

История ревизий отображается в рабочей области.

Сравнение ревизий объекта

Вы можете сравнить предыдущие ревизии объекта с текущей ревизией, сравнить ревизии, выбранные в списке, или сравнить ревизию объекта с ревизией другого однотипного объекта.

► Чтобы сравнить ревизии объекта:

1. Выберите объект и перейдите к окну свойств этого объекта.
2. В окне свойств задачи выберите раздел **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. [854](#)).
3. В рабочей области в списке ревизий объекта выберите ревизию для сравнения.
Для выбора более двух ревизий объекта используйте клавиши **SHIFT** и **CTRL**.
4. Выполните одно из следующих действий:
 - Нажмите на кнопку **Сравнить** и в раскрывающемся списке выберите одно из значений:
 - **Сравнить с текущей ревизией**
Выберите этот вариант, чтобы сравнить выбранную ревизию с текущей.
 - **Сравнить выбранные ревизии**
Выберите этот вариант, чтобы сравнить две выбранные ревизии.
 - **Сравнить с другой задачей**
При работе с ревизиями задач выберите вариант **Сравнить с другой задачей**, чтобы сравнить выбранную ревизию с ревизией другой задачи.
При работе с ревизиями политик выберите вариант **Сравнить с другой политикой**, чтобы сравнить выбранную ревизию с ревизией другой политики.
 - Откройте окно свойств требуемой ревизии двойным щелчком мыши. В открывшемся окне свойств ревизии нажмите на одну из следующих кнопок:
 - **Сравнить с текущей**
Нажмите на эту кнопку, чтобы сравнить выбранную ревизию с текущей.
 - **Сравнить с предыдущей**
Нажмите на эту кнопку, чтобы сравнить выбранную ревизию с предыдущей.

Отчет о сравнении ревизий в формате HTML отображается в вашем браузере по умолчанию.

В отчете можно свернуть некоторые блоки параметров ревизии. Чтобы свернуть блок параметров ревизии, нажмите на значок стрелки (▲) рядом с названием блока.

В ревизии Сервера администрирования попадает информация об изменениях, кроме информации из следующих областей:

- раздела **Трафик**;
- раздела **Правила назначения тегов**;
- раздела **Уведомление**;
- раздела **Точки распространения**;
- раздела **Вирусная атака**.

Из раздела **Вирусная атака** не будет записана информация о настройке активации политик по событию Вирусная атака.

Вы можете сравнивать ревизии удаленного объекта с ревизией существующего объекта, но не наоборот: вы не можете сравнивать ревизии существующего объекта с ревизией удаленного объекта.

Установка срока хранения ревизий объектов и информации об удаленных объектах

Срок хранения ревизий объекта такой же, как срок хранения информации об удаленных объектах. Срок, заданный по умолчанию, – 90 дней. Этого достаточно для регулярного аудита приложения.

Только пользователи с правами **Изменение** в области **Удаленные объекты** (см. раздел "**Назначение прав пользователям или группам пользователей**" на стр. [838](#)) могут изменить срок хранения ревизий объектов и информации об удаленных объектах.

► Чтобы изменить срок хранения ревизий объектов и информации об удаленных объектах:

1. В дереве консоли выберите Сервер администрирования, для которого нужно изменить срок хранения ревизий объектов и информации об удаленных объектах.
2. В контекстном меню объекта выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Хранилище истории ревизий** укажите требуемый срок хранения (в днях).
4. Нажмите на кнопку **ОК**.

Ревизии объектов и информация об удаленных объектах будут храниться указанное количество дней.

Просмотр ревизии объекта

Если вам понадобилось узнать, какие изменения проводились с объектом в определенный период, вы можете просмотреть ревизии объекта.

► Чтобы просмотреть ревизии объекта:

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. [854](#)) объекта.
2. В списке ревизий объекта выберите ревизию, параметры которой нужно посмотреть.
3. Выполните одно из следующих действий:
 - Нажмите на кнопку **Просмотреть ревизию**.
 - Откройте окно свойств ревизии двойным щелчком мыши по названию ревизии и нажмите на кнопку **Просмотреть ревизию**.

Отобразится отчет с параметрами выбранной ревизии объекта в формате HTML. В отчете можно свернуть некоторые блоки параметров ревизии объекта. Чтобы свернуть блок параметров ревизии, нажмите на значок стрелки (▲) рядом с названием блока.

Сохранение ревизии объекта в файле

Вы можете сохранить ревизию объекта в текстовом файле, например, чтобы отправить файл по электронной почте.

► Чтобы сохранить ревизию объекта в файле:

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. [854](#)) объекта.
2. В списке ревизий объекта выберите ревизию, параметры которой нужно сохранить.
3. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Сохранить в файл**.

Ревизия будет сохранена в файле формата TXT.

Откат изменений

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

► Чтобы откатить изменения объекта:

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. [854](#)) объекта.
2. В списке ревизий объекта выберите номер ревизии, к которой нужно откатить изменения.
3. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Добавление описания ревизии

Вы можете добавить описание для ревизии, чтобы в дальнейшем было проще найти необходимую ревизию в списке.

► *Чтобы добавить описание ревизии:*

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. [854](#)) объекта.
2. В списке ревизий объекта выберите ревизию, для которой нужно добавить описание.
3. Нажмите на кнопку **Описание**.
4. В окне **Описание ревизии объекта** введите текст описания ревизии.
По умолчанию описание ревизии объекта не заполнено.
5. Нажмите на кнопку **ОК**.

Удаление объектов

В этом разделе описано, как удалять объекты и просматривать информацию объектов после того, как они были удалены.

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователей;
- группы безопасности;
- группы администрирования.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения (см. раздел "Установка срока хранения ревизий объектов и информации об удаленных объектах" на стр. [856](#)) информации удаленных объектов такой же, как и срок хранения ревизий объектов (рекомендуемый срок 90 дней). Можно изменить время хранения только при наличии **права** на Изменение (см. раздел "Назначение прав пользователям или группам пользователей" на стр. [838](#)) для области **Удаленные объекты**.

Об удалении клиентских устройств

При удалении управляемого устройства из группы администрирования приложение перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные приложения "Лаборатории Касперского" – Агент администрирования и приложение безопасности, например Kaspersky Endpoint Security, – остаются на устройстве.

Kaspersky Security Center обрабатывает устройства из группы Нераспределенные устройства по следующим правилам:

- Если вы настроили правила перемещения устройств и устройство соответствует критериям правила перемещения, устройство автоматически перемещается в группу администрирования в соответствии с правилом.

- Устройство сохраняется в группе Нераспределенные устройства и автоматически удаляется из группы в соответствии с правилами хранения устройств.

Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования. Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

При удалении устройства с зашифрованным жестким диском данные, необходимые для расшифровки диска, также удаляются. Если вы установите флажок **Я понимаю риск и хочу удалить выбранные устройства** в окне подтверждения, которое открывается при удалении таких устройств (из группы **Нераспределенные устройства** или из группы **Управляемые устройства**), это означает, что вы знаете о последующем удалении данных.

В этом случае для расшифровки диска требуется выполнение следующих условий:

- Устройство повторно подключается к Серверу администрирования для восстановления данных, необходимых для расшифровки диска.
- Пользователь устройства помнит пароль для расшифровки.
- Приложение безопасности, которое использовалось для шифрования диска, например Kaspersky Endpoint Security для Windows, установлено на устройстве.

Если диск был зашифрован с помощью технологии Kaspersky Disk Encryption, вы также можете попробовать восстановить данные с помощью утилиты FDERT Restore <https://support.kaspersky.com/KESWin/12.6/en-US/130941.htm>.

При удалении устройства из группы Нераспределенные устройства вручную приложение удаляет устройство из списка. После удаления устройства установленные приложения "Лаборатории Касперского" (если они есть) остаются на устройстве. Затем, если устройство по-прежнему видно Серверу администрирования и вы настроили регулярный опрос сети (см. раздел "Обнаружение устройств" на стр. [324](#)), Kaspersky Security Center Linux обнаружит устройство во время опроса сети и снова добавит его в группу Нераспределенные устройства. Поэтому удалять устройство вручную целесообразно только в том случае, если оно невидимо для Сервера администрирования.

См. также:

Удаление объекта [859](#)

Удаление объекта

Вы можете удалять объекты, такие как политики, задачи, инсталляционные пакеты, внутренних пользователей и внутренние группы безопасности, если у вас есть права на изменение для категории Базовая функциональность (подробную информацию см. в разделе Назначение прав пользователям и группам пользователей (см. раздел "Назначение прав пользователям или группам пользователей" на стр. [838](#))).

► Чтобы удалить объект:

1. В рабочей области требуемой папки дерева консоли выберите объект.
2. Выполните одно из следующих действий:
 - В контекстном меню объекта выберите пункт **Удалить**.
 - Нажмите на кнопку **DELETE**.

Объект будет удален, и информация об этом будет записана в базу данных.

См. также:

Удаление объектов [858](#)

Просмотр информации об удаленных объектах

Информация об удаленных объектах хранится в папке **Удаленные объекты** такой же срок, как и ревизии объекта (рекомендуемый срок составляет 90 дней).

Только пользователи с правами на **Чтение** для области **Удаленные объекты** могут просматривать список удаленных объектов (подобную информацию см. в разделе **Назначение прав пользователям и группам пользователей** (см. раздел "Назначение прав пользователям или группам пользователей" на стр. [838](#))).

► Чтобы просмотреть список удаленных объектов,

В дереве консоли выберите пункт **Удаленные объекты** (по умолчанию папка **Удаленные объекты** вложена в папку **Дополнительно**).

Если у вас нет прав на чтение для области **Удаленные объекты**, в папке **Удаленные объекты** будет отображаться пустой список.

В рабочей области папки **Удаленные объекты** содержится следующая информация об удаленных объектах:

- **Название.** Название удаленного объекта.
- **Тип.** Тип объекта, такой как политика, задача или инсталляционный пакет.
- **Время.** Время, когда объект был удален.
- **Пользователь.** Учетная запись пользователя, который удалил объект.

► Чтобы просмотреть больше информации об удаленном объекте:

1. В дереве консоли выберите пункт **Удаленные объекты** (по умолчанию папка **Удаленные объекты** вложена в папку **Дополнительно**).
2. В рабочей области папки **Удаленные объекты** выберите нужный объект.

В правой части рабочей области отобразится поле для работы с выбранным

объектом.

3. Выполните одно из следующих действий:

- Перейдите по ссылке **Свойства** в блоке работы с выбранным объектом.
- В контекстном меню объекта выберите пункт **Свойства**.

Откроется окно свойств объекта, в котором отображается следующая информация:

- **Общие**
- **История ревизий** (см. раздел "**Работа с ревизиями объектов**" на стр. [852](#))

Удаление объектов из списка удаленных объектов

Только пользователи с правами **Изменение** для области **Удаленные объекты** могут удалять объекты из списка удаленных объектов (подобную информацию см. в разделе **Назначение прав пользователям и группам пользователей** (см. раздел "**Назначение прав пользователям или группам пользователей**" на стр. [838](#))).

► *Чтобы удалить объект из списка удаленных объектов:*

1. В дереве консоли выберите узел нужного Сервера администрирования и выберите папку **Удаленные объекты**.
2. В рабочей области папки выберите объект или объекты, которые вы хотите удалить.
3. Выполните одно из следующих действий:
 - Нажмите на кнопку **DELETE**.
 - В контекстном меню объекта или объектов, которые вы выбрали, выберите пункт **Удалить**.
4. В диалоговом окне нажмите на кнопку **Да**.

Объект удален из списка удаленных объектов. Вся информация объекта (включая все ревизии) удалена из базы данных. Вы не можете восстановить эту информацию.

Хранилища данных

Этот раздел содержит информацию о данных, которые хранятся на Сервере администрирования и используются для отслеживания состояния клиентских устройств и для их обслуживания.

Данные, которые используются для отслеживания состояния клиентских устройств и их обслуживания, отображаются в папке дерева консоли **Хранилища**.

Папка **Хранилища** содержит следующие объекты:

- загруженные Сервером администрирования обновления, которые распространяются на клиентские устройства (см. раздел "**Просмотр полученных обновлений**" на стр. [482](#));
- список оборудования, обнаруженного в сети;
- лицензионные ключи, обнаруженные на клиентских устройствах (см. раздел "**Приложения "Лаборатории Касперского": лицензирование и активация**" на стр. [388](#));
- файлы, помещенные приложениями безопасности в карантинные папки на устройствах;
- файлы, помещенные в резервные хранилища клиентских устройств;

- файлы, для которых приложения безопасности определили необходимость отложенной проверки.

Экспорт списка объектов, находящихся в хранилище, в текстовый файл

Вы можете экспортировать в текстовый файл список объектов, находящихся в хранилище.

► Чтобы экспортировать в текстовый файл список объектов, находящихся в хранилище:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку нужного вам хранилища.
2. В контекстном меню списка объектов хранилища выберите пункт **Экспортировать список**.

В результате откроется окно **Экспорт списка**, в котором вы можете указать имя текстового файла и адрес папки, в которую он будет помещен.

Инсталляционные пакеты

Kaspersky Security Center помещает в хранилища данных инсталляционные пакеты приложений "Лаборатории Касперского" и приложений сторонних производителей.

Инсталляционный пакет представляет собой набор файлов, необходимых для установки приложения. Инсталляционный пакет содержит параметры процесса установки и первоначальной конфигурации устанавливаемого приложения.

Если вы хотите установить какое-либо приложение на клиентское устройство, для этого приложения необходимо создать инсталляционный пакет (см. раздел "Создание инсталляционных пакетов приложений" на стр. [850](#)) или использовать уже созданный инсталляционный пакет. Список созданных инсталляционных пакетов содержится в папке дерева консоли **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**.

См. также:

Работа с инсталляционными пакетами[371](#)

Основные статусы файлов в хранилище

Приложения безопасности проверяют файлы на устройствах на наличие известных вирусов и других приложений, представляющих угрозу, присваивают статусы файлам и помещают некоторые файлы в хранилище.

Например, приложения безопасности могут:

- сохранять в хранилище копию файла перед удалением;
- изолировать в хранилище возможно зараженные файлы.

Основные статусы файлов приведены в таблице ниже. Вы можете получить более подробную информацию о действиях с файлами в справках приложений безопасности.

Таблица 75. Статусы файлов в хранилище

Название статуса	Описание статуса
Заражен	В файле найден участок кода известного вируса или другой представляющей угрозу приложению, информация о котором содержится в антивирусных базах "Лаборатории Касперского".
Не заражен	В файле не обнаружено известных вирусов или других вредоносных приложений, представляющих угрозу.
Предупреждение.	В файле содержится участок кода, частично совпадающий с контрольным участком кода известной угрозы.
Возможно зараженный	В файле содержится либо модифицированный код известного вируса, либо код, напоминающий вирус, пока не известный "Лаборатории Касперского".
Помещен в папку пользователем	Пользователь самостоятельно поместил файл в хранилище, например, поведение файла давало основание подозревать в нем наличие угрозы. Пользователь может проверить файл на наличие в нем угроз с помощью обновленных баз.
Ложное срабатывание	Приложение "Лаборатории Касперского" присвоило статус незараженному файлу как зараженному ввиду того, что его код напоминает код вируса. После проверки с применением обновленных баз файл определяется как незараженный.
Вылечен	Файл удалось вылечить.
Удален	Файл удален в результате обработки.
Защищен паролем	Файл не может быть обработан по причине того, что он защищен паролем.

См. также:

Значки статусов файлов в Консоли администрирования [937](#)

Срабатывание правил в режиме Интеллектуального обучения

В этом разделе представлена информация об обнаружениях, выполненных правилами Адаптивного контроля аномалий Kaspersky Endpoint Security для Windows на клиентских устройствах.

Правила обнаруживают аномальное поведение на клиентских устройствах и могут блокировать его. Если правила работают в режиме Интеллектуального обучения, они обнаруживают аномальное поведение и отправляют отчеты о каждом таком случае на Сервер администрирования Kaspersky Security Center. Эта информация хранится в виде списка в папке **Правила срабатываний в статусе Интеллектуальное обучение**, вложенной в папку **Хранилища**. Вы можете подтвердить обнаружение как корректное (см. раздел "Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий" на стр. [864](#)) или добавить его в исключения (см. раздел "Добавление исключений в правила Адаптивного контроля аномалий" на стр. [866](#)), после чего такой тип поведения не будет считаться аномальным.

Информация об обнаружениях хранится в журнале событий на Сервере администрирования (вместе с остальными событиями) и в отчете Адаптивный контроль аномалий.

Подробная информация об Адаптивном контроле аномалий, его правилах, их режимах и статусах приведена в справке Kaspersky Endpoint Security для Windows.

В этом разделе

Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий	864
Добавление исключений в правила Адаптивного контроля аномалий.....	866

Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий

► Чтобы просмотреть список обнаружений, выполненных с помощью правил Адаптивного контроля аномалий:

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. Выберите подпапку **Правила срабатываний в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).

В списке отображается следующая информация об обнаружении, выполняемая с помощью правил Адаптивного контроля аномалий:

- **Группа администрирования**

Имя группы администрирования, в которую включено устройство.

- **Имя устройства**

Имя клиентского устройства, на котором было применено правило.

- **Имя**

Имя правила, которое было применено.

- **Статус**

Исключение – если администратор обработал это обнаружение и добавил его как исключение из правил. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

Подтверждение – если администратор обработал это обнаружение и подтвердил его. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

Пусто – если администратор не обработал обнаружение.

- **Количество срабатываний для всех правил**

Количество обнаружений одного эвристического правила, одного процесса и одного клиентского устройства. Это количество рассчитано Kaspersky Endpoint Security.

- **Имя пользователя**

Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

- **Путь исходного процесса**

Путь к исходному процессу, то есть к процессу, выполнившему действие (подобную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного процесса**

Хеш SHA256 исходного файла процесса (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь исходного объекта**

Путь к объекту, который запустил процесс (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного объекта**

Хеш SHA256 исходного файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого процесса**

Путь к целевому процессу (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого процесса**

Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого объекта**

Путь к целевому объекту (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого объекта**

Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Обработан**

Дата обнаружения аномалии.

► *Чтобы просмотреть свойства каждого элемента:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. Выберите подпапку **Правила срабатываний в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).
3. В рабочей области папки **Правила срабатываний в статусе Интеллектуальное обучение** выберите нужный объект.
4. Выполните одно из следующих действий:
 - Перейдите по ссылке **Свойства** в рабочей области в правой части экрана.
 - В контекстном меню объекта выберите пункт **Свойства**.

В открывшемся окне свойства объекта отображается информация объекта.

Вы можете подтвердить или добавить в исключения (см. раздел "Срабатывание правил в режиме Интеллектуального обучения" на стр. [863](#)) любой объект в списке, обнаруженный правилами Адаптивного контроля аномалий.

► *Чтобы подтвердить объект,*

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Подтвердить**.

Статус элементов будет изменен на **Подтверждение**.

Ваше подтверждение влияет на статистику, используемую правилами (подробную информацию см. в справке Kaspersky Endpoint Security 11 для Windows).

► *Чтобы добавить объект в исключения,*

В контекстном меню объекта (или нескольких объектов) списка обнаружений выберите пункт **Добавить в исключения**.

В результате запустится мастер добавления исключений (см. раздел "Добавление исключений в правила Адаптивного контроля аномалий" на стр. [866](#)). Следуйте инструкциям мастера.

Если вы отклоните или подтвердите объект, он будет исключен из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования и больше не будет отображаться в списке.

Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления исключений позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security.

Вы можете запустить мастер с помощью одного из способов ниже.

► *Чтобы запустить мастер добавления исключений в папке Адаптивный контроль аномалий:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. Выберите подпапку **Правила срабатываний в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).
3. В рабочей области в списке обнаружений в контекстном меню объекта (или нескольких объектов) выберите пункт **Добавить в исключения**.

За один раз можно добавить до 1000 исключений. Если вы выберете больше элементов и попытаетесь добавить их в исключения, появится сообщение об ошибке.

В результате запустится мастер добавления исключений.

Чтобы запустить мастер добавления исключений из других узлов в дереве консоли:

- Откройте вкладку **События** главного окна Сервера администрирования, затем выберите **Запросы пользователей** или **Последние события**.
- В окне **Отчет о состоянии правил Адаптивного контроля аномалий** выберите столбец **Количество обнаружений**.

В этом разделе

Шаг 1. Лицензирование приложения.....	867
Шаг 2. Выбор политики (политик).....	867
Шаг 3. Обработка политики (политик).....	867

Шаг 1. Лицензирование приложения

Этот шаг можно пропустить, если у вас есть только приложения Kaspersky Endpoint Security для Windows и нет других приложений, поддерживающих правила Адаптивного контроля аномалий.

Мастер добавления исключений отображает список приложений "Лаборатории Касперского", для которых плагины управления позволяют добавлять исключения к политикам для этих приложений. Выберите приложение из списка и нажмите на кнопку **Далее**, чтобы продолжить выбор политики, для которой будет добавлено исключение.

Шаг 2. Выбор политики (политик)

Мастер отображает список политик (с профилями политик) для Kaspersky Endpoint Security.

Выберите все политики и профили политик, в которые вы хотите добавить исключения, и нажмите на кнопку **Далее**.

Шаг 3. Обработка политики (политик)

Мастер отображает ход обработки политики. Вы можете прервать обработку политики, нажав на кнопку **Отмена**.

Унаследованные политики не могут быть обновлены. Если у вас нет прав на изменение политики, такая политика также не будет обновлена.

Когда все политики обработаны (или обработка политик прервана), создается отчет. Отчет отображает, какие политики были успешно обновлены (зеленый значок), а какие политики не были обновлены (красный значок).

Это последний шаг мастера. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Карантин и резервное хранилище

Антивирусные приложения "Лаборатории Касперского", установленные на клиентских устройствах, в процессе проверки устройств могут помещать файлы на карантин или в резервное хранилище.

Карантин – это специальное хранилище, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения.

Резервное хранилище предназначено для хранения резервных копий файлов, которые были удалены или изменены в процессе лечения.

Kaspersky Security Center формирует общий список файлов, помещенных на карантин и в резервное хранилище приложениями "Лаборатории Касперского" на устройствах. Агенты администрирования клиентских устройств передают информацию о файлах на карантине и в резервных хранилищах на Сервер администрирования. Через Консоль администрирования можно просматривать свойства файлов, находящихся в хранилищах на устройствах, запускать проверку вредоносного ПО хранилищ и удалять из них файлы. Значки статусов файлов описаны в приложении (см. раздел "Значки статусов файлов в Консоли администрирования" на стр. [937](#)).

Работа с карантин и резервным хранилищем доступна для Антивируса Касперского для Windows Workstations и Антивируса Касперского для Windows Servers версий 6.0 и выше, а также для Kaspersky Endpoint Security 10 для Windows и выше.

Kaspersky Security Center не копирует файлы из хранилищ на Сервер администрирования. Все файлы размещаются в хранилищах на устройствах. Восстановление файлов выполняется на устройстве, где установлено приложение безопасности, поместившая файл в хранилище.

В этом разделе

Включение удаленного управления файлами в хранилищах.....	868
Просмотр свойств файла, помещенного в хранилище	869
Удаление файлов из хранилища.....	869
Восстановление файлов из хранилища	869
Сохранение файла из хранилища на диск	869
Сканирование файлов, находящихся на карантине	870

Включение удаленного управления файлами в хранилищах

По умолчанию удаленное управление файлами в хранилищах на клиентских устройствах отключено.

► Чтобы включить удаленное управление файлами в хранилищах на клиентских устройствах:

1. В дереве консоли выберите группу администрирования, для которой требуется включить удаленное управление файлами хранилищ.
2. В рабочей области группы откройте вкладку **Политики**.
3. На вкладке **Политики** выберите политику приложения безопасности, помещающей файлы в хранилища на устройствах.
4. В окне свойств политики в блоке **Информировать Сервер администрирования** установите флажки, соответствующие хранилищам, для которых вы хотите включить удаленное управление.

Расположение блока **Информировать Сервер администрирования** в окне свойств политики и названия флажков в блоке индивидуальны для каждого приложения безопасности.

Просмотр свойств файла, помещенного в хранилище

► Чтобы просмотреть свойства файла, помещенного на карантин или в резервное хранилище:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин (Резервное хранилище)** выберите файл, параметры которого требуется просмотреть.
3. В контекстном меню файла выберите пункт **Свойства**.

Удаление файлов из хранилища

► Чтобы удалить файл, помещенный на карантин или в резервное хранилище:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин (или Резервное хранилище)** с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется удалить.
3. Удалите файлы одним из следующих способов:
 - В контекстном меню файлов выберите пункт **Удалить**.
 - По ссылке **Удалить (Удалить)** при удалении одного файла в блоке работы с выбранными файлами.

В результате приложения безопасности, поместившие выбранные файлы в хранилища на клиентских устройствах, удалят файлы из этих хранилищ.

Восстановление файлов из хранилища

► Чтобы восстановить файл из карантина или резервного хранилища:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин (Резервное хранилище)** с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется восстановить.
3. Запустите процесс восстановления файлов одним из следующих способов:
 - В контекстном меню файлов выберите пункт **Восстановить**.
 - По ссылке **Восстановить** в блоке работы с выбранными файлами.

В результате приложения безопасности, поместившие файлы в хранилища на клиентских устройствах, восстановят файлы в исходные папки.

Сохранение файла из хранилища на диск

Kaspersky Security Center позволяет сохранять на диск копии файлов, помещенных приложением безопасности на карантин или в резервное хранилище на клиентском устройстве. Файлы копируются на устройство, на котором установлен Kaspersky Security Center, в указанную вами папку.

► Чтобы сохранить копию файла из карантина или резервного хранилища на жесткий диск:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин (Резервное хранилище)** выберите файл, который требуется скопировать на жесткий диск.
3. Запустите процесс копирования файла одним из следующих способов:
 - В контекстном меню файла выберите пункт **Сохранить на диск**.
 - В блоке работы с выбранным файлом нажмите на ссылку **Сохранить на диск**.

В результате приложение безопасности, поместившее файл на карантин на клиентском устройстве, сохранит копию файла в указанную папку.

Сканирование файлов, находящихся на карантине

► Чтобы проверить файлы, находящиеся на карантине:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин**.
2. В рабочей области папки **Карантин** с помощью клавиш **SHIFT** и **CTRL** выберите файлы, которые требуется проверить.
3. Запустите процесс проверки файлов одним из следующих способов:
 - В контекстном меню файла выберите пункт **Проверить**.
 - По ссылке **Проверить** в блоке работы с выбранными файлами.

Приложение запускает задачу проверки по требованию для приложений безопасности, которые поместили выбранные файлы на карантин, на устройствах, где хранятся эти файлы.

Активные угрозы

Информация о необработанных файлах, обнаруженных на клиентских устройствах, содержится в папке **Хранилища**, во вложенной папке **Активные угрозы**.

Отложенная обработка и дезинфекция выполняются приложением безопасности по запросу или после определенного события. Вы можете настраивать параметры отложенного лечения файлов.

В этом разделе

Дезинфекция необработанного файла	870
Сохранение необработанного файла на диск	871
Удаление файлов из папки "Активные угрозы"	871

Дезинфекция необработанного файла

► Чтобы запустить лечение необработанного файла:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Активные угрозы**.

2. В рабочей области папки **Активные угрозы** выберите файл, который требуется вылечить.
3. Запустите процесс лечения файла одним из следующих способов:
 - В контекстном меню файла выберите пункт **Лечить**.
 - По ссылке **Лечить** в блоке работы с выбранным файлом.

В результате выполняется попытка лечения файла.

Если файл вылечен, приложение безопасности, установленное на клиентском устройстве, восстанавливает его в исходную папку. Запись о файле удаляется из списка папки **Активные угрозы**. Если лечение файла невозможно, приложение безопасности, установленное на устройстве, удаляет файл с устройства. Запись о файле удаляется из списка папки **Активные угрозы**.

Возможности лечения и удаления файлов могут различаться в зависимости от установленного приложения безопасности, его версии и параметров.

Сохранение необработанного файла на диск

Kaspersky Security Center позволяет сохранять на диск копии необработанных файлов, обнаруженные на клиентских устройствах. Файлы копируются на устройство, на котором установлен Kaspersky Security Center, в указанную вами папку.

Вы можете сохранить только копии файлов, которые были удалены или изменены в процессе лечения, если эти копии хранятся в хранилище <https://support.kaspersky.com/KESWin/12.6/en-US/178491.htm> Kaspersky Endpoint Security для Windows на управляемом устройстве.

► Чтобы сохранить копию необработанного файла на диск:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Активные угрозы**.
2. В рабочей области папки **Активные угрозы** выберите файлы, которые требуется скопировать на диск.
3. Запустите процесс копирования файла одним из следующих способов:
 - В контекстном меню файла выберите пункт **Сохранить на диск**.
 - В блоке работы с выбранным файлом нажмите на ссылку **Сохранить на диск**.

В результате приложение безопасности клиентского устройства, на котором обнаружен выбранный необработанный файл, сохранит копию файла в указанную папку.

Удаление файлов из папки "Активные угрозы"

► Чтобы удалить файл из папки **Активные угрозы**:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Активные угрозы**.
2. В рабочей области папки **Активные угрозы** с помощью клавиш **SHIFT** и **CTRL** выберите файлы, которые требуется удалить.

3. Удалите файлы одним из следующих способов:

- В контекстном меню файлов выберите пункт **Удалить**.
- По ссылке **Удалить (Удалить)** при удалении одного файла в блоке работы с выбранными файлами.

В результате приложения безопасности, поместившие выбранные файлы в хранилища на клиентских устройствах, удаляют файлы из этих хранилищ. Записи о файлах удаляются из списка в папке **Активные угрозы**.

Kaspersky Security Network и Kaspersky Private Security Network

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN) и Kaspersky Private Security Network (KPSN). Приведена информация о KSN и KPSN, а также инструкции по включению KPSN, настройке доступа к KPSN, по просмотру статистики использования прокси-сервера KSN.

В этом разделе

О KSN и KPSN	873
Настройка доступа к KPSN	874
Включение и отключение KPSN	875
Просмотр принятого Положения о KSN	876
Просмотр статистики прокси-сервера KSN	876
Принятие обновленного Положения о KSN	877
Enhanced protection with Kaspersky Security Network	878
Проверка, работает ли точка распространения как прокси-сервер KSN	878

О KSN и KPSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о приложениях, установленных на клиентских устройствах.

Участвуя в KSN, вы в соответствии с Положением о KSN соглашаетесь в автоматическом режиме передавать в "Лабораторию Касперского" информацию о работе приложений "Лаборатории Касперского", установленных на клиентских устройствах под управлением Kaspersky Security Center. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN (см. раздел "Настройка доступа к KPSN" на стр. [874](#)).

Приложение предлагает присоединиться к KSN во время установки приложения и во время работы мастера первоначальной настройки. Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с приложением (см. раздел "Включение и отключение KPSN" на стр. [875](#)).

Использование Kaspersky Security Network приводит к выходу приложения из сертифицированного состояния. Необходимо использовать Kaspersky Private Security Network или отказаться от использования KSN.

Вы можете использовать Kaspersky Private Security Network (далее также KPSN) вместо Kaspersky Security Network, чтобы не использовать отправку данных вашей организации за пределы локальной сети организации.

Kaspersky Private Security Network (KPSN) – это решение, позволяющее получать доступ к данным Kaspersky Security Network через сервер, размещенный внутри сети вашей организации. KPSN позволяет приложениям "Лаборатории Касперского" получать доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсах и программном обеспечении. KPSN не передает статистику и файлы в "Лабораторию Касперского". Для получения подробной информации см. "Kaspersky Private Security Network. Подготовительные процедуры и руководство по эксплуатации".

Служба Kaspersky Private Security Network разработана для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

- отсутствия подключения серверов к интернету;
- законодательного запрета на отправку любых данных за пределы страны;
- требований корпоративной безопасности на отправку любых данных за пределы локальной сети организации.

Клиентские устройства, находящиеся под управлением Сервера администрирования, для взаимодействия с KSN или KPSN могут использовать службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет и серверам KPSN.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования (см. раздел "Настройка доступа к KPSN" на стр. [874](#)).

Настройка доступа к KPSN

► *Чтобы настроить доступ Сервера администрирования к KPSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить доступ к KPSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите раздел **Параметры прокси-сервера KSN**.
4. Установите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы включить службу прокси-сервера KPSN.

Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

5. Снимите флажок **Я принимаю условия использования Kaspersky Security Network**.
6. Установите флажок **Настроить KPSN** и по кнопке **Выбрать файл с параметрами KSN** загрузите параметры KPSN (файлы с расширениями pkcs7, pem).

Работу с Локальным KSN поддерживают не все приложения "Лаборатории Касперского". Подробная информация приводится в Руководствах к соответствующим приложениям "Лаборатории Касперского".

Если для работы с KPSN вы используете версии приложений ниже Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2 или ниже Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, рекомендуется использовать подчиненные Серверы администрирования, для которых не настроено использование KPSN.

7. Настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:

- В поле ввода **TCP-порт** укажите номер TCP-порта, через который будет выполняться подключение к прокси-серверу KPSN. По умолчанию подключение к прокси-серверу KPSN выполняется через порт 13111.
- Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию флажок снят, подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

8. Установите флажок **Подключать подчиненные Серверы администрирования к KSN через главный Сервер**.

Если флажок установлен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KPSN. Если флажок снят, подчиненные Серверы администрирования подключаются к KPSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Прокси-сервер KSN** также установлен флажок **Использовать Сервер администрирования как прокси-сервер**.

9. Нажмите на кнопку **ОК**.

В результате параметры доступа к KPSN будут сохранены.

Включение и отключение KPSN

► Чтобы включить KPSN, выполните следующие действия:

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить KPSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервера KSN**.
4. Установите флажок **Настроить KPSN**.
5. Нажмите на кнопку **Выбрать файл с параметрами KSN** загрузите параметры KPSN (файлы с расширениями rkcs7, rem).
В результате KPSN будет включен.
6. Нажмите на кнопку **ОК**.

► Чтобы выключить KPSN, выполните следующие действия:

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервера KSN**.
4. Снимите флажок **Настроить KPSN**.
В результате KPSN будет выключен.
5. Нажмите на кнопку **ОК**.

Просмотр принятого Положения о KSN

При включении Kaspersky Security Network (KSN) вам нужно прочитать и принять Положение о KSN. Вы можете просмотреть принятое Положение о KSN в любое время.

► Чтобы просмотреть принятое Положение о KSN:

1. В дереве консоли выберите Сервер администрирования, для которого включен KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервера KSN**.
4. Перейдите по ссылке **Просмотреть принятые Положения о KSN**.

В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

Просмотр статистики прокси-сервера KSN

Прокси-сервер KSN – это служба, обеспечивающая взаимодействие между инфраструктурой Kaspersky Security Network и клиентскими устройствами, находящимися под управлением Сервера администрирования.

Использование прокси-сервера KSN предоставляет вам следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

В окне свойств Сервера администрирования вы можете настроить параметры прокси-сервера KSN и просмотреть статистическую информацию об использовании прокси-сервера KSN.

► Чтобы просмотреть статистику работы прокси-сервера KSN:

1. В дереве консоли выберите Сервер администрирования, для которого нужно просмотреть статистику KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Статистика прокси-сервера KSN**.

В этом разделе отображается фактическая статистика работы прокси-сервера KSN (количество записей в кеше, количество обработанных пакетов в кеше и полученных пакетов). Также, если Сервер администрирования подключен к KSN, отображается соответствующее информационное сообщение.

Если необходимо, выполните дополнительные действия:

- по кнопке **Обновить** обновите статистическую информацию об использовании прокси-сервера KSN;
- по кнопке **Экспортировать в файл** экспортируйте данные статистики в файл формата CSV;
- по кнопке **Проверить подключение к KSN** проверьте, подключен ли Сервер администрирования к KSN в настоящий момент.

4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN (см. раздел "Просмотр принятого Положения о KSN" см. стр. [876](#)), которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования или при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с версией Положения о KSN, которую вы приняли ранее.

После обновления Сервера администрирования или после обновления с предыдущей версии Сервера администрирования, обновленное Положение о KSN отображается автоматически. Если вы отклоните обновленное Положение о KSN, вы все равно сможете просмотреть и принять его позже.

► *Чтобы просмотреть и принять или отклонить обновленное Положение о KSN:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. На вкладке **Мониторинг** в разделе **Мониторинг** перейдите по ссылке **Принятое Положение о Kaspersky Security Network устарело**.
Откроется окно **Положение о KSN**.
3. Внимательно прочтите Положение о KSN, а затем примите решение. Если вы принимаете условия обновленного Положения о KSN, нажмите на кнопку **Я принимаю условия Лицензионного соглашения**. Если вы отклоняете условия обновленного Положения о KSN, нажмите на кнопку **Отмена**.

В зависимости от вашего выбора KSN продолжит работу в соответствии с условиями текущего или обновленного Положения о KSN. Вы можете в любой момент просмотреть текст принятого Положения о KSN (см. раздел "Просмотр принятого Положения о KSN" см. стр. [876](#)) в свойствах Сервера администрирования.

Дополнительная защита с использованием Kaspersky Security Network

"Лаборатория Касперского" предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков "Лаборатории Касперского" обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте "Лаборатории Касперского".

Проверка, работает ли точка распространения как прокси-сервер KSN

На управляемом устройстве, которое выполняет роль точки распространения, вы можете включить прокси-сервер KSN. Управляемое устройство работает как прокси-сервер KSN, если на нем запущена служба ksnproxy. Вы можете проверить включить или выключить эту службу на устройстве локально.

Вы можете назначить устройство с операционной системой Windows или Linux в качестве точки распространения. Способ проверки точки распространения зависит от операционной системы этой точки распространения.

► *Чтобы проверить, работает ли точка распространения с операционной системой Windows как прокси-сервер KSN:*

1. На устройстве, которое выполняет роль точки распространения, в Windows откройте окно **Службы (Все приложения → Администрирование → Службы)**.
2. В списке служб проверьте, запущена ли служба прокси-сервера KSN – ksnproxy.

Если служба ksnproxy запущена, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN Proxy для управляемых устройств, входящих в область действия точки распространения.

При необходимости службу ksnproxy можно выключить. В этом случае Агент администрирования на точке распространения больше не участвует в Kaspersky Security Network. Для этого требуются права локального администратора.

► *Чтобы проверить, работает ли точка распространения с операционной системой Linux как прокси-сервер KSN:*

1. На устройстве, выполняющем роль точки распространения, отобразится список запущенных процессов.
2. В списке запущенных процессов проверьте запущен ли процесс `/opt/kaspersky/ksc64/sbin/ksnproxy`.

Если процесс `/opt/kaspersky/ksc64/sbin/ksnproxy` запущен, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN для управляемых устройств, входящих в область действия точки распространения.

Переключение между онлайн-справкой и офлайн-справкой

Если у вас нет доступа в интернет, вы можете использовать офлайн-справку.

► Чтобы переключиться между онлайн-справкой и офлайн-справкой:

1. В главном окне приложения Kaspersky Security Center выберите в дереве консоли узел **Kaspersky Security Center**.
2. Перейдите по ссылке **Параметры общего интерфейса**.
Откроется окно параметров.
3. В окне свойств нажмите на ссылку **Использовать офлайн-справку**.
4. Нажмите на кнопку **ОК**.

Параметры применены и сохранены. Вы можете в любой момент изменить параметры и начать пользоваться онлайн-справкой в любое время.

Экспорт событий в SIEM-системы

В этом разделе описана процедура экспорта событий, зарегистрированных в Kaspersky Security Center, во внешние системы управления событиями информационной безопасности (SIEM-системы, Security Information and Event Management).

См. также:

События компонентов Kaspersky Security Center	636
Лицензии и возможности Kaspersky Security Center	29
Сценарий: мониторинг и отчеты.....	593

Сценарий: настройка экспорта событий в SIEM-системы

Kaspersky Security Center позволяет выполнять настройку одним из способов: экспорт в любую SIEM-систему, использующую формат Syslog, экспорт в QRadar, Splunk, ArcSight SIEM-системы, использующие форматы LEEF и CEF, или экспорт событий в SIEM-системы прямо из базы Kaspersky Security Center. По завершении этого сценария Сервер администрирования автоматически отправляет события в SIEM-систему.

Предварительные требования

Перед началом настройки экспорта событий в Kaspersky Security Center:

- Узнайте больше о методах экспорта событий (см. раздел "Об экспорте событий" на стр. [883](#)).
- Убедитесь, что у вас есть значения системных параметров (см. раздел "Предварительные условия" на стр. [881](#)).

Вы можете выполнять шаги этого сценария в любом порядке.

Процесс экспорта событий в SIEM-систему состоит из следующих шагов:

- Настройка SIEM-системы для получения событий из Kaspersky Security Center

Инструкции: Настройка экспорта событий в SIEM-системе (см. раздел "О настройке экспорта событий в SIEM-системе" на стр. [884](#)).

- Выбор события, которые вы хотите экспортировать в SIEM-систему:

Инструкции:

- Консоль администрирования: Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog (на стр. [886](#)), Выбор общих событий для экспорта в формате Syslog (на стр. [889](#)).
- Kaspersky Security Center Web Console: Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog, Выбор общих событий для экспорта в формате Syslog.
- Настройка экспорта событий в SIEM-систему одним из следующих способов:

- Укажите протоколы TCP/IP, UDP или TLS over TCP.

Инструкции:

- Консоль администрирования: Настройка экспорта событий в SIEM-системы (см. раздел "Настройка Kaspersky Security Center для экспорта событий в SIEM-систему" на стр. [892](#)).
- Kaspersky Security Center Web Console: Настройка экспорта событий в SIEM-системы.
- Использование экспорта событий напрямую из базы данных Kaspersky Security Center (см. раздел "Экспорт событий напрямую из базы данных" на стр. [894](#)). В базе данных Kaspersky Security Center представлен набор публичных представлений; вы можете найти описание этих общедоступных представлений в документе `klakdb.chm`.

Результаты

После настройки экспорта событий в SIEM-систему вы можете просматривать результаты экспорта (см. раздел "Просмотр результатов экспорта" на стр. [899](#)), если вы выбрали события, которые хотите экспортировать.

См. также:

Об экспорте событий	883
Предварительные условия	881
О событиях в Kaspersky Security Center	881
О настройке экспорта событий в SIEM-системе	884
Экспорт событий напрямую из базы данных	894
Просмотр результатов экспорта.....	899

Предварительные условия

При настройке автоматического экспорта событий в Kaspersky Security Center необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

- **Протокол**

Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы	879

О событиях в Kaspersky Security Center

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Вы можете экспортировать эту информацию во внешние SIEM-системы (см.

раздел "Сценарий: настройка экспорта событий в SIEM-системы" см. стр. [879](#)). Экспорт информации о событиях во внешние SIEM-системы позволяет администраторам SIEM-систем оперативно реагировать на события системы безопасности, произошедшие на управляемых устройствах или группах администрирования.

Типы событий

В Kaspersky Security Center существуют следующие типы уведомлений:

- Общие события. Эти события возникают во всех управляемых приложениях "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- Специфические события управляемых приложений "Лаборатории Касперского". Каждое управляемое приложение "Лаборатории Касперского" имеет собственный набор событий.

Источники событий

События могут генерироваться следующими приложениями:

- Компонентами приложения Kaspersky Security Center:
 - Сервер администрирования (см. раздел "События Сервера администрирования" см. стр. [638](#))
 - Агент администрирования (см. раздел "События Агента администрирования" см. стр. [669](#))
 - Сервер iOS MDM
- Управляемые приложения "Лаборатории Касперского"

Подробнее о событиях, генерируемых управляемыми приложениями "Лаборатории Касперского", см. в документации соответствующего приложения.

Просмотреть полный список событий, которые может генерировать приложение, можно на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

Уровень важности события

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы приложения или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа приложения может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе приложения или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

См. также:

События компонентов Kaspersky Security Center	636
Сценарий: настройка экспорта событий в SIEM-системы	879
Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog ...	886
Выбор общих событий для экспорта в формате Syslog.....	889

Об экспорте событий

Вы можете использовать экспорт событий в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ предупреждений систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться в панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Консоли администрирования Kaspersky Security Center. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Kaspersky Security Center, а затем получение событий в SIEM-системе, либо наоборот.

Способы отправки событий из Kaspersky Security Center

Существует три способа отправки событий из Kaspersky Security Center во внешние системы:

- Отправка событий по протоколу Syslog в любую SIEM-систему.

По протоколу Syslog можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. Протокол Syslog – это стандартный протокол регистрации сообщений. Вы можете использовать этот протокол для экспорта событий в любую SIEM-систему.

Для этого нужно отметить события, которые вы хотите передать в SIEM-систему. Вы можете отметить события с помощью Консоли администрирования (см. раздел "Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog" см. стр. [886](#)) или Kaspersky Security Center Web Console). Только отмеченные события будут передаваться в SIEM-систему. Если вы ничего не отметили, никакие события не будут передаваться.

- Отправка событий по протоколам CEF и LEEF в системы QRadar, Splunk и ArcSight.

Протоколы CEF и LEEF можно использовать для экспорта общих событий (см. раздел "О событиях в Kaspersky Security Center" на стр. [881](#)). При экспорте событий по протоколам CEF и LEEF у вас нет возможности выбора определенных экспортируемых событий. Вместо этого выполняется экспорт всех общих событий. В отличие от протокола Syslog, протоколы CEF и LEEF не являются универсальными. Протоколы CEF и LEEF предназначены для соответствующих SIEM-систем (QRadar, Splunk и ArcSight). Поэтому при выборе экспорта событий по одному из этих протоколов в SIEM-системе используется нужный анализатор.

- Напрямую из базы данных Kaspersky Security Center в любую SIEM-систему.

Этот способ экспорта событий можно использовать для получения событий напрямую из публичных представлений базы данных с помощью SQL-запросов. Результаты выполнения запроса сохраняются в .xml файл, который можно использовать в качестве входных данных для внешней системы. Напрямую из базы данных можно экспортировать только события, доступные в публичных представлениях.

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky Security Center. Для этого необходимо выполнить настройку SIEM-системы. Конфигурация зависит от конкретной используемой SIEM-системы. Однако в конфигурациях всех SIEM-систем существует ряд общих этапов, таких как настройка приемника и анализатора.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

О настройке экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Kaspersky Security Center.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

Настройка приемника сообщений

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Kaspersky Security Center. В общем случае в SIEM-системе необходимо указать следующие параметры:

- Протокол экспорта или тип входных данных

Протокол передачи сообщений, TCP/IP или UDP. Необходимо указать тот же протокол, который был выбран в Kaspersky Security Center для передачи событий.

- **Порт**

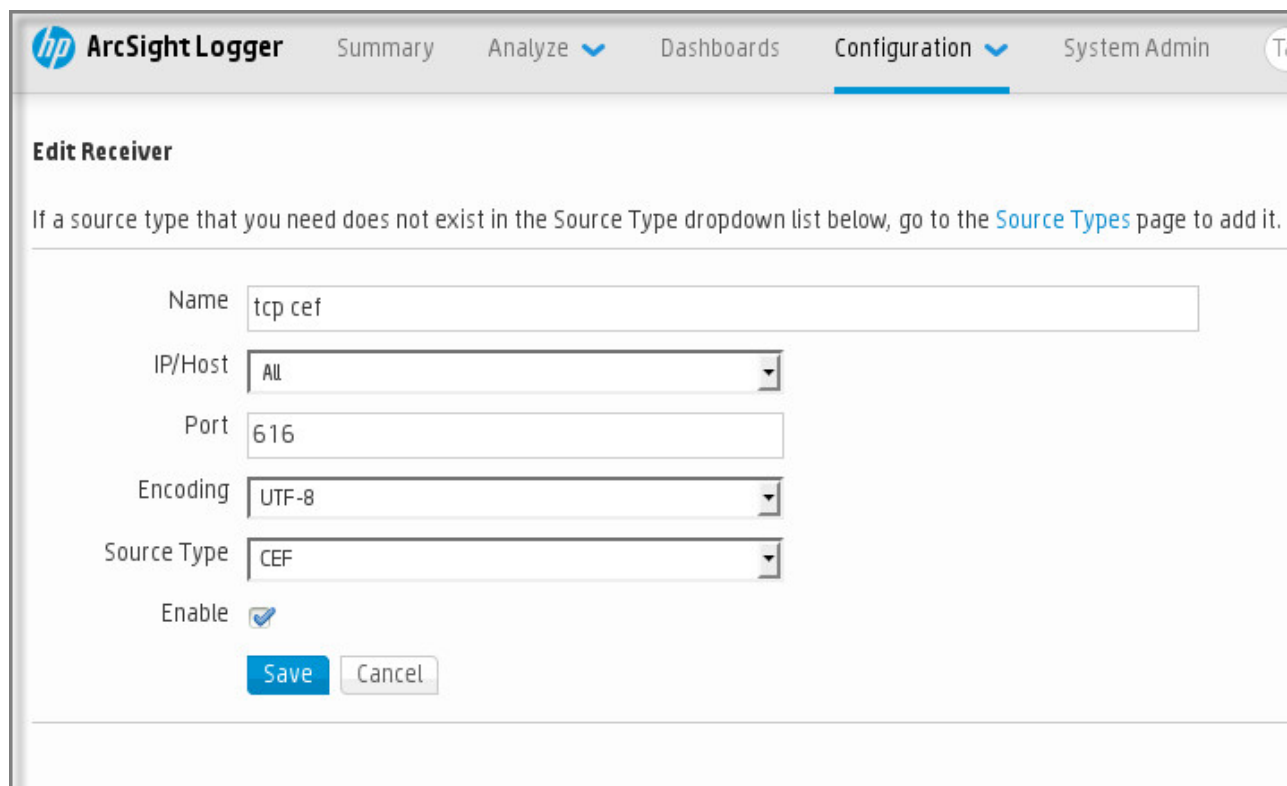
Номер порта для подключения к Kaspersky Security Center. Необходимо указать тот же номер порта, который был выбран в Kaspersky Security Center для передачи событий.

- **Протокол передачи сообщений или тип исходных данных**

Протокол, используемый для экспорта событий в SIEM-систему. Может являться одним из стандартных протоколов: Syslog, CEF или LEEF. SIEM-система выбирает анализатор событий, соответствующий указанному протоколу.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На рисунке ниже приведен пример настройки приемника в ArcSight.



The screenshot shows the 'Edit Receiver' configuration window in the ArcSight Logger interface. The window has a title bar with the ArcSight logo and navigation tabs: Summary, Analyze, Dashboards, Configuration (selected), and System Admin. Below the title bar, the 'Edit Receiver' section is active. A note states: 'If a source type that you need does not exist in the Source Type dropdown list below, go to the [Source Types](#) page to add it.' The configuration fields are as follows:

- Name:** tcp cef
- IP/Host:** All (dropdown menu)
- Port:** 616
- Encoding:** UTF-8 (dropdown menu)
- Source Type:** CEF (dropdown menu)
- Enable:** ☒

At the bottom of the form are two buttons: 'Save' (in blue) and 'Cancel' (in grey).

Рисунок 7. Пример настройки приемника сообщений

Анализатор сообщений

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, для того чтобы информация о событиях была должным образом передана в SIEM-систему. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения сообщения на поля, такие как идентификатор сообщения, уровень важности, описание, параметры.

В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky Security Center, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

Выбор событий для экспорта в SIEM-системы в формате Syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберете экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, управляемого этой политикой.

Выбор событий для управляемого приложения. Если вы выбираете экспортируемые события для управляемого приложения, установленного на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этом приложении.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

В этом разделе

Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog ... [886](#)

Выбор общих событий для экспорта в формате Syslog..... [889](#)

Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших в отдельном управляемом приложении, установленном на управляемом устройстве, выберите для приложения события для экспорта. В случае, если ранее экспортируемые события были выбраны в политике, вам не удастся переопределить выбранные события для отдельного приложения, управляемой этой политикой.

► Чтобы выбрать события для отдельного управляемого приложения:

1. В дереве консоли Kaspersky Security Center выберите узел **Управляемые устройства** и перейдите на вкладку **Устройства**.
2. Откройте контекстное меню требуемого устройства по правой клавише мыши и выберите пункт **Свойства**.
3. В открывшемся окне свойств устройства выберите раздел **Приложения**.
4. В появившемся списке приложений выберите приложение, события которой требуется экспортировать, и нажмите на кнопку **Свойства**.
5. В окне свойств приложения выберите раздел **Настройка событий**.
6. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в SIEM-систему, и нажмите на кнопку **Свойства**.
7. В открывшемся окне свойств событий выберите параметр **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отметить выбранные события для экспорта в формате Syslog. Выключите параметр **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отменить выбор событий для экспорта в формате Syslog.

Если свойства события заданы в политике, поля этого окна недоступны для редактирования.

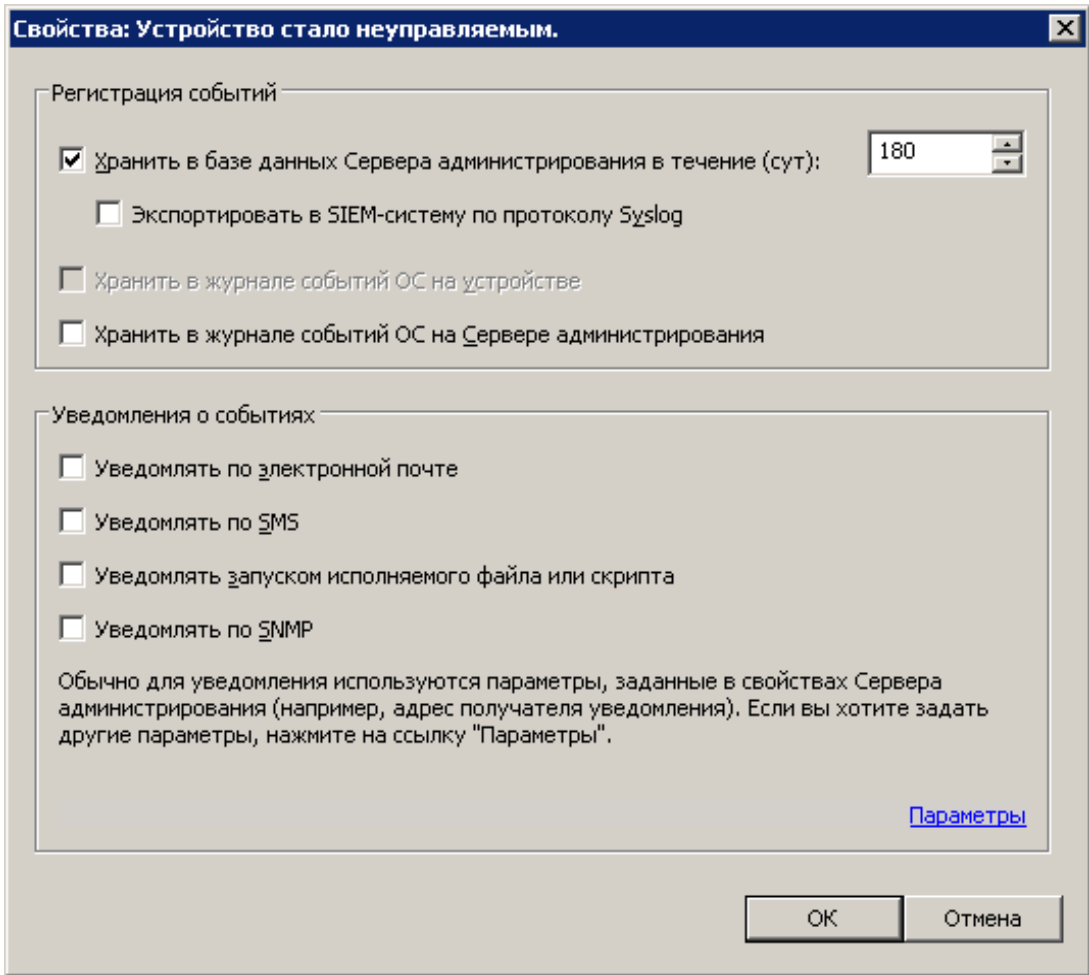


Рисунок 8. Окно свойств событий

- 8. Нажмите на кнопку **OK**, чтобы сохранить изменения.
- 9. Нажмите на кнопку **OK** в окне свойств приложения и в окне свойств устройства.

Выбранные события будут отправляться в SIEM-систему в формате Syslog. События, выбор которых вы отменили параметром **Экспортировать в SIEM-систему по протоколу Syslog**, не будут экспортироваться в SIEM-систему. Экспорт начнется сразу после того, как вы включите автоматический экспорт и выберете экспортируемые события. Выполните настройку SIEM-системы, чтобы обеспечить получение событий из Kaspersky Security Center.

См. также

Сценарий: настройка экспорта событий в SIEM-системы 879

Выбор общих событий для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших во всех приложениях, управляемых определенной политикой, выберите экспортируемые события в политике. В этом случае вы не можете выбрать события для отдельного управляемого приложения.

► *Чтобы выбрать общие события для экспорта в SIEM-систему:*

1. В дереве консоли Kaspersky Security Center выберите узел **Политики**.
2. Откройте контекстное меню требуемой политики по правой клавише мыши и выберите пункт **Свойства**.
3. В открывшемся окне свойств политики выберите раздел **Настройка событий**.
4. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в SIEM-систему, и нажмите на кнопку **Свойства**.

Если требуется выбрать все события, нажмите на кнопку **Выделить все**.

5. В открывшемся окне свойств событий выберите параметр **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отметить выбранные события для экспорта в формате Syslog.

Снимите флажок **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отменить выбор событий для экспорта в формате Syslog.

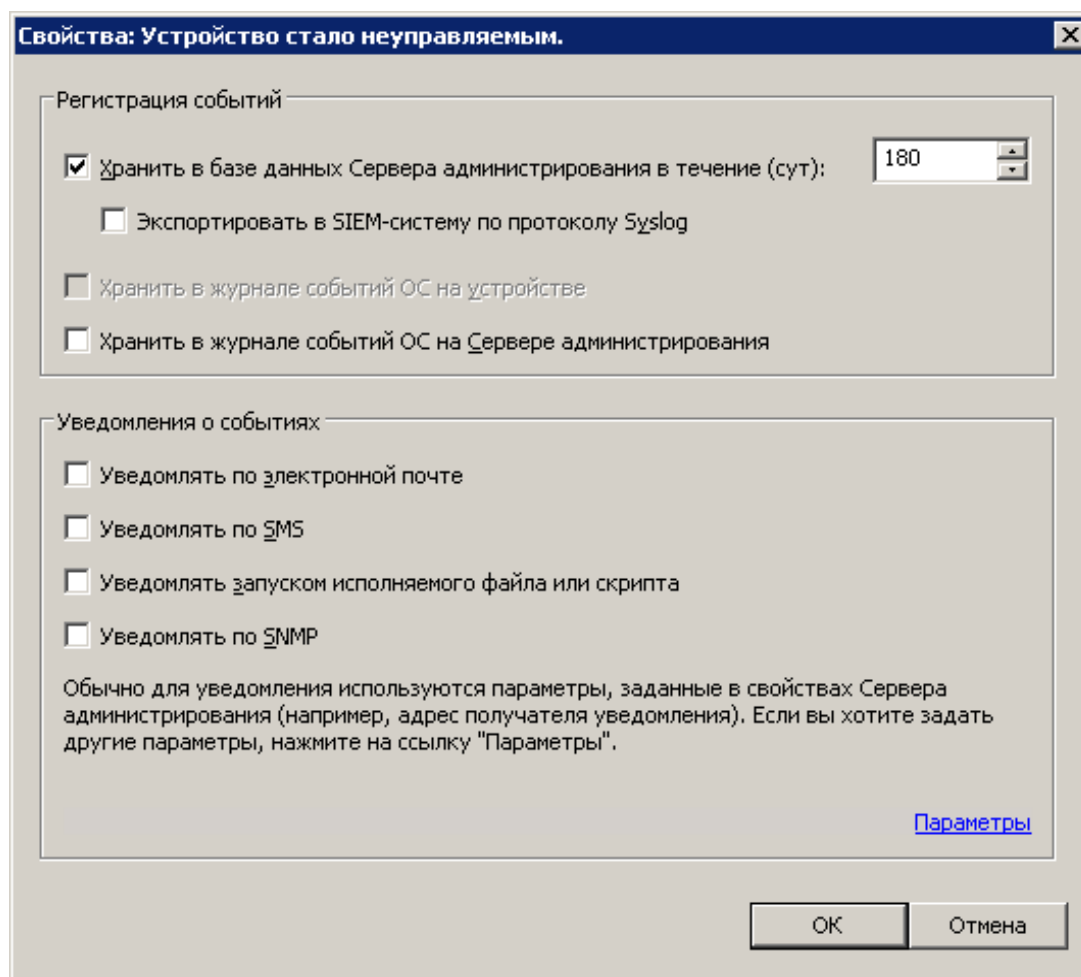


Рисунок 9. Окно свойств событий

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

7. В окне свойств политики нажмите на кнопку **ОК**.

Выбранные события будут отправляться в SIEM-систему в формате Syslog. События, выбор которых вы отменили параметром **Экспортировать в SIEM-систему по протоколу Syslog**, не будут экспортироваться в SIEM-систему. Экспорт начнется сразу после того, как вы включите автоматический экспорт и выберете экспортируемые события. Выполните настройку SIEM-системы, чтобы обеспечить получение событий из Kaspersky Security Center.

См. также

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

Об экспорте событий в формате Syslog

Используя формат Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других приложениях "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Формат Syslog определяется документами Request for Comments (RFC), опубликованными Internet Engineering Task Force. Стандарт RFC 5424 (<https://tools.ietf.org/html/rfc5424>) используется для экспорта событий из Kaspersky Security Center во внешние системы.

В Kaspersky Security Center можно настроить экспорт событий во внешние системы в формате Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Kaspersky Security Center таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky Security Center начинается сразу после включения автоматического экспорта.
2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

Об экспорте событий в форматах CEF и LEEF

Форматы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий (см. раздел "О событиях в Kaspersky Security Center" на стр. [881](#)), а также событий, переданных приложениями "Лаборатории Касперского" Серверу администрирования. Набор экспортируемых событий определен заранее, возможность выбирать экспортируемые события отсутствует.

Формат экспорта можно выбрать в зависимости от того, какую SIEM-систему вы используете. В следующей таблице приведены SIEM-системы и соответствующие им форматы экспорта.

Таблица 76. Форматы экспорта событий в SIEM-систему

SIEM-система	Формат экспорта
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) – это специализированный формат событий для IBM Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center (<https://www.ibm.com/support/knowledgecenter/>).
- CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа. Для протокола CEF должна использоваться кодировка UTF-8.

При автоматическом экспорте Kaspersky Security Center отправляет общие события в SIEM-систему. Автоматический экспорт событий начинается сразу после включения. В этом разделе описана процедура включения автоматического экспорта событий.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

Настройка Kaspersky Security Center для экспорта событий в SIEM-систему

Вы можете включить автоматический экспорт событий в Kaspersky Security Center.

Только общие события (см. раздел "О событиях в Kaspersky Security Center" на стр. [881](#)) могут быть экспортированы от управляемых приложений в форматах CEF и LEEF. Специфические события приложений (см. раздел "О событиях в Kaspersky Security Center" на стр. [881](#)) не могут быть экспортированы от управляемых приложений в форматах CEF и LEEF. Если необходимо экспортировать события управляемых приложений или пользовательский набор событий, который настроен с помощью политик управляемых приложений, используйте экспорт событий в формате Syslog.

► Чтобы включить автоматический экспорт общих событий:

1. В дереве консоли Kaspersky Security Center выберите узел с именем Сервера администрирования, события которого необходимо экспортировать.
2. В рабочей области выбранного Сервера администрирования перейдите на вкладку **События**.

3. Нажмите на стрелку рядом со ссылкой **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите пункт **Настроить экспорт в SIEM-систему**.

Откроется окно свойств событий на разделе **Экспорт событий**.

4. В разделе **Экспорт событий** укажите следующие параметры экспорта:

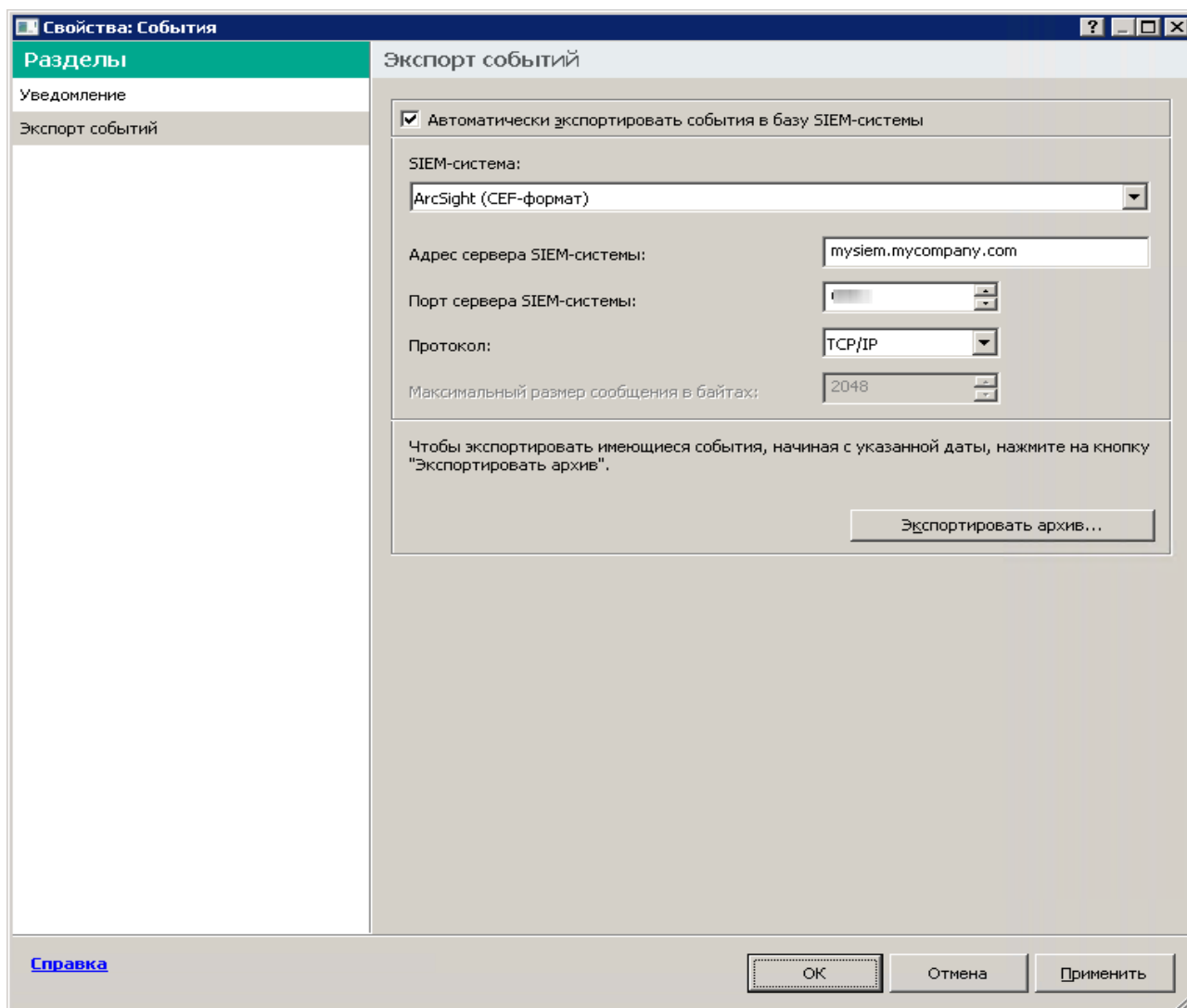


Рисунок 10. Раздел Экспорт событий

- **Автоматически экспортировать события в базу SIEM-системы**

Установите этот флажок, для того чтобы включить автоматический экспорт событий в SIEM-систему. При установке этого флажка все поля в разделе **Экспорт событий** становятся доступными для редактирования.

- **SIEM-система**

Выберите, в какую SIEM-систему будет выполняться экспорт событий: QRadar, Splunk или ArcSight.

- **Адрес сервера SIEM-системы**

Укажите адрес сервера SIEM-системы. Адрес сервера можно указать в формате DNS- или NetBIOS-имени или IP-адреса

- **Порт сервера SIEM-системы**

Укажите номер порта для соединения с сервером SIEM-системы. Этот номер порта должен совпадать с номером порта, который вы указываете в настройках приемника SIEM-системы для получения событий (см. раздел Настройка SIEM-системы).

- **Протокол**

Если вы выбрали формат Syslog, вам нужно указать:

- **Максимальный размер сообщения в байтах**

Укажите максимальный размер в байтах одного сообщения, передаваемого в SIEM-систему. Каждое событие передается одним сообщением. Если реальная длина сообщения превышает указанное значение, сообщение обрезается и данные могут быть утеряны. По умолчанию размер сообщения составляет 2048 байт. Данное поле доступно только в случае, если вы выбрали формат Syslog в поле **SIEM-система**.

5. Если требуется выполнить экспорт в SIEM-систему событий, произошедших после определенной даты в прошлом, нажмите на кнопку **Экспортировать архив** и укажите дату, начиная с которой будет выполнен экспорт событий. По умолчанию экспорт событий начинается сразу после включения.
6. Нажмите на кнопку **ОК**.

Автоматический экспорт событий включен.

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться в SIEM-систему.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы	879
Выбор событий для экспорта в SIEM-системы в формате Syslog	886

Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Kaspersky Security Center, не используя интерфейс Kaspersky Security Center. Можно создавать запросы непосредственно к публичным представлениям и извлекать из них данные о событиях или создавать собственные представления на базе существующих публичных представлений и обращаться к ним для получения требуемых данных.

Публичные представления

Для вашего удобства в базе данных Kaspersky Security Center предусмотрен набор публичных представлений. Описание публичных представлений приведено в документе klakdb.chm.

Публичное представление `v_akpub_ev_event` содержит набор полей, соответствующих параметрам событий в базе данных. В документе `klakdb.chm` также содержится информация о публичных представлениях, относящихся к другим объектам Kaspersky Security Center, например, устройствам, приложениям, пользователям. Вы можете использовать эту информацию при создании запросов.

В этом разделе приведены инструкции по созданию SQL-запроса с помощью утилиты `klsql2`, а также пример такого запроса.

Вы также можете использовать любые другие приложения для работы с базами данных для создания SQL-запросов и представлений баз данных. Информация о том, как посмотреть параметры подключения к базе данных Kaspersky Security Center, например, имя инстанса и имя базы данных, приведена в соответствующем разделе (см. раздел "Просмотр имени базы данных Kaspersky Security Center" на стр. [897](#)).

См. также:

Сценарий: настройка экспорта событий в SIEM-системы	879
В этом разделе	
Создание SQL-запроса с помощью утилиты <code>klsql2</code>	895
Пример SQL-запроса, созданного с помощью утилиты <code>klsql2</code>	896
Просмотр имени базы данных Kaspersky Security Center	897

Создание SQL-запроса с помощью утилиты `klsql2`

В этой статье приведены инструкции по загрузке и использованию утилиты `klsql2`, а также по созданию SQL-запроса с использованием этой утилиты.

► Чтобы использовать утилиту `klsql2`:

1. Найдите утилиту `klsql2` в папке установки Kaspersky Security Center. Путь установки по умолчанию: `<Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center`. Не используйте версии утилиты `klsql2`, предназначенные для старых версий Kaspersky Security Center.
2. Создайте файл `src.sql` в любом текстовом редакторе и поместите файл в одну папку с утилитой.
3. В файле `src.sql` введите требуемый SQL-запрос и сохраните файл.
4. На устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, в командной строке введите следующую команду для запуска SQL-запроса из файла `src.sql` и сохранения результатов в файл `result.xml`:

```
klsql2 -i src.sql -u <имя пользователя> -p <пароль> -o result.xml
```

где <имя пользователя> и <пароль> являются учетными данными учетной записи пользователя, имеющего доступ к базе данных.

5. При необходимости введите имя учетной записи и пароль пользователя, имеющего доступ к базе данных.
6. Откройте созданный файл result.xml и посмотрите результаты выполнения SQL-запроса.

Вы можете редактировать файл src.sql и создавать в нем любые SQL-запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить SQL-запрос и сохранить результаты в файл.

См. также

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

Пример SQL-запроса, созданного с помощью утилиты klsql2

В этом разделе приведен пример SQL-запроса, созданного с помощью утилиты klsql2.

Следующий пример показывает, как получить список событий, произошедших на устройствах пользователей за последние 7 дней, и отсортировать его по времени возникновения событий, самые недавние события отображаются первыми.

Пример:

```
SELECT
e.nId,                                /* идентификатор
события */
e.tmRiseTime,                          /* время
возникновения события */
e.strEventType,                       /* внутреннее имя
типа события */
e.wstrEventTypeDisplayName,           /* отображаемое имя
события */
e.wstrDescription,                   /* отображаемое
описание события */
e.wstrGroupName,                     /* имя группы устройств */
h.wstrDisplayName,                   /* отображаемое имя
устройства, на котором произошло событие */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp      /* IP-адрес
устройства, на котором произошло событие */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

См. также:

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

Просмотр имени базы данных Kaspersky Security Center

Может быть полезно знать имя базы данных, если вам нужно, например, отправить SQL-запрос и подключиться к базе данных из редактора скриптов SQL.

► Чтобы просмотреть имя базы данных Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования выберите раздел **Дополнительно**, а затем **Информация об используемой базе данных**.
3. В разделе **Информация об используемой базе данных** обратите внимание на следующие свойства базы данных (см. рис. ниже):
 - **Имя экземпляра**

Имя экземпляра используемой базы данных Kaspersky Security Center.
Значение по умолчанию – .\KAV_CS_ADMIN_KIT.

- **Имя базы данных**

Имя базы данных SQL Kaspersky Security Center. Значение по умолчанию – KAV.

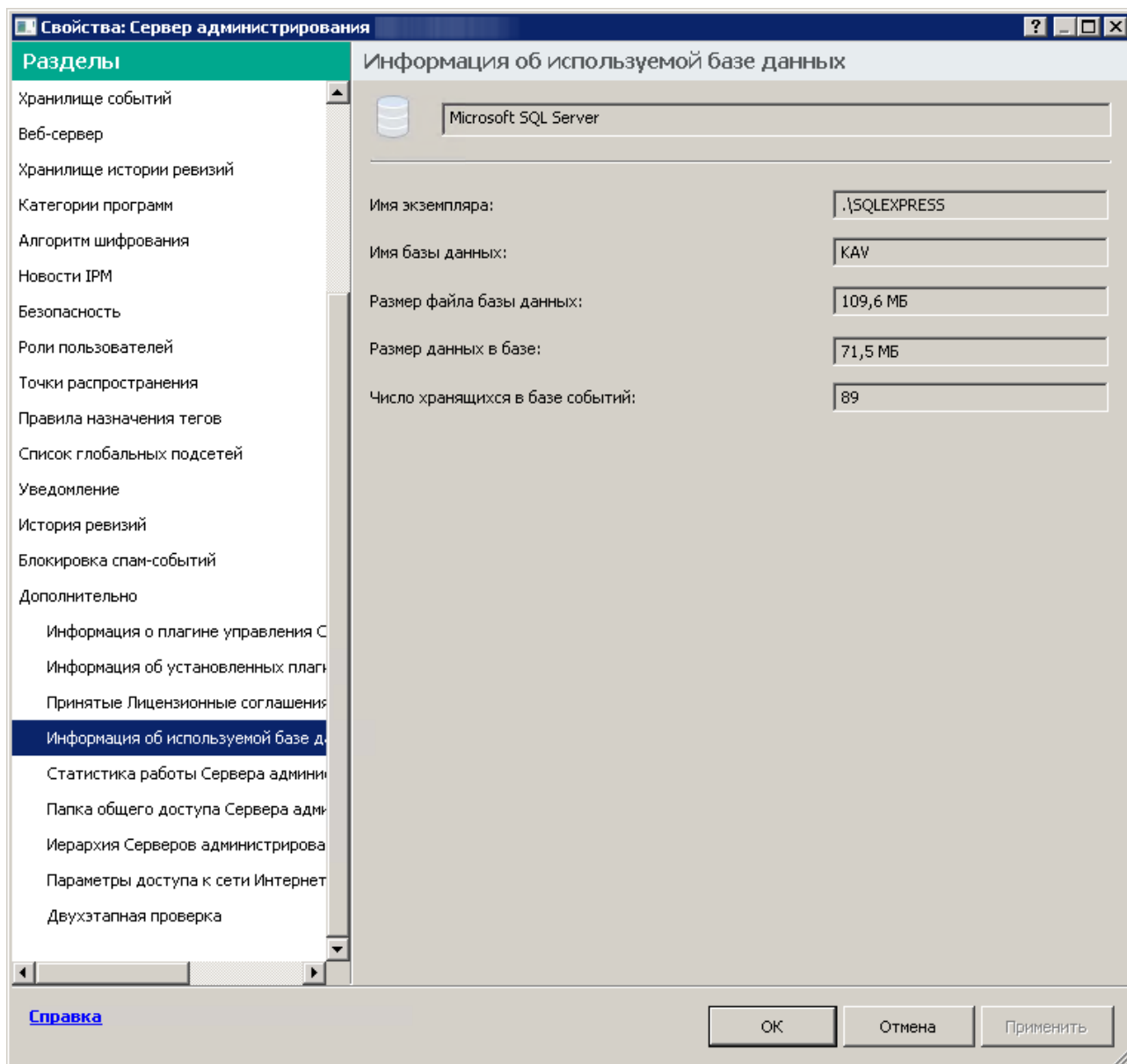


Рисунок 11. Имя базы данных SQL Kaspersky Security Center

4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Используйте это имя базы данных для подключения и обращения к базе данных в ваших SQL-запросах.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Kaspersky Security Center события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте и при необходимости исправьте настройки Kaspersky Security Center и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. Например, первое событие – это критическое событие Сервера администрирования: *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.

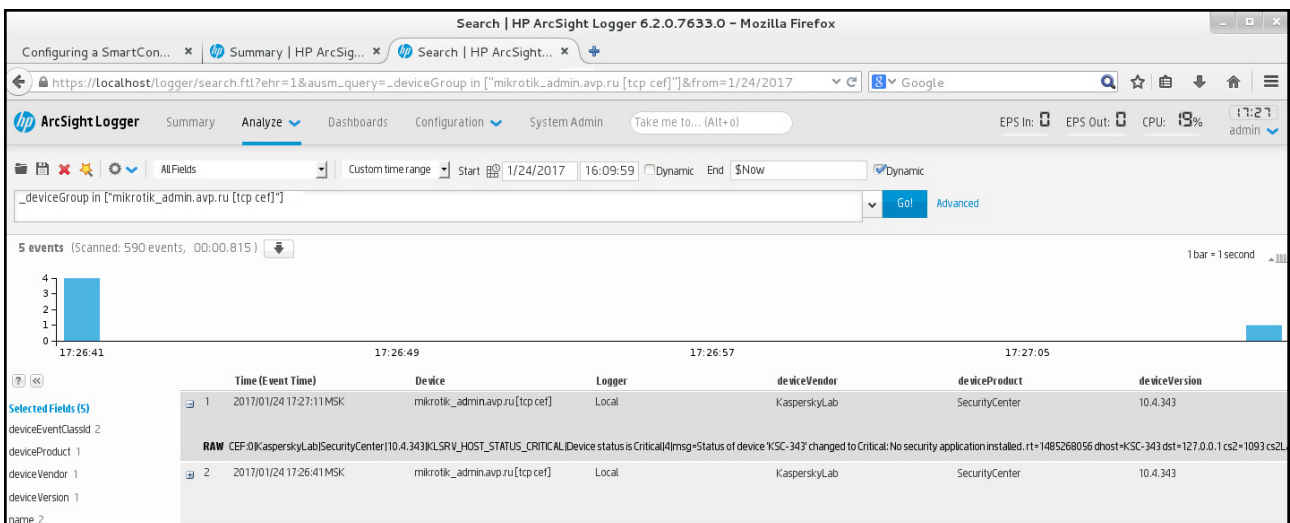


Рисунок 12. Пример событий

См. также:

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

Использование SNMP для отправки статистики приложениям сторонних производителей

В этом разделе описывается, как получить информацию от Сервера администрирования с помощью SNMP-протокола в Windows. Kaspersky Security Center содержит SNMP-агент, который передает статистику работы Сервера администрирования приложениям сторонних производителей с помощью OID.

В этом разделе также содержится информация о действиях для решения проблем, которые могут возникнуть при использовании SNMP для Kaspersky Security Center.

В этом разделе

Настройка SNMP-службы для использования с Kaspersky Security Center	900
SNMP-агент и идентификаторы объектов	901
Получение имени счетчика строк из идентификатора объекта	901
Значения идентификаторов объектов для SNMP	902
Устранение неисправностей	911

Настройка SNMP-службы для использования с Kaspersky Security Center

В этом разделе описано, как настроить SNMP-службу в Windows для получения информации от Сервера администрирования с помощью Simple Network Management Protocol (SNMP).

По умолчанию поддержка SNMP в Windows выключена.

► Чтобы включить поддержку SNMP в Windows:

1. Перейдите в **Панель управления**.
2. Откройте меню **Установка и удаление приложений**.
3. Нажмите на **Включение или отключение компонентов Windows**.
4. В списке компонентов Windows перейдите к функции SNMP и нажмите на кнопку **ОК**.
5. Перейдите в **Панель управления** → **Администрирование** → **Службы**.
6. Выберите **SNMP-службу** и запустите ее.
7. Проверьте, работает ли прослушивание, проверив его с помощью `netstat` для UDP-порта.

Поддержка SNMP в Windows включена.

► Чтобы настроить SNMP-службу в Windows:

1. Убедитесь, что компонент **Агент SNMP** Kaspersky Security Center был установлен во время обычной (см. раздел "Шаг 3. Выбор компонентов для установки" на стр. [235](#)) или тихой установки.
2. Убедитесь, что **SNMP-служба** и **служба SNMP-ловушки** Windows запущены.

- Убедитесь, что в вашей системе установлен MIB Browser ManageEngine.
- В свойствах **SNMP-службы** на вкладке **Безопасность** добавьте два сообщества со следующими правами:

Сообщество	Права
kaspersky	NOTIFY
public	READ WRITE

- В поле **Принимать SNMP-пакеты от этих устройств** добавьте IP-адрес устройства, на котором установлен ManageEngine MIB Browser, например 10.10.10.105.
- На вкладке **Ловушки** введите `kaspersky` в поле **Имя сообщества**.
- Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно свойств службы.
- В ManageEngine MIB Browser загрузите файл `adminkit.mib` из папки установки Kaspersky Security Center. По умолчанию файл `adminkit.mib` находится в папке <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp.
- В поле **Устройство** окна ManageEngine MIB Browser добавьте IP-адрес устройства, на котором установлен Сервер администрирования Kaspersky Security Center.

SNMP-служба настроена на получение информации от Сервера администрирования с использованием Simple Network Management Protocol (SNMP).

SNMP-агент и идентификаторы объектов

Для Kaspersky Security Center SNMP-агент реализован в виде динамической библиотеки `kl SNMPag.dll`, которая регистрируется установщиком при установке Сервера администрирования. SNMP-агент работает внутри процесса `snmp.exe` (который является службой Windows). Приложения сторонних производителей используют SNMP-протокол для получения статистики (которая представлена в виде счетчиков) производительности Сервера администрирования.

Каждый счетчик имеет уникальный *идентификатор объекта* (далее также OID, object identifier). Идентификатор объекта – это последовательность чисел, разделенных точками. Идентификаторы объектов Сервера администрирования начинаются с префикса 1.3.6.1.4.1.23668.1093. OID счетчика – это соединение этого префикса с суффиксом, описывающим счетчик. Например, счетчик со значением OID 1.3.6.1.4.1.23668.1093.1.1.4 имеет суффикс со значением 1.1.4.

Вы можете использовать SNMP-клиент (например, Zabbix) для контроля состояния вашей системы. Чтобы получить информацию, вы можете найти значение OID и ввести это значение в свой SNMP-клиент. Затем ваш SNMP-клиент вернет вам другое значение, которое характеризует состояние вашей системы.

Список счетчиков и типы счетчиков находятся в файле `adminkit.mib` на Сервере администрирования. *MIB* расшифровывается как Management Information Base. Вы можете импортировать и анализировать файлы `.mib` с помощью приложения MIB Viewer, которое предназначено для запроса и отображения значений счетчиков.

Получение имени счетчика строк из идентификатора объекта

Чтобы использовать идентификатор объекта (OID) для передачи информации приложениям сторонних производителей, вам может потребоваться получить имя счетчика строк из этого OID.

► Чтобы получить имя счетчика строк из OID:

1. Откройте в текстовом редакторе файл `adminkit.mib`, расположенный на Сервере администрирования.
2. Найдите пространство имен, описывающее первое значение (слева направо).
Например, для суффикса OID 1.1.4 это будет `"counters" ( ::= { kladminkit 1 } )`.
3. Найдите пространство имен, описывающее второе значение.
Например, для суффикса OID 1.1.4 это будет `counters 1`, что означает `deployment`.
4. Найдите пространство имен, описывающее третье значение.
Например, для суффикса OID 1.1.4 это будет `deployment 4`, что означает `hostsWithAntivirus`.

Имя счетчика строк – это объединение этих значений, например, `<MIB base namespace>.counters.deployment.hostsWithAntivirus`, и это соответствует идентификатору OID со значением 1.3.6.1.4.1.23668.1093.1.1.4.

Значения идентификаторов объектов для SNMP

В таблице ниже приведены значения и описания идентификатора объекта (далее также OID), которые используются для передачи информации о производительности Сервера администрирования приложениям сторонних производителей.

Таблица 77. Значения и описания параметров идентификаторов объектов для SNMP

Значение идентификатора объекта	Числовой тип данных	OID	Описание
<code>deploymentStatus</code>	INTEGER { <code>ok(0)</code> , <code>info(1)</code> , , <code>warning(2)</code> , <code>critical(3)</code> }	.1.3.6.1.4.1.23668.1093.1.1.1	Статус развертывания. Статус может принимать одно из следующих значений: • Информационное сообщение. Лицензия больше не действует для N устройств. • Предупреждение. Одно из следующих: M устройств с установленными приложениями "Лаборатории Касперского" на N устройствах в группах Сервера администрирования (N > M). Срок действия лицензии L истекает на N устройствах через M дней. Задача T по установке приложений успешно

Значение идентификатора объекта	Числовой тип данных	OID	Описание
			завершена на N устройствах, для M устройств требуется перезагрузка. • Критический. Срок действия лицензии истек для N устройств. • ОК. Ничего из вышеперечисленного.
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.1.2.1	Причина <code>deploymentStatus</code> показывает, что в группах Сервера администрирования слишком много устройств, на которых не установлены управляемые приложения. Значение равно 1 в случае обнаружения нескольких устройств без управляемых приложений и 0 в другом случае.
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.1.2.2	Причина <code>deploymentStatus</code> показывает, что на некоторых устройствах не удалось выполнить задачу удаленной установки. Количество этих устройств можно получить с помощью <code>hostsRemoteInstallFailed</code>.
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.1.2.3	Причина <code>deploymentStatus</code> показывает, что есть несколько устройств, у которых истекает срок действия лицензии через семь дней. Количество этих устройств можно получить с помощью <code>hostsLicenseExpiring</code>.
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.1.2.4	Причина <code>deploymentStatus</code> показывает, что есть несколько устройств, у которых срок действия лицензии истек. Вы можете узнать количество этих устройств с помощью <code>hostsLicenseExpired</code>.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
hostsInGroups	Counter 32	.1.3.6.1.4.1.23668.109 3.1.1.3	Количество устройств в группах Сервера администрирования.
hostsWithAntivirus	Counter 32	.1.3.6.1.4.1.23668.109 3.1.1.4	Количество устройств в группах Сервера администрирования с установленными управляемыми приложениями.
hostsRemoteInstallFailed	Counter 32	.1.3.6.1.4.1.23668.109 3.1.1.5	Количество устройств, на которых не удалось выполнить задачу удаленной установки.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.109 3.1.1.6	Идентификатор лицензионного ключа, срок действия которого скоро истечет (менее чем через 7 дней).
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.109 3.1.1.7	Идентификатор лицензионного ключа, срок действия которого истек.
licenceExpiringDays	Unsigned 32	.1.3.6.1.4.1.23668.109 3.1.1.8	Количество дней до истечения срока действия лицензии. Для этого параметра срок действия лицензии истек, если до истечения срока его действия осталось менее 7 дней. Если до истечения срока действия осталось более 7 дней, значение равно 0.
hostsLicenceExpiring	Counter 32	.1.3.6.1.4.1.23668.109 3.1.1.9	Количество устройств с лицензией, срок действия которой скоро истекает (менее чем через 7 дней).
hostsLicenceExpired	Counter 32	.1.3.6.1.4.1.23668.109 3.1.1.10	Количество устройств, у которых истек срок действия лицензии.
updatesStatus	INTEGER { ok(0), info(1) }	.1.3.6.1.4.1.23668.109 3.1.2.1	Состояние обновления антивирусных баз. Статус может принимать одно из следующих значений:

Значение идентификатора объекта	Числовой тип данных	OID	Описание
	, warning (2), critical(3) }		• Информационное сообщение. Антивирусные базы на Сервере администрирования или на устройствах не обновлялись более одного дня; с момента установки приложения прошло менее одного дня. • Предупреждение. Антивирусные базы на Сервере администрирования или на устройствах не обновлялись более 3 дней. Это значение можно изменить в свойствах группы. • Критический. Антивирусные базы на Сервере администрирования или на устройствах не обновлялись более 7 дней. Это значение можно изменить в свойствах группы. • ОК. Ничего из вышеперечисленного.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.2.2.1	Эта причина показывает, что Сервер администрирования не обновлялся в течение долгого времени. Время, которое считается долгим, указывается в <code>updatesStatus</code> .
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.2.2.2	Эта причина показывает, что некоторые устройства не обновлялись в течение долгого времени (по умолчанию Критическое – 7 дней и более, Предупреждение – 3 дня). Вы можете узнать количество этих устройств с помощью <code>hostsNotUpdated</code> .
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.109 3.1.2.3	Дата последнего обновления антивирусных баз на Сервере администрирования.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
hostsNotUpdated	Counter 32	.1.3.6.1.4.1.23668.109 3.1.2.4	Количество устройств, содержащих антивирусные базы, которые давно не обновлялись (по умолчанию Критическое – 7 дней и более, Предупреждение – 3 дня). Если есть устройства со статусом обновления Критическое , учитываются только эти устройства. Вы можете получить статус обновления с помощью <code>updatesStatus</code> .
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.109 3.1.3.1	Статус постоянной защиты. Одно из следующих: • Предупреждение. Одно из следующих: На устройстве, входящем в группу Сервера администрирования, обнаружено нарушение безопасности. Из-за ошибок шифрования некоторые устройства изменили состояние защиты. Полная проверка давно не выполнялась. • Критический. На некоторых устройствах в группах Сервера администрирования не работает антивирусная защита. • ОК. Ничего из вышеперечисленного.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.3.2.1	Эта причина показывает, что приложение безопасности не работает на некоторых устройствах. Вы можете узнать количество этих устройств с помощью <code>hostsAntivirusNotRunning</code> .
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.3.2.2	Эта причина показывает, что на некоторых устройствах постоянная защита не работает. Вы можете узнать количество этих устройств с помощью

Значение идентификатора объекта	Числовой тип данных	OID	Описание
			hostsRealtimeNotRunning.
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.3.2.4	Эта причина показывает, что есть некоторые устройства, содержащие не вылеченные объекты. Вы можете узнать количество этих устройств с помощью hostsNotCuredObject.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.3.2.5	Эта причина показывает, что на некоторых устройствах обнаружены угрозы. Вы можете узнать количество этих устройств с помощью hostsTooManyThreats.
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.3.2.6	Эта причина показывает статус вирусной атаки. Значение равно 1, если определенное количество вирусов было обнаружено в течение определенного времени, и 0 в других случаях. Количество вирусов и время указывается на Сервере администрирования с помощью параметра Вирусная атака.
hostsAntivirusNotRunning	Counter 32	.1.3.6.1.4.1.23668.109 3.1.3.3	Количество устройств, на которых не запущены приложения безопасности.
hostsRealtimeNotRunning	Counter 32	.1.3.6.1.4.1.23668.109 3.1.3.4	Количество устройств, на которых не запущена постоянная защита.
hostsRealtimeLevelChanged	Counter 32	.1.3.6.1.4.1.23668.109 3.1.3.5	Количество устройств с недопустимым уровнем постоянной защиты.
hostsNotCuredObject	Counter 32	.1.3.6.1.4.1.23668.109 3.1.3.6	Количество устройств с не вылеченными объектами.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
hostsTooManyThreats	Counter 32	.1.3.6.1.4.1.23668.1093.1.3.7	Количество устройств, которые содержат угрозы.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	Статус полной проверки. Одно из следующих: • Информационное сообщение. С момента установки приложения прошло менее 7 дней. • Предупреждение. Полная проверка не производилась более 7 дней с момента установки приложения. • Критический. Полная проверка не производилась более 14 дней с момента установки приложения. • ОК. Ничего из вышеперечисленного.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Эта причина показывает, что на некоторых устройствах не выполнялась проверка в течение определенного времени. Вы можете узнать количество этих устройств с помощью <code>hostsNotScannedLately</code> . Время указывается в <code>fullScanStatus</code> .
hostsNotScannedLately	Counter 32	.1.3.6.1.4.1.23668.1093.1.4.3	Количество устройств, на которых не выполнялась проверка в течение определенного времени. Время указывается в <code>fullScanStatus</code> .
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	Состояние логической сети Сервера администрирования. Одно из следующих: • Предупреждение. Если есть устройства со статусом Предупреждение, к которым нет доступа, или если есть устройства, которые не

Значение идентификатора объекта	Числовой тип данных	OID	Описание
			принадлежат ни к какой группе Сервера администрирования. • Критический. Если есть устройства, контроль над которыми потерян Сервером администрирования, или есть устройства со статусом Критический, к которым нет доступа. • ОК. Ничего из вышеперечисленного.
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.5.2.1	Эта причина показывает, что некоторые устройства в течение долгого времени не были подключены к Серверу администрирования (7 дней и более для устройства со статусом Предупреждение и 4 дня для устройства со статусом Критический). Вы можете узнать количество этих устройств с помощью <code>hostsNotConnectedLongTime</code>.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.109 3.1.5.2.2	Эта причина показывает, что есть устройства, контроль над которыми потерян Сервером администрирования. Вы можете узнать количество этих устройств с помощью <code>hostsControlLost</code>.
hostsFound	Counter 32	.1.3.6.1.4.1.23668.109 3.1.5.3	Количество обнаруженных Сервером администрирования устройств, не входящих ни в одну группу Сервера администрирования.
groupsCount	Counter 32	.1.3.6.1.4.1.23668.109 3.1.5.4	Количество групп Сервера администрирования.
hostsNotConnectedLongTime	Counter 32	.1.3.6.1.4.1.23668.109 3.1.5.5	Количество устройств, которые долгое время не подключались к Серверу администрирования.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
			Время, которое считается долгим, указывается в <code>notConnectedLongTime</code> .
<code>hostsControlLost</code>	Counter 32	.1.3.6.1.4.1.23668.109 3.1.5.6	Количество устройств, которые не контролируются Сервером администрирования.
<code>eventsStatus</code>	INTEGER { <code>ok(0)</code> , <code>warning(1)</code> , <code>critical(2)</code> }	.1.3.6.1.4.1.23668.109 3.1.6.1	Состояние подсистемы событий. Одно из следующих: • Предупреждение. Одно из следующих: Устройства групп Сервера администрирования давно не выполняли поиск обновлений Windows. Есть устройства с проблемами, связанные со статусом. • Критический. Одно из следующих: Хотя бы на одном устройстве произошло событие с уровнем важности "Критическое". Хотя бы на одном устройстве произошло событие с уровнем важности "Отказ функционирования". Есть событие неудачного завершения задачи хотя бы на одном устройстве. Устройства групп Сервера администрирования давно не выполняли поиск обновлений Windows. Есть устройства с проблемами, связанные со статусом. • ОК. Ничего из вышеперечисленного.
<code>criticalEventOccured</code>	INTEGER { <code>off(0)</code> , <code>on(1)</code> }	.1.3.6.1.4.1.23668.109 3.1.6.2.1	Причина <code>eventsStatus</code> показывает, что на Сервере администрирования произошли критические события. Вы можете получить количество этих событий с помощью

Значение идентификатора объекта	Числовой тип данных	OID	Описание
			<code>criticalEventsCount</code> . Значение равно 1, если есть хотя бы одно критическое событие на любом устройстве, и 0 в другом случае.
<code>criticalEventsCount</code>	Counter 32	.1.3.6.1.4.1.23668.109 3.1.6.3	Количество критических событий на Сервере администрирования.

Устранение неисправностей

В этом разделе перечислены решения нескольких типичных проблем, с которыми вы можете столкнуться при использовании SNMP-службы.

Приложение стороннего производителя не может подключиться к SNMP-службе

Убедитесь, что SNMP-служба установлена и настроена, как описано в разделе Настройка SNMP-службы для использования с Kaspersky Security Center (см. раздел "Настройка SNMP-службы для использования с Kaspersky Security Center" на стр. [900](#)).

SNMP-служба работает, но приложение стороннего производителя не может получить никаких значений

Разрешите трассировку SNMP-агента и убедитесь, что создан непустой файл. Это означает, что SNMP-агент зарегистрирован правильно и работает. После этого разрешите подключения от SNMP-службы в параметрах службы. Если служба работает на том же устройстве, что и SNMP-агент, список IP-адресов должен содержать либо IP-адрес этого устройства, либо `loopback 127.0.0.1`.

В Windows должна работать SNMP-служба, которая взаимодействует с агентами. Вы можете указать пути к SNMP-агентам в реестре Windows с помощью `regedit`.

- Для Windows 10:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- Для Windows Vista и Windows Server 2008:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

Вы также можете разрешить трассировку SNMP-агента с помощью `regedit`.

- для 32-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- для 64-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
"TraceLevel"=dword:00000004
"TraceDir"="C:\\"

Значения не соответствуют статусам Консоли администрирования

Для снижения нагрузки на Сервер администрирования реализовано кеширование значений для SNMP-агента. Задержка между актуализацией кеша и изменяемыми значениями на Сервере администрирования может вызвать несоответствие между значениями, возвращаемыми SNMP-агентом, и фактическими. При работе с приложениями сторонних производителей следует учитывать возможную задержку.

Приложения

В этом разделе содержится справочная и дополнительная информация, касающаяся использования Kaspersky Security Center.

В этом разделе

Дополнительные возможности	913
Особенности работы с интерфейсом управления.....	921
Справочная информация	927
Поиск и экспорт данных	937
Параметры задач.....	951
Глобальный список подсетей	966
Использование Агента администрирования для Windows, macOS и Linux: сравнение	967

Дополнительные возможности

В этом разделе рассматривается ряд дополнительных функций приложения Kaspersky Security Center, предназначенных для расширения возможностей централизованного управления приложениями на устройствах.

В этом разделе

Автоматизация работы Kaspersky Security Center. Утилита klakaut	914
Работа с внешними инструментами.....	914
Режим клонирования диска Агента администрирования	914
Подготовка эталонного устройства с установленным Агентом администрирования для создания образа операционной системы.....	916
Настройка параметров получения сообщений от компонента Мониторинг файловых операций	917
обслуживание Сервера администрирования;	918
Доступ к общедоступным DNS-серверам	919
Окно Способ уведомления пользователей	920
Окно Выборка устройств	920
Окно Определение названия создаваемого объекта.....	920
Раздел Категории программ	920

Автоматизация работы Kaspersky Security Center. Утилита klakaut

Вы можете автоматизировать работу Kaspersky Security Center с помощью утилиты klakaut. Утилита klakaut и справочная система для нее расположены в папке установки Kaspersky Security Center.

Работа с внешними инструментами

Kaspersky Security Center позволяет сформировать список *внешних инструментов* (далее также *инструментов*) – приложений, которые вызываются для клиентского устройства из Консоли администрирования при помощи группы контекстного меню **Внешние инструменты**. Для каждого инструмента из списка создается отдельная команда меню, с помощью которой Консоль администрирования запускает соответствующую инструменту приложение.

Приложение запускается на рабочем месте администратора. В качестве аргументов командной строки приложение может принимать атрибуты удаленного клиентского устройства (NetBIOS-имя, DNS-имя, IP-адрес). Подключение к удаленному устройству может выполняться при помощи туннелированного соединения.

По умолчанию для каждого клиентского устройства список внешних инструментов содержит следующие сервисные приложения:

- **Удаленная диагностика** – утилита удаленной диагностики Kaspersky Security Center.
- **Удаленный рабочий стол** – стандартный компонент Microsoft Windows "Подключение к удаленному рабочему столу".
- **Управление компьютером** – стандартный компонент Microsoft Windows.

► *Чтобы добавить или удалить внешние инструменты, а также изменить их параметры,*

В контекстном меню выбранного устройства выберите пункт **Внешние инструменты** → **Настроить внешние инструменты**.

Откроется окно **Внешние инструменты**. В этом окне можно добавлять внешние инструменты или изменять их параметры с помощью кнопок **Добавить** и **Изменить**. Чтобы удалить внешние инструменты, нажмите на кнопку удаления со значком красного крестика (✗).

Режим клонирования диска Агента администрирования

Клонирование жесткого диска "эталонного" устройства является распространенным способом установки программного обеспечения на новые устройства. Если Агент администрирования на жестком диске "эталонного" устройства во время клонирования работает в обычном режиме, возникает следующая проблема:

После развертывания на новых устройствах эталонного образа диска с Агентом администрирования эти устройства отображаются в Консоли администрирования одним значком. Проблема возникает потому, что при клонировании на новых устройствах сохраняются одинаковые внутренние данные, позволяющие Серверу администрирования связать устройство со значком в Консоли администрирования.

Избежать проблемы с неверным отображением новых устройств в Консоли администрирования после клонирования помогает специальный *режим клонирования диска Агента администрирования*. Используйте этот режим, если вы разворачиваете программное обеспечение (с Агентом администрирования) на новых устройствах путем клонирования диска.

В режиме клонирования диска Агент администрирования работает, но не подключается к Серверу администрирования. При выходе из режима клонирования Агент администрирования удаляет внутренние данные, из-за наличия которых Сервер администрирования связывает несколько устройств с одним значком в Консоли администрирования. По завершении клонирования образа "эталонного" устройства, новые устройства отображаются в Консоли администрирования нормально (отдельными значками).

Сценарий использования режима клонирования диска Агента администрирования

1. Администратор устанавливает Агент администрирования на "эталонном" устройстве.
2. Администратор проверяет подключение Агента администрирования к Серверу администрирования с помощью утилиты `klmover` (см. раздел "Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита `klmover`" на стр. [757](#)).
3. Администратор включает режим клонирования диска Агента администрирования.
4. Администратор устанавливает на устройство программное обеспечение, патчи и выполняет любое количество перезагрузок устройства.
5. Администратор выполняет клонирование жесткого диска "эталонного" устройства на любое число устройств.
6. Для каждой клонированной копии должны быть выполнены следующие условия:
 - a. имя устройства изменено;
 - b. устройство перезагружено;
 - c. режим клонирования диска выключен.

Включение и выключение режима клонирования диска с помощью утилиты `klmover`

► Чтобы включить или выключить режим клонирования диска Агента администрирования:

1. Запустите утилиту `klmover` на устройстве с установленным Агентом администрирования, который нужно клонировать.
Утилита `klmover` находится в папке установки Агента администрирования.
2. Чтобы включить режим клонирования диска, в командной строке Windows введите команду `klmover -cloningmode 1`.
Агент администрирования переключается в режим клонирования диска.
3. Чтобы запросить текущее состояние режима клонирования диска, в командной строке введите команду `klmover -cloningmode`.
В результате в окне утилиты отобразится информация о том, включен или выключен режим клонирования диска.
4. Чтобы выключить режим клонирования диска, в командной строке утилиты введите команду `klmover -cloningmode 0`.

См. также:

Развертывание захватом и копированием образа устройства	167
Подготовка эталонного устройства с установленным Агентом администрирования для создания образа операционной системы	916

Подготовка эталонного устройства с установленным Агентом администрирования для создания образа операционной системы

Вы можете создать образ операционной системы эталонного устройства с установленным Агентом администрирования, а затем развернуть образ на сетевых устройствах. В этом случае вы создаете образ операционной системы эталонного устройства, на котором Агент администрирования еще не запущен. Если вы запустите Агент администрирования на эталонном устройстве до создания образа операционной системы, идентификация Сервера администрирования устройств, развернутых из образа операционной системы эталонного устройства, будет проблематичной.

► Чтобы подготовить эталонное устройство для создания образа операционной системы:

1. Убедитесь, что операционная система Windows установлена на эталонном устройстве, также установите другое программное обеспечение, которое вам нужно на этом устройстве.
2. На эталонном устройстве в параметрах сетевых подключений Windows отключите эталонное устройство от сети, в которой установлен Kaspersky Security Center.
3. На эталонном устройстве запустите локальную установку Агента администрирования с помощью файла `setup.exe`.

Запускается мастер установки Агента администрирования Kaspersky Security Center. Следуйте далее указаниям мастера.

4. На странице **Сервера администрирования** мастера укажите IP-адрес Сервера администрирования.

Если вы не знаете точный адрес Сервера администрирования, введите `localhost`. Вы можете изменить IP-адрес позже, используя утилиту `klmover` (см. раздел "Подключение клиентского устройства к Серверу администрирования вручную. Утилита `klmover`" на стр. [750](#)) с ключом `- address`.

5. На странице **Запустить приложение** в мастере отключите параметр **Запустить приложение в процессе установки**.
6. После завершения установки Агента администрирования не перезагружайте устройство перед созданием образа операционной системы.

Если вы перезагрузите устройство, вам нужно будет повторить весь процесс подготовки эталонного устройства для создания образа операционной системы.

7. На эталонном устройстве в командной строке запустите утилиту `sysprep` (см. раздел "Настройка параметров утилиты `sysprep.exe`" на стр. [848](#)) и выполните следующую команду: `sysprep.exe /generalize /oobe /shutdown`.

Эталонное устройство готово к созданию образа операционной системы (см. раздел "Создание инсталляционных пакетов приложений" на стр. [850](#)).

См. также:

Режим клонирования диска Агента администрирования	914
Развертывание захватом и копированием образа устройства	167

Настройка параметров получения сообщений от компонента Мониторинг файловых операций

Управляемые приложения, такие как Kaspersky Security для Windows Server или Kaspersky Security для виртуальных сред Легкий агент, отправляют сообщения от компонента Мониторинг файловых операций в Kaspersky Security Center. Kaspersky Security Center позволяет также следить за неизменностью критически важных областей систем (например, веб-серверы, банкоматы) и оперативно реагировать на нарушения целостности таких систем. Для этого реализована поддержка получения сообщений от компонента Мониторинг файловых операций. Компонент Мониторинг файловых операций позволяет следить не только за файловой системой устройства, но и за ветками реестра, состоянием сетевого экрана и состоянием подключенного оборудования.

Требуется выполнить настройку Kaspersky Security Center, чтобы получать сообщения от компонента Мониторинг файловых операций без использования приложений Kaspersky Security для Windows Server или Kaspersky Security для виртуальных сред Легкий агент.

► Чтобы настроить параметры получения сообщений от компонента Мониторинга файловых операций:

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
 - для 32-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
 - для 64-разрядной системы:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
3. Создайте ключи:
 - Создайте ключ KLSRV_EVP_FIM_PERIOD_SEC, чтобы указать интервал времени подсчета числа обработанных событий. Задайте следующие параметры:
 - a. Укажите название ключа KLSRV_EVP_FIM_PERIOD_SEC.
 - b. Укажите тип ключа DWORD.
 - c. Задайте диапазон значений промежутка времени от 43 200 до 172 800 секунд. По умолчанию промежуток проверки равен 86 400 секунд.
 - Создайте ключ KLSRV_EVP_FIM_LIMIT для ограничения количества принимаемых событий за указанный промежуток времени. Задайте следующие параметры:
 - a. Укажите название ключа KLSRV_EVP_FIM_LIMIT.
 - b. Укажите тип ключа DWORD.
 - c. Задайте диапазон значений принимаемых событий от 2000 до 50 000. По умолчанию количество событий равно 20 000.
 - Создайте ключ KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC для подсчета событий с точностью до определенного промежутка времени. Задайте следующие параметры:
 - a. Укажите название ключа KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC.
 - b. Укажите тип ключа DWORD.

- с. Задайте диапазон значений от 120 до 600 секунд. Временной интервал, установленный по умолчанию, составляет 300 секунд.
- Создайте ключ KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC, чтобы после указанного значения времени приложение выполняло проверку того, что число событий, обработанных за промежуток времени, становится меньше заданного ограничения. Проверка выполняется при достижении ограничения приема событий. Если условие выполняется, возобновляется сохранение событий в базу данных. Задайте следующие параметры:
 - а. Укажите название ключа KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC.
 - б. Укажите тип ключа DWORD.
- с. Задайте диапазон значений от 600 до 3600 секунд. Временной интервал, установленный по умолчанию, составляет 1800 секунд.

Если ключи не созданы, используются значения по умолчанию.

4. Перезапустите службу Сервера администрирования.

Ограничения получения событий от компонента Мониторинга файловых операций будут настроены. Результаты работы компонента Мониторинг файловых операций можно посмотреть в отчетах **Топ 10 правил Мониторинга файловых операций / Контроля целостности системы, наиболее часто срабатывающие на устройствах и Топ 10 устройств с правилами Мониторинга файловых операций / Контроля целостности системы, срабатывающими чаще всего.**

обслуживание Сервера администрирования;

Обслуживание Сервера администрирования позволяет освободить место в папке Сервера администрирования и уменьшить объем базы данных за счет удаления ненужных объектов. Это поможет вам повысить производительность и надежность работы приложения. Рекомендуется выполнять обслуживание Сервера администрирования не реже одного раза в неделю.

Обслуживание Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания Сервера администрирования приложение выполняет следующие действия:

- Удаляет ненужные папки и файлы из папки хранилища.
- Удаляет ненужные записи из таблиц (также известные как "висячие указатели").
- Очищает кеш.
- Обслуживает базу данных (если вы используете SQL Server или PostgreSQL в качестве СУБД):
 - проверяет базу данных на наличие ошибок (доступно только для SQL Server);
 - перестраивает индексы базы данных;
 - обновляет статистику базы данных;
 - сжимает базу данных (если необходимо).

Задача *Обслуживание Сервера администрирования* поддерживает MariaDB версии 10.3 и выше. Если используется MariaDB версии 10.2 или ниже, администраторам следует обслуживать базу данных самостоятельно.

► Чтобы создать задачу Обслуживание Сервера администрирования:

1. В дереве консоли выберите узел Сервера администрирования, для которого нужно создать задачу *Обслуживание Сервера администрирования*.
2. Выберите папку **Задачи**.
3. В рабочей области папки **Новая задача** нажмите на кнопку **Задачи**.
Запустится мастер создания задачи.
4. В окне мастера **Выбор типа задачи** выберите тип задачи **Обслуживание Сервера администрирования** и нажмите на кнопку **Далее**.
5. Если во время обслуживания нужно сжимать базу данных Сервера администрирования, в окне мастера **Параметры** установите флажок **Сжать базу данных**.
6. Следуйте дальнейшим шагам мастера.

Созданная задача отображается в списке задач в рабочей области папки **Задачи**. Для одного Сервера администрирования может выполняться только одна задача *Обслуживание Сервера администрирования*. Если задача *Обслуживание Сервера администрирования* для Сервера администрирования уже создана, создание еще одной задачи *Обслуживание Сервера администрирования* невозможно.

Доступ к общедоступным DNS-серверам

Если доступ к серверам "Лаборатории Касперского" через системный DNS невозможен, Kaspersky Security Center может использовать публичные DNS-серверы в следующем порядке:

1. Google Public DNS (8.8.8.8).
2. Cloudflare DNS (1.1.1.1).
3. Alibaba Cloud DNS (223.6.6.6).
4. Quad9 DNS (9.9.9.9).
5. CleanBrowsing (185.228.168.168).

Запросы к DNS-серверам могут содержать доменные адреса и общедоступный IP-адрес Сервера администрирования, так как приложение устанавливает TCP/UDP-соединение с DNS-сервером. Если Kaspersky Security Center использует общедоступный DNS-сервер, обработка данных регулируется политикой конфиденциальности соответствующего сервиса.

► Чтобы настроить использование публичного DNS с помощью утилиты *klscflag*:

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой *klscflag*. Утилита *klscflag* расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Чтобы выключить использование публичного DNS, выполните следующую команду:

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
```
3. Чтобы включить использование публичного DNS, выполните следующую команду:

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
```

Окно Способ уведомления пользователей

В окне **Способ уведомления пользователей** можно настроить параметры уведомления пользователя об установке сертификата на мобильное устройство:

- **Показать QR-код в мастере.** При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения устройства.
- **Отправить QR-код пользователю.** При выборе этого варианта вы можете настроить параметры оповещения пользователя о подключении устройства.

В блоке параметров **По электронной почте** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью сообщений электронной почты. Этот способ оповещения доступен, только если настроен SMTP-сервер (см. раздел "Шаг 7. Настройка параметров отправки уведомлений по электронной почте" на стр. [288](#)).

В блоке параметров **С помощью SMS** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью SMS-сообщений. Этот способ оповещения доступен, только если включено SMS-оповещение.

По ссылке **Изменить сообщение** в блоках параметров **По электронной почте** и **С помощью SMS** просмотрите и при необходимости отредактируйте текст уведомления.

См. также:

Установка сертификата пользователю [842](#)

Окно Выборка устройств

В этом окне можно указать выборку устройств, сведения о которых будут отображаться в рабочей области на вкладке **Статистика узла Отчеты и уведомления**.

Выберите выборку из списка **Выборка устройств**. В списке перечислены выборки, заданные по умолчанию, и выборки, созданные пользователем.

Окно Определение названия создаваемого объекта

В окне укажите название создаваемого объекта. Имя не может превышать 100 символов и не может содержать специальные символы ("*<>? \:|).

Раздел Категории программ

В этом разделе можно настроить распространение информации о категориях приложений на клиентские устройства.

Передавать все данные (для Агентов администрирования версии Service Pack 2 и ниже)

Если выбран этот вариант, при изменении категории приложений на клиентские устройства передаются все данные категории. Этот вариант передачи данных используется для Агентов администрирования версии Service Pack 2 и ниже.

Передавать только измененные данные (для Агентов администрирования)

версии Service Pack 2 и выше)Если выбран этот вариант, при изменении категории приложений на клиентские устройства передаются не все данные категории, а только те данные, которые были изменены. Этот вариант передачи данных используется для Агентов администрирования версии Service Pack 2 и выше.

Используйте эти параметры в следующих задачах

Создание категорий приложений 574

Особенности работы с интерфейсом управления

Этот раздел содержит описание приемов работы в главном окне Kaspersky Security Center.

В этом разделе

Дерево консоли 921

Как обновить данные в рабочей области 925

Как перемещаться по дереву консоли 926

Как открыть окно свойств объекта в рабочей области.....926

Как выбрать группу объектов в рабочей области 926

Как изменить набор граф в рабочей области 926

Дерево консоли

Дерево консоли (см. рис. ниже) предназначено для отображения сформированной в сети иерархии Серверов администрирования, структуры их групп администрирования, а также других объектов приложения (например, папок **Хранилища** и **Управление приложениями**). Пространство имен Kaspersky

Security Center может содержать несколько узлов с именами серверов, соответствующих установленным и включенным в структуру сети Серверам администрирования.

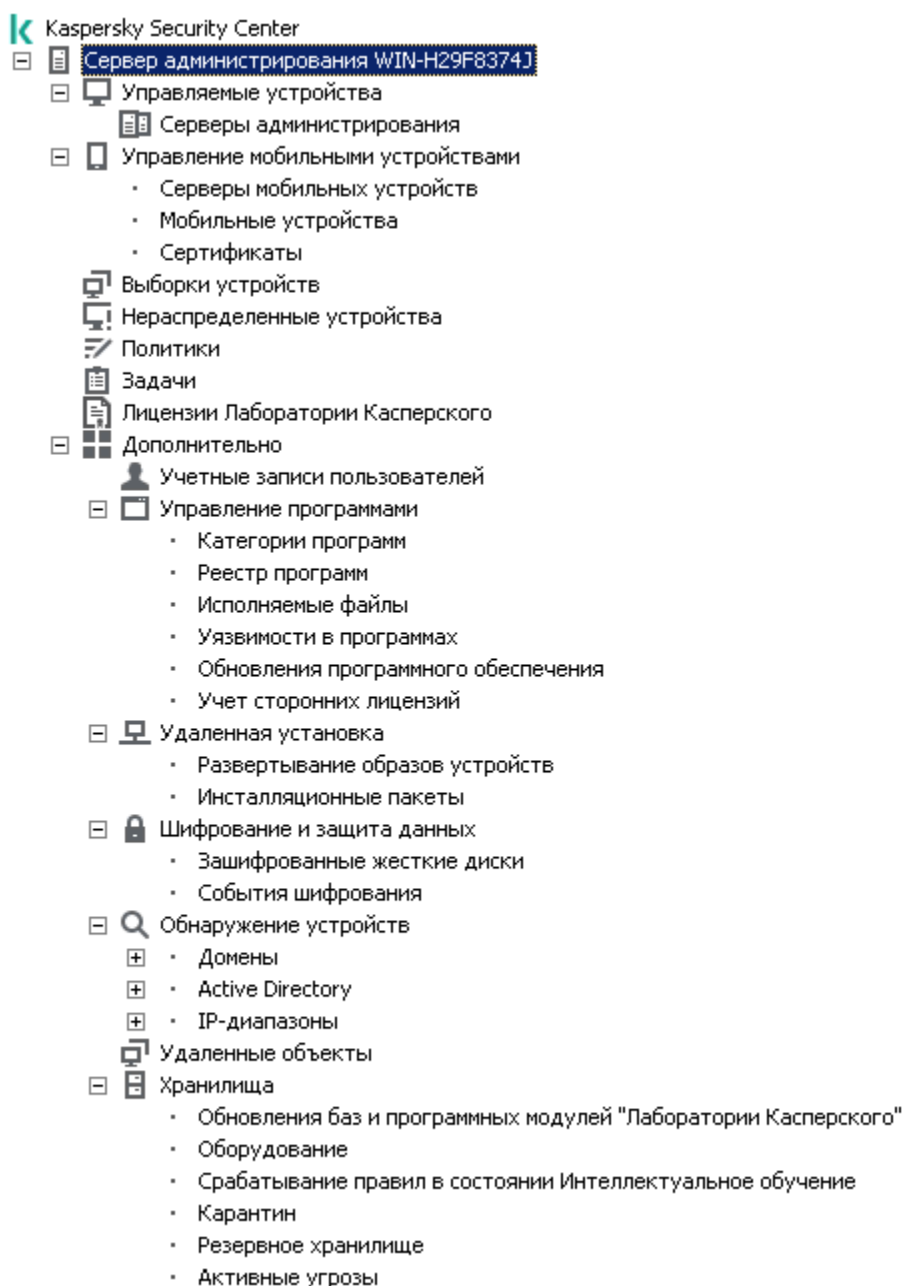


Рисунок 13. Дерево консоли

Узел Сервер администрирования

Узел **Сервер администрирования – <Имя устройства>** является контейнером и отображает структурную организацию указанного Сервера администрирования.

В рабочей области узла **Сервер администрирования** содержится сводная информация о текущем состоянии приложения и устройств, находящихся под управлением Сервера администрирования.

Информация в рабочей области распределена по вкладкам:

- **Мониторинг.** На вкладке Мониторинг в реальном времени отображается информация о работе приложения и текущем состоянии клиентских устройств. Важные сообщения для администратора (например, сообщения об уязвимостях, ошибках, обнаружении вирусов) выделяются цветом. По ссылкам на вкладке **Мониторинг** можно выполнять типовые задачи администратора (например, установить и настроить приложение безопасности на клиентских устройствах), а также переходить к другим папкам дерева консоли.
- **Статистика.** Содержит набор диаграмм, сгруппированных по темам (состояние защиты, антивирусная статистика, обновления и прочее). В диаграммах в визуальной форме представлена текущая информация о работе приложения и состоянии клиентских устройств.
- **Отчеты.** Содержит шаблоны отчетов, формируемых приложением. На вкладке вы можете формировать отчеты из предустановленных шаблонов, а также создавать собственные шаблоны отчетов.
- **События.** Содержит записи о событиях, зарегистрированных во время работы приложения. Для удобства чтения и сортировки записи распределены по тематическим выборкам. На вкладке вы можете просмотреть выборки событий, сформированные автоматически, а также создать собственные выборки.

Папки в составе узла Сервер администрирования

В состав узла **Сервер администрирования – <Имя устройства>** входят следующие папки:

- **Управляемые устройства.** Папка предназначена для хранения, отображения, настройки и изменения структуры групп администрирования, групповых политик и групповых задач.
- **Управление мобильными устройствами.** Папка предназначена для управления мобильными устройствами. Папка **Управление мобильными устройствами** содержит следующие вложенные папки:
 - **Серверы мобильных устройств.** Предназначена для управления Серверами iOS.
 - **Мобильные устройства.** Предназначена для управления мобильными устройствами KES и iOS MDM.
 - **Сертификаты.** Предназначена для управления сертификатами мобильных устройств.
- **Выборки устройств.** Папка предназначена для быстрого выбора устройств, соответствующих определенным критериям (выборки устройств), среди всех управляемых устройств. Например, вы можете быстро выбрать устройства, на которых не установлено приложение безопасности, и перейти к этим устройствам (просмотреть их список). С выбранными устройствами можно выполнять действия, например, назначать для них задачи. Вы можете использовать предустановленные выборки, а также создавать собственные (пользовательские) выборки.
- **Нераспределенные устройства.** В папке содержится список устройств, не входящих ни в одну группу администрирования. Вы можете выполнять действия с нераспределенными устройствами, например, перемещать их в группы администрирования, устанавливая на них приложения.
- **Политики.** Папка предназначена для просмотра и создания политик.
- **Задачи.** Папка предназначена для просмотра и создания задач.
- **Лицензии "Лаборатории Касперского".** Содержит список доступных лицензионных ключей для приложений "Лаборатории Касперского". В рабочей области папки вы можете добавлять новые лицензионные ключи в хранилище лицензионных ключей, распространять лицензионные ключи на управляемые устройства, просматривать отчет об использовании лицензионных ключей.

- **Дополнительно.** Папка содержит набор вложенных папок, соответствующих различным группам функциональностей приложения.

Папка Дополнительно. Перемещение папок в дереве консоли

В состав папки **Дополнительно** входят следующие папки:

- **Учетные записи пользователей.** Папка содержит список учетных записей пользователей сети.
- **Управление приложениями.** Папка предназначена для управления приложениями, установленными на устройствах в сети. Папка **Управление приложениями** содержит следующие вложенные папки:
 - **Категории приложений.** Предназначена для работы с пользовательскими категориями приложений.
 - **Реестр приложений.** Содержит список приложений на устройствах с установленным Агентом администрирования.
 - **Исполняемые файлы.** Содержит список исполняемых файлов, хранящихся на клиентских устройствах с установленным Агентом администрирования.
 - **Уязвимости в приложениях.** Содержит список уязвимостей в приложениях на устройствах с установленным Агентом администрирования.
 - **Обновления программного обеспечения.** Содержит список обновлений приложений, полученных Сервером администрирования, которые могут быть распространены на устройства.
 - **Учет сторонних лицензий.** Содержит список групп лицензионных приложений. С помощью групп лицензионных приложений можно отслеживать использование лицензий на сторонние приложения (не приложения "Лаборатории Касперского") и нарушение лицензионных ограничений.
- **Удаленная установка.** Папка предназначена для управления удаленной установкой операционных систем и приложений. Папка **Удаленная установка** содержит следующие вложенные папки:
 - **Развертывание образов устройств.** Предназначена для развертывания образов операционных систем на устройствах.
 - **Инсталляционные пакеты.** Содержит список инсталляционных пакетов, которые могут использоваться для удаленной установки приложений на устройства.
- **Шифрование и защита данных.** Папка предназначена для управления процессом шифрования данных на жестких и съемных дисках.
- **Опрос сети.** Папка предназначена для отображения сети, в которой установлен Сервер администрирования. Информацию о структуре сети и входящих в ее состав устройствах Сервер администрирования получает в ходе регулярных опросов сети Windows, IP-диапазонов и Active Directory, сформированных в сети организации. Результаты опросов отображаются в рабочих областях соответствующих папок: **Домены**, **IP-диапазоны** и **Active Directory**.
- **Хранилища.** Папка предназначена для работы с объектами, которые используются для мониторинга состояния устройств и их обслуживания. Папка **Хранилища** содержит следующие вложенные папки:
 - **Срабатывание правил в состоянии Интеллектуальное обучение.** Содержит список обнаружений, выполняемых правилами Kaspersky Endpoint Security, работающими в режиме Интеллектуального обучения на клиентских устройствах.
 - **Обновления и патчи ПО "Лаборатории Касперского".** Содержит список обновлений, полученных Сервером администрирования, которые могут быть распространены на устройства.

- **Оборудование.** Содержит список оборудования, подключенного к сети организации.
- **Карантин.** Содержит список объектов, помещенных антивирусными приложениями в карантинные папки на устройствах.
- **Резервное хранилище.** Папка содержит список резервных копий файлов, удаленных или измененных в процессе лечения на устройствах.
- **Необработанные файлы.** Содержит список файлов, для которых приложения безопасности определили необходимость отложенного лечения.

Вы можете изменять набор папок, вложенных в папку **Дополнительно**. Вложенные папки, которые активно используются, можно перемещать из папки **Дополнительно** на уровень выше. Папки, которые используются в работе редко, можно помещать в папку **Дополнительно**.

► Чтобы переместить из папки **Дополнительно** вложенную папку:

1. В дереве консоли выберите вложенную папку, которую вы хотите переместить из папки **Дополнительно**.
2. В контекстном меню вложенной папки выберите пункт **Вид** → **Переместить из папки Дополнительно**.

Вы также можете вынести вложенную папку из папки **Дополнительно** в рабочей области папки **Дополнительно**, по ссылке **Переместить из папки Дополнительно** в блоке с названием вложенной папки.

► Чтобы переместить папку в папку **Дополнительно**:

1. В дереве консоли выберите папку, которую нужно переместить в папку **Дополнительно**.
2. В контекстном меню папки выберите пункт **Вид** → **Переместить в папку Дополнительно**.

См. также:

Основной сценарий установки.....56

Как обновить данные в рабочей области

В Kaspersky Security Center данные рабочей области (такие как статусы устройств, статистика и отчеты) никогда не обновляются автоматически.

► Чтобы обновить данные в рабочей области, выполните одно из следующих действий:

- нажмите на клавишу **F5**;
- в контекстном меню объекта в дереве консоли выберите пункт **Обновить**;
- Нажмите на значок обновления () в рабочей области.

Как перемещаться по дереву консоли

Для перемещения по дереву консоли вы можете использовать следующие кнопки, расположенные в панели инструментов:

-  – переход на один шаг назад;
-  – переход на один шаг вперед;
-  – переход на один уровень вверх.

Можно также воспользоваться навигационной цепочкой, расположенной в правом верхнем углу рабочей области. Навигационная цепочка содержит полный путь к той папке дерева консоли, в которой вы находитесь в текущий момент. Все элементы цепочки, кроме последнего, являются ссылками на объекты дерева консоли.

Как открыть окно свойств объекта в рабочей области

Свойства большинства объектов Консоли администрирования можно изменять в окне свойств объекта.

► *Чтобы открыть окно свойств объекта, расположенного в рабочей области, выполните одно из следующих действий:*

- в контекстном меню объекта выберите пункт **Свойства**;
- выберите объект и нажмите комбинацию клавиш **ALT+ENTER**.

Как выбрать группу объектов в рабочей области

Вы можете выбрать группу объектов в рабочей области. Выбор группы объектов можно использовать, например, для создания набора устройств и последующего формирования задач для него.

► *Чтобы выбрать диапазон объектов:*

1. Выберите первый объект диапазона и нажмите на клавишу **SHIFT**.
2. Удерживая нажатой клавишу **SHIFT**, выберите последний объект диапазона.

Диапазон будет выбран.

► *Чтобы объединить отдельные объекты в группу:*

1. Выберите первый объект в составе группы и нажмите на клавишу **CTRL**.
2. Удерживая нажатой клавишу **CTRL**, выберите остальные объекты группы.

Объекты будут объединены в группу.

Как изменить набор граф в рабочей области

Консоль администрирования позволяет изменять набор граф, отображаемых в рабочей области.

► Чтобы изменить набор граф в рабочей области:

1. Выберите объект дерева консоли, для которого вы хотите изменить набор граф.
2. В рабочей области папки откройте окно настройки набора граф по ссылке **Добавить или удалить столбцы**.
3. В окне **Добавить или удалить столбцы** сформируйте набор граф для отображения.

Справочная информация

В этом разделе в таблицах представлена сводная информация о контекстном меню объектов Консоли администрирования, а также о статусах объектов дерева консоли и рабочей области.

В этом разделе

Команды контекстного меню	927
Список управляемых устройств. Значение граф	930
Статусы устройств, задач и политик	935
Значки статусов файлов в Консоли администрирования	937

Команды контекстного меню

В этом разделе содержится перечень объектов Консоли администрирования и соответствующий им набор пунктов контекстного меню (см. таблицу ниже).

Таблица 78. Элементы контекстного меню объектов Консоли администрирования

Объект	Пункт меню	Назначение пункта меню
Общие пункты контекстного меню	Поиск	Открыть окно поиска устройств.
	Обновить	Обновить отображение выбранного объекта.
	Экспортировать список	Экспортировать текущий список в файл.
	Свойства	Открыть окно свойств выбранного объекта.
	Вид → Добавить или удалить столбцы	Добавить или удалить графы в таблице объектов в рабочей области.
	Вид → Крупные значки	Отображать объекты в рабочей области в виде крупных значков.
	Вид → Мелкие значки	Отображать объекты в рабочей области в виде мелких значков.

Объект	Пункт меню	Назначение пункта меню
	Вид → Список	Отображать объекты в рабочей области в виде списка.
	Вид → Таблица	Отображать объекты в рабочей области в виде таблицы.
	Вид → Настройка интерфейса	Настроить отображение элементов Консоли администрирования.
Kaspersky Security Center	Создать → Сервер администрирования	Добавить в дерево консоли Сервер администрирования.
<Имя Сервера администрирования>	Подключиться к Серверу администрирования	Подключиться к Серверу администрирования.
	Отключиться от Сервера администрирования	Отключиться от Сервера администрирования.
Управляемые устройства	Установить приложение	Запустить мастер удаленной установки приложения.
	Вид → Настройка интерфейса	Настроить отображение элементов интерфейса.
	Удалить	Удалить Сервер администрирования из дерева консоли.
	Установить приложение	Запустить мастер удаленной установки для группы администрирования.
	Обнулить счетчик вирусов	Обнулить счетчики вирусов для устройств, входящих в состав группы администрирования.
	Просмотреть отчет об угрозах	Создать отчет об угрозах и вирусной активности устройств, входящих в состав группы администрирования.
	Создать → Группу	Создать группу администрирования.
	Все задачи → Новая структура групп	Создать структуру групп администрирования на основе структуры доменов или Active Directory.
	Все задачи → Показать сообщение	Запустить мастер создания сообщения для пользователей устройств, входящих в группу администрирования.
Управляемые устройства → Серверы администрирования	Создать → Подчиненный Сервер администрирования	Запустить мастер добавления подчиненного Сервера администрирования.

Объект	Пункт меню	Назначение пункта меню
	Создать → Виртуальный Сервер администрирования	Запустить мастер создания виртуального Сервера администрирования.
Управление мобильными устройствами → Мобильные устройства	Создать → Мобильное устройство	Подключить новое мобильное устройство пользователя.
Управление мобильными устройствами → Сертификаты	Создать → Сертификат	Создать сертификат.
	Создать → Мобильное устройство	Подключить новое мобильное устройство пользователя.
Выборки устройств	Создать → Новая выборка	Создать выборку устройств.
	Все задачи → Импортировать	Импортировать выборку из файла.
Лицензии Лаборатории Касперского	Добавить код активации или файл ключа	Добавить лицензионный ключ в хранилище Сервера администрирования.
	Активировать приложение	Запустить мастер создания задачи активации приложения.
	Отчет об использовании лицензионных ключей	Создать и просмотреть отчет о лицензионных ключах на клиентских устройствах.
Управление приложениями → Категории приложений	Создать → Категорию	Создать категорию приложений.
Управление приложениями → Реестр приложений	Фильтр	Настроить фильтр для списка приложений.
	Наблюдаемые приложения	Настроить публикацию событий об установке приложений.
	Удалить неустановленные приложения	Удалить из списка информацию о приложениях, которые уже не установлены на устройствах сети.
Управление приложениями → Обновления программного обеспечения	Принять Лицензионные соглашения обновлений	Принять Лицензионные соглашения обновлений программного обеспечения.
Управление приложениями → Учет сторонних лицензий	Создать → Группу лицензионных приложений	Создать группу лицензионных приложений.
Удаленная установка → Инсталляционные пакеты	Показать текущие версии приложений	Просмотреть список актуальных версий приложений "Лаборатории Касперского", выложенных на интернет-серверах.
	Создать → Инсталляционный пакет	Создать инсталляционный пакет.

Объект	Пункт меню	Назначение пункта меню
	Все задачи → Обновить базы	Обновить базы приложений в инсталляционных пакетах.
	Все задачи → Показать общий список автономных пакетов	Просмотреть список автономных инсталляционных пакетов, созданных для инсталляционных пакетов.
Обнаружение устройств → Домены	Все задачи → Активность устройств	Настроить параметры реакции Сервера администрирования на отсутствие активности устройств в сети.
Обнаружение устройств → IP-диапазоны	Создать → IP-диапазон	Создать IP-диапазон.
Хранилища → Обновления баз и модулей приложений "Лаборатории Касперского"	Загрузить обновления	Открыть окно свойств задачи загрузки обновлений в хранилище Сервера администрирования.
	Параметры загрузки обновлений	Настроить параметры задачи загрузки обновлений в хранилище Сервера администрирования.
	Отчет об используемых антивирусных базах	Создать и просмотреть отчет о версиях баз.
	Все задачи → Очистить хранилище обновлений	Очистить хранилище обновлений на Сервере администрирования.
Хранилища → Оборудование	Создать → Устройство	Создать сетевое устройство.

Список управляемых устройств. Значение граф

В таблице ниже представлены названия и описания граф списка управляемых устройств.

Таблица 79. Значение граф списка управляемых устройств

Название графы	Значение
Имя	NetBIOS-имя клиентского устройства. Описание значков имени устройств приведено в приложении (см. раздел "Статусы устройств, задач и политик" на стр. 935).
Тип операционной системы	Тип операционной системы клиентского устройства.
Windows-домен	Наименование Windows-домена, в котором находится клиентское устройство.
Агент администрирования установлен	Результат установки на клиентское устройство Агента администрирования: <i>Да, Нет, Нет данных</i> .

Название графы	Значение
Агент администрирования запущен	Результат функционирования Агента администрирования: <i>Да, Нет, Нет данных.</i>
Постоянная защита	Установлено приложение безопасности: <i>Да, Нет, Нет данных.</i>
Последнее подключение к Серверу администрирования	Время, прошедшее с момента соединения клиентского устройства с Сервером администрирования.
Последнее обновление антивирусных баз	Время, прошедшее с момента последнего обновления управляемых устройств.
Статус	Текущий статус клиентского устройства: <i>ОК, Критический, Предупреждение.</i>

Название графы	Значение
Описание статуса	Причины изменения статуса клиентского устройства на <i>Критический</i> или <i>Предупреждение</i>. Статус устройства изменяется на <i>Предупреждение</i> или <i>Критический</i> по следующим причинам: • Приложение безопасности не установлено. • Обнаружено много вирусов. • Уровень постоянной защиты отличается от уровня, установленного администратором. • Давно не выполнялся поиск вредоносного ПО. • Базы устарели. • Давно не подключался. • Обнаружены активные угрозы. • Требуется перезагрузка. • Установлены несовместимые приложения. • Обнаружены уязвимости в приложениях. • Давно не выполнялась проверка обновлений Центра обновления Windows. • Недопустимый статус шифрования. • Параметры мобильного устройства не соответствуют политике. • Есть необработанные проблемы безопасности. • Статус устройства определен приложением. • На устройстве заканчивается дисковое пространство. • Срок действия лицензии скоро истекает. Статус устройства изменяется только на <i>Критический</i> по следующим причинам: • Срок действия лицензии истек. • Устройство стало неуправляемым. • Защита выключена. • Приложение безопасности не запущено. Управляемые приложения "Лаборатории Касперского" на клиентских устройствах могут пополнять список описаний статусов. Kaspersky Security Center может получать описание статуса клиентского устройства от управляемых приложений "Лаборатории Касперского" на этом устройстве. Если статус, присвоенный устройству управляемыми приложениями, не совпадает со статусом, присвоенным Kaspersky Security Center, в Консоли администрирования отображается статус, наиболее критичный для безопасности устройства. Например, если одно из управляемых приложений присвоило устройству статус <i>Критический</i>, а Kaspersky Security Center – статус <i>Предупреждение</i>, то в Консоли администрирования для устройства отобразится статус <i>Критический</i> и описание этого статуса от управляемого приложения.
Информация обновлена	Время, прошедшее с момента последней успешной синхронизации клиентского устройства с Сервером администрирования (то есть с момента последнего опроса сети).
DNS-имя	Имя DNS-домена клиентского устройства.
DNS-домен	Основной DNS-суффикс.

Название графы	Значение
IP-адрес	IP-адрес клиентского устройства. Рекомендовано использовать IPv4 адрес.
Последнее появление в сети	Продолжительность видимости клиентского устройства в сети.
Последняя полная проверка	Дата и время последней проверки клиентского устройства, выполненной приложением безопасности по требованию пользователя.
Всего обнаружено угроз	Количество обнаруженных угроз.
Статус постоянной защиты	Статус постоянной защиты: <i>Запускается, Выполняется, Выполняется (максимальная защита), Выполняется (максимальная скорость), Выполняется (рекомендуемые параметры), Выполняется (с пользовательскими параметрами), Остановлена, Приостановлена, Сбой.</i>
IP-адрес соединения	IP-адрес подключения к Серверу администрирования Kaspersky Security Center.
Версия Агента администрирования	Версия Агента администрирования.
Версия приложения	Версия приложения безопасности, установленного на клиентском устройстве.
Выпуск антивирусных баз	Версия антивирусных баз.
Время начала последней сессии	Дата и время последнего включения клиентского устройства.
Требуется перезагрузка	Требуется перезагрузка клиентского устройства.
Точка распространения	Имя устройства, выполняющего роль точки распространения для этого клиентского устройства.
Описание	Описание клиентского устройства, полученное при сканировании сети.
Статус шифрования	Статус шифрования данных клиентского устройства.
Состояние WUA	Состояние Агент Центра обновления Windows клиентского устройства. Значение <i>Да</i> соответствует клиентским устройствам, которые получают обновления через Центр обновления Windows от Сервера администрирования. Значение <i>Нет</i> соответствует клиентским устройствам, которые получают обновления через Центр обновления Windows из других источников.

Название графы	Значение
Архитектура операционной системы	Разрядность операционной системы клиентского устройства.
Статус защиты от спама	Статус компонента защиты от спама: <i>Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Нет данных.</i>
Статус защиты данных от утечек	Статус компонента защиты от утечки данных: <i>Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Нет данных.</i>
Статус защиты для серверов совместной работы	Статус компонента фильтрации содержимого: <i>Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Нет данных.</i>
Статус антивирусной защиты почтовых серверов	Статус компонента антивирусной защиты почтовых серверов: <i>Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Нет данных.</i>
Статус Endpoint Sensor	Статус компонента Endpoint Detection and Response component (КАТА): <i>Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Нет данных.</i>
Создано	Время, когда значок <Имя устройства> был создан. Этот атрибут используется для сравнения различных событий друг с другом.
Имя виртуального или подчиненного Сервера администрирования	Имя виртуального или подчиненного Сервера администрирования. Эта графа доступна только в списках, содержащих устройства с разных Серверов администрирования.
Родительская группа	Название группы администрирования (см. стр. 44), в которой находится значок <Имя устройства>. Эта графа доступна только в списках, содержащих устройства с разных Серверов администрирования.
Под управлением другого Сервера администрирования	Параметр может принимать одно из следующих значений: • True – если при удаленной установке приложений безопасности на устройство окажется, что устройством управляет другой Сервер администрирования. • False в противном случае.
Номер сборки операционной системы	Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки (см. раздел "Настройка выборки устройств" см. стр. 623), кроме указанного.

Название графы	Значение
Идентификатор выпуска операционной системы	Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска (см. раздел "Настройка выборки устройств" см. стр. 623), кроме указанного.

Статусы устройств, задач и политик

В таблице ниже представлен список значков, отображающихся в дереве консоли и в рабочей области Консоли администрирования рядом с именами устройств, задач и политик. Эти значки характеризуют статус объектов.

Таблица 80. Статусы устройств, задач и политик

Иконка	Состояние
	Устройство с операционной системой для рабочих станций, обнаруженное в сети и не входящее в состав какой-либо группы администрирования.
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом <i>ОК</i> .
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом <i>Предупреждение</i> .
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом <i>Критический</i> .
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Устройство с операционной системой для серверов, обнаруженное в сети и не входящий в состав какой-либо группы администрирования.
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом <i>ОК</i> .
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом <i>Предупреждение</i> .
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом <i>Критический</i> .
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Мобильное устройство, обнаруженное в сети и не входящее в состав какой-либо группы администрирования.
	Мобильное устройство, входящее в состав группы администрирования, со статусом <i>ОК</i> .
	Мобильное устройство, входящее в состав группы администрирования, со статусом <i>Предупреждение</i> .

	Мобильное устройство, входящее в состав группы администрирования, со статусом <i>Критический</i> .
	Мобильное устройство, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Устройство с защитой на уровне UEFI, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. Устройство с защитой на уровне UEFI не в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>ОК</i> . Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>ОК</i> . Устройство с защитой на уровне UEFI не в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>Предупреждение</i> . Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>Предупреждение</i> . Устройство с защитой на уровне UEFI не в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>Критический</i> . Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>Критический</i> . Устройство с защитой на уровне UEFI не в сети.
	Активная политика.
	Неактивная политика.
	Активная политика, унаследованная от группы, созданной на главном Сервере администрирования.
	Активная политика, унаследованная от группы верхнего уровня иерархии.
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии <i>Ожидает выполнения</i> или <i>Завершена успешно</i> .
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии <i>Выполняется</i> .
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии <i>Сбой</i> .
	Задача, унаследованная от группы, созданной на главном Сервере администрирования.
	Задача, унаследованная от группы верхнего уровня иерархии.

Значки статусов файлов в Консоли администрирования

Для упрощения работы с файлами в Консоли администрирования Kaspersky Security Center рядом с именами файлов отображаются значки (см. таблицу ниже). Значки сигнализируют о статусах, присвоенных файлам управляемыми приложениями "Лаборатории Касперского" на клиентских устройствах. Значки отображаются в рабочей области папок **Карантин**, **Резервное хранилище** и **Активные угрозы**.

Статусы присваиваются объектам приложением Kaspersky Endpoint Security, установленным на клиентском устройстве, на котором находится объект.

Таблица 81. Соответствие значков статусам файлов

Иконка	Состояние
	Файл со статусом <i>Заражен</i> .
	Файл со статусом <i>Предупреждение</i> или <i>Возможно зараженный</i> .
	Файл со статусом <i>Добавлено пользователем</i> .
	Файл со статусом <i>Ложное срабатывание</i> .
	Файл со статусом <i>Вылечен</i> .
	Файл со статусом <i>Удален</i> .
	Файл в папке Карантин со статусом <i>Не заражен</i> , <i>Защищен паролем</i> или <i>Необходимо отправить в "Лабораторию Касперского"</i> . Если рядом со значком нет описания статуса, это означает, что управляемое приложение "Лаборатории Касперского" на клиентском устройстве передало Kaspersky Security Center неизвестный статус.
	Файл в папке Резервное хранилище со статусом <i>Не заражен</i> , <i>Защищен паролем</i> или <i>Необходимо отправить в "Лабораторию Касперского"</i> . Если рядом со значком нет описания статуса, это означает, что управляемое приложение "Лаборатории Касперского" на клиентском устройстве передало Kaspersky Security Center неизвестный статус.
	Файл в папке Активные угрозы со статусом <i>Не заражен</i> , <i>Защищен паролем</i> или <i>Необходимо отправить в "Лабораторию Касперского"</i> . Если рядом со значком нет описания статуса, это означает, что управляемое приложение "Лаборатории Касперского" на клиентском устройстве передало Kaspersky Security Center неизвестный статус.

Поиск и экспорт данных

В этом разделе содержится информация о способах поиска данных и об экспорте данных.

В этом разделе

Поиск устройств	938
Параметры поиска устройств	939
Использование масок в строковых переменных	950
Использование регулярных выражений в строке поиска	950
Экспорт списков из диалоговых окон	951

Поиск устройств

Kaspersky Security Center позволяет искать устройства на основании заданных критериев. Результаты поиска можно сохранить в текстовом файле.

Функция поиска позволяет находить следующие устройства:

- клиентские устройства в группах администрирования Сервера администрирования и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования и его подчиненных Серверов.

► Чтобы искать клиентские устройства, входящие в группу администрирования:

1. В дереве консоли выберите папку группы администрирования.
2. В контекстном меню папки группы администрирования выберите пункт **Поиск**.
3. На вкладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

► Чтобы искать нераспределенные устройства:

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Поиск**.
3. На вкладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

► Чтобы искать устройства независимо от того, входят они в состав групп администрирования или нет:

1. В дереве консоли выберите узел **Сервер администрирования %s**.
2. В контекстном меню узла Сервера администрирования выберите пункт **Поиск**.
3. На вкладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

В окне **Поиск** вы можете также искать группы администрирования и подчиненные Серверы администрирования с помощью раскрывающегося списка в правом верхнем углу окна. Поиск групп администрирования и подчиненных Серверов администрирования недоступен при открытии окна **Поиск** из папки **Нераспределенные устройства**.

Для поиска устройств вы можете использовать в полях ввода окна **Поиск** регулярные выражения (см. раздел «Использование регулярных выражений в строке поиска» на стр. [950](#)).

Полнотекстовый поиск в окне **Поиск** доступен:

- на вкладке **Сеть** в поле **Описание**;
- на вкладке **Оборудование** в полях **Устройство**, **Поставщик** и **Описание**.

См. также:

Параметры поиска устройств[939](#)

Параметры поиска устройств

Ниже представлены описания параметров поиска управляемых устройств (см. раздел "Поиск устройств" на стр. [938](#)). Результаты поиска отображаются в таблице в нижней части окна.

Сеть

На вкладке **Сеть** можно настроить критерии поиска устройств на основании их сетевых данных:

- **Имя устройства или IP-адрес**
Имя устройства в сети Windows (NetBIOS-имя).
- **Windows-домен**
Будут отображаться все устройства, входящие в указанный домен Windows.
- **Группа администрирования**
Будут отображаться устройства, входящие в указанную группу администрирования.
- **Описание**
Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие** или в разделе **Заметки**.
Для описания текста в поле **Комментарий** допустимо использовать следующие символы:

- Внутри одного слова:
 - *. Заменяет любую строку длиной 0 и более символов.

Пример:

Для описания слов **Сервер**, **Серверный** или **Серверная** можно

использовать строку **Сервер***

- **?**. Заменяет любой один символ.

Пример:

Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

Символ ***** или **?** не может использоваться как первый символ в описании текста.

- Для связи нескольких слов:
 - Пробел. Обозначает наличие в тексте хотя бы одного из слов, разделенных пробелами.

Пример:

Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

- **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

Пример:

Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

- **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

Пример:

Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

- **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

Пример:

Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

• IP-диапазон

Если флажок установлен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

По умолчанию флажок снят.

• Под управлением другого Сервера администрирования

Выберите одно из следующих значений:

- **Да**. Только клиентские устройства, управляемые другими Серверами администрирования, будут включены в выборку.
- **Нет**. Только клиентские устройства, управляемые этим же Сервером администрирования, будут включены в выборку.
- **Значение не выбрано**. Критерий не применяется.

Теги

На вкладке **Теги** можно настроить поиск устройств по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

- **Применить, если есть хотя бы один из выбранных тегов**

Если флажок установлен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если флажок снят, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию флажок снят.

- **Тег должен присутствовать**

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

По умолчанию выбран этот вариант.

- **Тег должен отсутствовать**

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Active Directory

На вкладке **Active Directory** можно указать, что устройства следует искать в подразделении (OU) или группе Active Directory. Также можно включить в выборку устройства из всех дочерних подразделений указанного подразделения Active Directory. Чтобы выбрать устройства, укажите следующие параметры:

- **Устройство в подразделении Active Directory**

Если флажок установлен, в выборку будут включаться устройства из подразделения Active Directory, указанного в поле ввода.

По умолчанию флажок снят.

- **Включать дочерние подразделения**

Если флажок установлен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

По умолчанию флажок снят.

- **Устройство является членом группы Active Directory**

Если флажок установлен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

По умолчанию флажок снят.

Сетевая активность

На вкладке **Сетевая активность** можно указать критерии поиска устройств на основании их сетевой активности:

- **Это устройство является точкой распространения**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** В выборку будут включены устройства, являющиеся агентами обновлений.
- **Нет.** Устройства, являющиеся агентами обновлений, не будут включены в выборку.
- **Значение не выбрано.** Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Включен.** В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
- **Выключен.** В выборку будут включаться устройства, на которых флажок **Не разрывать соединение с Сервером администрирования** снят.
- **Значение не выбрано.** Критерий не применяется.

- **Переключение профиля подключения**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Нет.** В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Значение не выбрано.** Критерий не применяется.

- **Последнее подключение к Серверу администрирования**

С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

Если флажок установлен, то в выборку попадают только новые устройства, обнаруженные при опросе сети за количество дней, которое указано в поле **Период обнаружения (сут)**.

Если флажок снят, то в выборку попадают все устройства, обнаруженные при опросе сети.

По умолчанию флажок снят.

- **Устройство в сети**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** Приложение включает в выборку устройства, которые видимы в сети в

настоящий момент.

- **Нет.** Приложение включает в выборку устройства, которые не видимы в сети в настоящий момент.
- **Значение не выбрано.** Критерий не применяется.

Приложение

На вкладке **Приложение** можно указать критерии поиска устройств на основании выбранного управляемого приложения:

- **Название приложения**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию приложения "Лаборатории Касперского".

В списке представлены названия только тех приложений, для которых на рабочем месте администратора установлены плагины управления.

Если приложение не выбрано, то критерий не применяется.

- **Версия приложения**

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии приложений "Лаборатории Касперского".

Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для приложения наименованию или номеру пакета обновления.

Если поле не заполнено, то критерий не применяется.

- **Последнее обновление модулей приложения**

С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей приложений, установленных на устройствах.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей приложений, установленных на устройствах.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Устройство находится под управлением Kaspersky Security Center**

В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

- **Да.** Приложение включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
- **Нет.** Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
- **Значение не выбрано.** Критерий не применяется.

- **Приложение безопасности установлено**

В раскрывающемся списке можно включить в состав выборки устройства, на которых установлено приложение защиты:

- **Да.** Приложение включает в выборку устройства, на которых установлено приложение защиты.
- **Нет.** Приложение включает в выборку устройства, на которых не установлено приложение защиты.
- **Значение не выбрано.** Критерий не применяется.

Операционная система

На вкладке **Операционная система** можно настроить следующие критерии поиска устройств на основании установленной на них операционной системы:

- **Версия операционной системы**

Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Архитектура операционной системы**

В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Неизвестно, x86, AMD64, IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Версия пакета обновления операционной системы**

В поле можно указать версию пакета установленной операционной системы (в формате X.Y), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Номер сборки операционной системы**

Этот параметр применим только для операционных систем Windows.

Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Идентификатор выпуска операционной системы**

Этот параметр применим только для операционных систем Windows.

Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

Статус устройства

На вкладке **Статус устройства** можно указать критерии поиска устройств по статусу устройства от управляемого приложения:

- **Статус устройства**

Раскрывающийся список, в котором можно выбрать один из статусов устройства:

OK, Критический, Предупреждение.

- **Статус постоянной защиты**

Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

- **Описание статуса устройства**

В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *OK, Критический, Предупреждение.*

- **Статус устройства определен приложением**

Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

Компоненты защиты

На вкладке **Компоненты защиты** можно настроить параметры поиска клиентских устройств по состоянию защиты.

- **Дата выпуска баз**

Если флажок установлен, поиск клиентских устройств выполняется по дате выпуска баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

По умолчанию флажок снят.

- **Последняя проверка**

Если флажок установлен, поиск клиентских устройств выполняется по времени последнего поиска вирусов. В полях ввода можно указать интервал, в течение которого поиск вирусов выполнялся в последний раз.

По умолчанию флажок снят.

- **Всего обнаружено угроз**

Если флажок установлен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

По умолчанию флажок снят.

Реестр приложений

На вкладке **Реестр приложений** можно настроить параметры поиска устройств в зависимости от того, какие приложения на них установлены:

- **Название приложения**

Раскрывающийся список, в котором можно выбрать приложение. Устройства, на которых установлено указанное приложение, будут включены в выборку.

- **Версия приложения**

Поле ввода, в котором указывается версия выбранного приложения.

- **Поставщик**

Раскрывающийся список, в котором можно выбрать производителя установленного на устройстве приложения.

- **Статус приложения**

Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено, Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

Если флажок установлен, поиск будет выполняться по данным об обновлении приложений, установленных на искомым устройствах. После установки флажка названия полей ввода **Название приложения** и **Версия приложения** меняются на **Имя обновления** и **Версия обновления**.

По умолчанию флажок снят.

- **Название несовместимого приложения безопасности**

Раскрывающийся список, в котором можно выбрать приложения защиты сторонних производителей. Во время поиска устройства, на которых установлено выбранное приложение, будут включены в выборку.

- **Тег приложения**

В раскрывающемся списке можно выбрать тег приложения. Все устройства, на которых установлены приложения, имеющие выбранный тег в описании, включаются в выборку устройств.

Иерархия Серверов администрирования

На вкладке **Иерархия Серверов администрирования**, установите флажок **Включая данные с подчиненных Серверов до уровня**, если вы хотите, чтобы информация, хранящаяся на подчиненных Серверах администрирования, учитывалась при поиске устройств, а в поле ввода можно указать уровень вложенности подчиненного Сервера администрирования, с которого учитывается информация при поиске устройств. По умолчанию флажок снят.

Виртуальные машины

На вкладке **Виртуальные машины** можно настроить параметры поиска устройств в зависимости от того, являются эти устройства виртуальными машинами или частью инфраструктуры виртуальных рабочих столов (VDI):

- **Является виртуальной машиной**

В раскрывающемся списке можно выбрать следующие элементы:

- **Да.** Искомые устройства должны являться виртуальными машинами.
- **Нет.** Искомые устройства не должны являться виртуальными машинами.

- **Тип виртуальной машины**

В раскрывающемся списке можно выбрать производителя виртуальной машины.

Раскрывающийся список доступен, если в раскрывающемся списке **Является виртуальной машиной** указано значение **Да**.

- **Часть Virtual Desktop Infrastructure**

В раскрывающемся списке можно выбрать следующие элементы:

- **Да.** Искомые устройства должны являться частью Virtual Desktop Infrastructure.
- **Нет.** Искомые устройства не должны являться частью Virtual Desktop Infrastructure.

Оборудование

На вкладке **Оборудование** можно настроить поиск клиентских устройств по установленному на них оборудованию:

- **Устройство**

В раскрывающемся списке можно выбрать тип оборудования, которое должно быть установлено на клиентском устройстве, чтобы оно отображалось в результатах поиска.

В поле поддерживается полнотекстовый поиск.

- **Поставщик**

В раскрывающемся списке можно выбрать производителя оборудования, которое должно быть установлено на устройстве, чтобы устройство отображалось в результатах поиска.

В поле поддерживается полнотекстовый поиск.

- **Описание**

Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Инвентарный номер**

Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Частота процессора (МГц)**

Диапазон частот процессора. Устройства с процессорами, соответствующими диапазону частот в полях ввода (включительно), будут включены в состав выборки.

- **Виртуальных ядер процессора**

Диапазон количества виртуальных ядер процессора. Устройства с процессорами, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ)**

Диапазон значений объема жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ)**

Диапазон значений объема оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону в полях ввода (включительно), будут включены в состав выборки.

Уязвимости и обновления

На вкладке **Уязвимости и обновления** можно настроить критерии поиска устройств по источнику обновлений Центра обновления Windows:

- **WUA переключен на Сервер администрирования**

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **Да.** Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Windows Update с Сервера администрирования.
- **Нет.** Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Windows Update из другого источника.

Пользователи

На вкладке **Пользователи** можно настроить параметры поиска устройств по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся указанным пользователем.

- **Пользователь, когда-либо выполнявший вход в систему**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Проблемы, связанные со статусом управляемых приложений

На вкладке **Проблемы, связанные со статусом управляемых приложений** можно настроить поиск по описаниям статусов устройств от управляемого приложения:

- **Описание статуса устройства**

Вы можете установить флажки для описаний статусов от управляемого приложения, при получении которых устройства будут включаться в выборку.

Статусы компонентов управляемых приложений

На вкладке **Статусы компонентов управляемых приложений** можно настроить поиск по статусам компонентов управляемых приложений:

- **Статус защиты данных от утечек**

Поиск устройств по статусу компонента защиты от утечки данных (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус защиты для серверов совместной работы**

Поиск устройств по статусу компонента защиты для серверов совместной работы (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу компонента антивирусной защиты почтовых серверов (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

Шифрование

- **Шифрование**

Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Возможные значения: *AES56, AES128, AES192, AES256*.

Облачные сегменты

На вкладке **Облачные сегменты** можно настроить поиск по принадлежности к облачным сегментам:

- **Устройство находится в облачном сегменте**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать сегмент поиска.

Если также установлен флажок **Включая вложенные объекты**, то поиск ведется по всем вложенным объектам указанного сегмента.

В результаты поиска включаются устройства только из выбранного сегмента.

- **Устройство обнаружено с помощью API**

В раскрывающемся списке можно выбрать, обнаруживается ли устройство средствами API.

- **Да.** Устройство обнаруживается с помощью AWS API. Это значит, что устройство обязательно находится в облачном окружении.
- **Нет.** Устройство не обнаруживается с помощью AWS API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но по каким-то причинам недоступно для поиска с помощью AWS API.
 - **Значение не выбрано.** Критерий не применяется.

Компоненты приложения

Этот раздел содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в Консоли администрирования.

В разделе **Компоненты приложения** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранному приложению:

- **Статус**

Поиск устройств в соответствии со статусом компонента, отправленным управляемым приложением на Сервер администрирования. Вы можете выбрать один из следующих статусов: *Нет данных от устройства, Остановлено, Запускается, Приостановлено, Выполняется, Сбой* или *Не установлено*. Если выбранный компонент приложения, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

Статусы, отправленные приложениями:

- *Запускается* – компонент в настоящее время находится в процессе инициализации.
- *Выполняется* – компонент включен и работает правильно.
- *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемом приложении.
- *Сбой* – во время выполнения операции компонента произошла ошибка.
- *Остановлено* – компонент отключен и в данный момент не работает.
- *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки приложения.

В отличие от других статусов, статус *Нет данных от устройства* не отправляется управляемым приложением. Этот параметр показывает, что приложения не имеют информации о выбранном статусе компонента. Например, это может произойти, если выбранный компонент не принадлежит ни одному из приложений, установленных на устройстве, или устройство выключено.

• Версия

Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, 3.4.1.0, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

См. также:

Использование регулярных выражений в строке поиска	950
Поиск устройств	938

Использование масок в строковых переменных

Для строковых переменных допустимо использование масок. Для создания масок вы можете использовать следующие регулярные выражения:

- Знак подстановки (*) – любая строка длиной 0 или более символов.
- Вопросительный знак (?) – один любой символ.
- [<интервал>] – Заменяет один символ из заданного диапазона или множества.
Например: [0–9] – любая цифра. [abcdef] – один из символов a, b, c, d, e, f.

Использование регулярных выражений в строке поиска

Для поиска отдельных слов и символов вы можете использовать в строке поиска следующие регулярные выражения:

- *. Заменяет последовательность любого количества символов. Например, для поиска слов "Сервер", "Серверный" или "Серверная" в строке поиска нужно ввести выражение `Сервер*`.
- ?. Заменяет любой один символ. Например, для поиска слов "Окно" или "Окна" в строке поиска нужно ввести выражение `Окн?`.

Текст в строке поиска не может начинаться с ?.

- [[интервал](#)]. Заменяет один символ из заданного диапазона или множества. Например, для поиска любой цифры в строке поиска нужно ввести выражение [\[0–9\]](#). Для поиска одного из символов a, b, c, d, e, f в строке поиска нужно ввести выражение [\[abcdef\]](#).

Для полнотекстового поиска вы можете использовать в строке поиска следующие регулярные выражения:

- Пробел. Результат: все устройства, описания которых содержат любое из перечисленных слов. Например, для поиска фразы, содержащей слово "Подчиненный" или "Виртуальный" (или оба этих слова), в строке поиска нужно ввести выражение [Подчиненный Виртуальный](#).
- Знак "плюс" (+), AND или &&. При написании перед словом обозначает обязательное наличие слова в тексте. Например, для поиска фразы, содержащей и слово "Подчиненный", и слово "Виртуальный", в строке поиска можно ввести выражения: [+Подчиненный+Виртуальный](#), [Подчиненный AND Виртуальный](#), [Подчиненный && Виртуальный](#).
- OR или ||. При написании между словами обозначает наличие одного или другого слова в тексте. Например, для поиска фразы, содержащей или слово "Подчиненный", или слово "Виртуальный", в строке поиска можно ввести выражения: [Подчиненный OR Виртуальный](#), [Подчиненный || Виртуальный](#).
- Знак "минус" (-). При написании перед словом обозначает обязательное отсутствие слова в тексте. Например, для поиска фразы, в которой должно присутствовать слово "Подчиненный", и должно отсутствовать слово "Виртуальный", нужно ввести в строке поиска выражение [+Подчиненный-Виртуальный](#).
- "[<фрагмент текста>](#)". Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте. Например, для поиска фразы, содержащей словосочетание "Подчиненный Сервер", нужно ввести в строке поиска выражение "[Подчиненный Сервер](#)".

Полнотекстовый поиск доступен в следующих блоках фильтрации:

- в блоке фильтрации списка событий по графам **Событие** и **Описание**;
- в блоке фильтрации учетных записей пользователей по графе **Имя**;
- в блоке фильтрации реестра приложений по графе **Название**, если в блоке **Показывать в списке** выбран критерий фильтрации **без группировки**.

Экспорт списков из диалоговых окон

В диалоговых окнах приложения вы можете экспортировать в текстовые файлы списки объектов.

Экспорт списка объектов возможен для тех разделов диалогового окна, которые содержат кнопку **Экспортировать в файл**.

Параметры задач

В этом разделе перечислены параметры задач Kaspersky Security Center.

В этом разделе

Общие параметры задач.....	952
Параметры задачи загрузки обновлений в хранилище Сервера администрирования.....	959
Параметры задачи загрузки обновлений в хранилища точек распространения	960
Параметры задачи поиска уязвимостей и требуемых обновлений.	961
Параметры задачи установки требуемых обновлений и закрытия уязвимостей	963

Общие параметры задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:

- Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

- Параметры расписания задачи:

- **Параметры Запуск по расписанию:**

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и

Начать с. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрывающимся списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При загрузке обновлений в хранилище**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При загрузке обновлений в хранилище**, задача будет запускаться после загрузки

обновлений в хранилище.

- **При обнаружении вирусной атаки**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемым списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемом списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** — только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать случайную задержку запуска задачи в интервале (мин)**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- Окно Выбор устройств, которым будет назначена задача:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**

В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **Задать адреса устройств вручную или импортировать из списка**

Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- Параметры учетной записи:

- **Учетная запись по умолчанию**

Задача будет запускаться под той же учетной записью, под которой была установлено и запущено приложение, выполняющее эту задачу.

По умолчанию выбран этот вариант.

- **Задать учетную запись**

Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

- **Учетная запись**

Учетная запись, от имени которой будет запускаться задача.

- **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:
 - **Распределить по подгруппам**
 - **Распространить на подчиненные и виртуальные Серверы администрирования**
- Дополнительные параметры расписания:
 - **Активировать устройства перед запуском задачи функцией Wake-on-LAN за (мин)**

Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройства после выполнения задачи**. Параметр находится в этом же окне.

По умолчанию параметр выключен.

- **Выключать устройства после выполнения задачи**

Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

По умолчанию параметр выключен.

- **Остановить, если задача выполняется дольше (мин)**

По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:
 - Блок **Сохранять информацию о результатах:**
 - **На Сервере администрирования в течение (сут)**

События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

По умолчанию параметр включен.

- **Хранить в журнале событий ОС на устройстве**

События приложения, связанные с выполнением задачи, хранятся локально в журнале событий Windows каждого клиентского устройства.

По умолчанию параметр выключен.

- **Хранить в журнале событий ОС на Сервере**

События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в журнале событий Windows операционной системы Сервера администрирования.

По умолчанию параметр выключен.

- **Сохранять все события**

Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

- **Сохранять события, связанные с ходом выполнения задачи**

Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением задачи.

- **Сохранять только результат выполнения задачи**

Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

- **Уведомлять администратора о результатах**

Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

По умолчанию отключены все способы уведомлений.

- **Уведомлять только об ошибках**

Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

По умолчанию параметр включен.

- Параметры безопасности
- Параметры области действия задачи

В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

- **Устройства**

Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

- **Выборка устройств**

Вы можете изменить выборку устройств, к которым применяется задача.

- **Исключения из области действия задачи**

Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**

Параметры задачи загрузки обновлений в хранилище Сервера администрирования

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Источники обновлений**
- **Прочие параметры**

Принудительно обновить подчиненные Серверы

Если параметр включен, после получения обновлений Сервер администрирования будет запускать задачи получения обновлений подчиненными Серверами администрирования. В противном случае задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

По умолчанию параметр выключен.

Копировать полученные обновления в дополнительные папки

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

По умолчанию параметр выключен.

Не обновлять устройства и подчиненные Серверы администрирования принудительно до окончания копирования

Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

По умолчанию параметр выключен.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Раздел **Параметры**, блок **Состав обновлений**:

Загрузить файлы различий

Этот параметр включает функцию загрузки файлов различий (см. раздел "Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского" см. стр. [467](#)).

По умолчанию параметр выключен.

- Раздел **Проверка обновлений**

Выполнять проверку обновлений перед распространением

Задача проверки обновлений

Эта задача проверяет загруженные обновления перед тем как распространить их на все устройства, для которых Сервер администрирования выбран в качестве источника обновлений.

В этом поле можно указать задачу *Проверка обновлений*, которая была создана ранее. Также вы можете создать другую задачу *Проверка обновлений*.

См. также:

Общие параметры задач.....	952
Создание задачи для загрузки обновлений в хранилище Сервера администрирования.....	469
Проверка полученных обновлений	479

Параметры задачи загрузки обновлений в хранилища точек распространения

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Источники обновлений**

- **Прочие параметры → Папка для хранения обновлений**

Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

Параметры, заданные после создания задачи

Вы можете указать следующие параметры в разделе **Параметры** в блоке **Состав обновлений** только после создания задачи.

Загрузить файлы различий

Этот параметр включает функцию загрузки файлов различий (см. раздел "Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского" см. стр. [467](#)).

По умолчанию параметр выключен.

См. также:

Общие параметры задач.....	952
Создание задачи загрузки обновлений в хранилища точек распространения	474

Параметры задачи поиска уязвимостей и требуемых обновлений.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Соединяться с сервером обновлений для актуализации данных**

Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

- Сервер администрирования Kaspersky Security Center (см. параметры политики Агента администрирования (см. стр. [789](#))).
- Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
- Серверы обновления Microsoft.

Если этот параметр включен, Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows,

которую он получил из источника обновлений Microsoft ранее и которая хранится в кеше устройства.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент Центра обновления Windows на управляемом устройстве подключается к серверу обновлений Microsoft, чтобы получить обновления, только если включен параметр **Соединиться с сервером обновлений для актуализации данных** и параметр **Активный** в группе параметров **Режим поиска Центра обновления Windows**.
- Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, полученную ранее от источника обновлений Microsoft и сохраненную в кеше устройства, если включен параметр **Соединиться с сервером обновлений для актуализации данных** и параметр **Пассивный** в группе параметров **Режим поиска Центра обновления Windows**, или если параметр **Соединиться с сервером обновлений для актуализации данных** выключен, а в группе параметров **Режим поиска Центра обновления Windows** выбран параметр **Активный**.
- Независимо от параметра **Соединиться с сервером обновлений для актуализации данных** (включен он или выключен), если в группе параметров **Выключен** выбран параметр **Режим поиска Центра обновления Windows**, Kaspersky Security Center не запрашивает информацию об обновлениях.

• Поиск уязвимостей и сторонних обновлений, перечисленных "Лабораторией Касперского"

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

По умолчанию параметр включен.

• Укажите пути для дополнительного поиска приложений в файловой системе

Папки, в которых Kaspersky Security Center выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. раздел "Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center" см. стр. [773](#)), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

См. также:

Общие параметры задач.....	952
Поиск уязвимостей в приложениях	535

Параметры задачи установки требуемых обновлений и закрытия уязвимостей

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Задать правила установки обновлений**

Эти правила применяются при установке обновлений на клиентские устройства. Если правила не указаны, задача не выполняется. Дополнительную информацию о работе с правилами см. в разделе Правила установки обновлений (см. стр. [567](#)).

- **Начинать установку в момент перезагрузки или выключения устройства**

Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

По умолчанию параметр выключен.

- **Устанавливать требуемые общесистемные компоненты**

Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (прerequisites), необходимые для установки этого обновления. Например, такими prerequisites могут являться обновления операционной системы.

Если этот параметр выключен, необходимо установить prerequisites вручную.

По умолчанию параметр выключен.

- **Разрешать установку новой версии приложения при обновлении**

Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии приложения.

Если этот параметр выключен, приложение не обновляется. Можно позднее установить новые версии приложений вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию приложения или если требуется проверить обновление в тестовой инфраструктуре.

По умолчанию параметр включен.

После установки новой версии приложения может быть нарушена работа других приложений, установленных на клиентских устройствах и зависящих от работы обновляемой приложения.

- **Загружать обновления на устройство, не устанавливая их**

Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Загрузить обновления для**.

Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

По умолчанию параметр выключен.

- **Загрузить обновления для**

Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине

значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. раздел "Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center" см. стр. [773](#)), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Параметры, заданные после создания задачи

Вы можете задать параметры, перечисленные ниже, только после создания задачи. Полное описание параметров задачи см. в разделе Общие параметры задач (на стр. [952](#)).

- **Общие.** В этом разделе отображается общая информация о задаче. Также можно указать, на какие устройства должна применяться задача *Установка требуемых обновлений и закрытие уязвимостей*:
 - **Распределить по подгруппам**
 - **Распространить на подчиненные и виртуальные Серверы администрирования**
- Обновления для установки

В разделе **Обновления для установки** вы можете просмотреть список обновлений, которые заданы в задаче. Отображаются только обновления, соответствующие параметрам выбранной задачи.

- Пробная установка обновлений:
 - **Не проверять.** Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.
 - **Выполнить проверку на указанных устройствах.** Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.
 - **Выполнить проверку на устройствах в указанной группе.** Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задать тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.
 - **Выполнить проверку на указанном проценте устройств.** Выберите этот вариант, если вы хотите выполнить проверку обновлений на части устройств. В поле **Процент тестовых**

устройств из общего числа устройств укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.

См. также:

Общие параметры задач.....	952
Установка обновлений на устройства вручную.....	513
Заккрытие уязвимостей в приложениях	541

Глобальный список подсетей

В этом разделе приведена информация и глобальном списке подсетей, которые вы можете использовать в правилах.

Чтобы сохранить информацию о подсетях вашей сети, вы можете настроить глобальный список подсетей для каждого Сервера администрирования. Этот список позволит сопоставить пары {IP-адрес, маска} и физические единицы, такие как офисы филиалов. Вы можете использовать подсети из этого списка в сетевых правилах и параметрах.

Добавление подсети в глобальный список подсетей

Вы можете добавлять подсети и их описание в глобальный список подсетей.

► *Чтобы добавить подсеть в глобальный список подсетей:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне **Свойства** в панели **Разделы** выберите раздел **Список глобальных подсетей**.
4. Нажмите на кнопку **Добавить**.
Откроется окно **Новая подсеть**.
5. Заполните следующие поля:

- **Общие параметры**

IP-адрес подсети, которую вы добавляете.

- **Маска подсети**

Маска подсети, которую вы добавляете.

- **Имя**

Имя подсети. Имя подсети должно быть уникальным для всего глобального списка подсетей. Если вы указали имя подсети, которое уже существует в списке, то ей будет добавлен индекс, например: ~~1, ~~2.

- **Описание**

Описание может содержать дополнительную информацию, например, о филиале, которому принадлежит эта подсеть. Этот текст возникает везде, где отображается список подсетей, например, в списке правил ограничения трафика.

Это поле не обязательно для заполнения и может быть пустым.

1. Нажмите на кнопку **ОК**.

Подсеть появится в списке подсетей.

Просмотр и изменение свойств подсети в глобальном списке подсетей

Вы можете просматривать и изменять свойства подсетей в глобальном списке подсетей.

► *Чтобы просмотреть или изменить свойства подсети в глобальном списке подсетей:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне **Свойства** в панели **Разделы** выберите раздел **Список глобальных подсетей**.
4. В списке выберите требуемую подсеть.
5. Нажмите на кнопку **Свойства**.
Откроется окно **Новая подсеть**.
6. Если необходимо, измените параметры (см. раздел "Добавление подсети в глобальный список подсетей" на стр. [966](#)) подсети.
7. Нажмите на кнопку **ОК**.

Если вы сделали изменения, то они будут сохранены.

Использование Агента администрирования для Windows, macOS и Linux: сравнение

Использование Агента администрирования зависит от операционной системы устройства. Свойства политики Агента администрирования (см. раздел "Параметры политики Агента администрирования" см. стр. [789](#)) и инсталляционного пакета (см. раздел "Параметры инсталляционного пакета Агента администрирования" на стр. [201](#)) зависят от операционной системы. В таблице ниже сравниваются возможности и сценарии использования Агента администрирования, доступные для операционных систем Windows, macOS и Linux.

Таблица 82. Сравнение функций Агента администрирования

Функция Агента администрирования	Windows	macOS	Linux
Установка			
Автоматическое создание инсталляционного пакета Агента администрирования, после установки Kaspersky Security Center (см. раздел "Инсталляционные пакеты" на стр. 165)	✓	—	—

Функция Агента администрирования	Windows	macOS	Linux
Принудительная установка с помощью соответствующих параметров задачи удаленной установки приложения Kaspersky Security Center (см. раздел "Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center" на стр. 171)	✓	✓	✓
Установка приложений с помощью рассылки пользователям устройств ссылок на автономные пакеты, сформированные Kaspersky Security Center (см. раздел "Запуск автономных пакетов, сформированных Kaspersky Security Center" на стр. 173)	✓	✓	✓
Установка путем клонирования образа жесткого диска с операционной системой и установленным Агентом администрирования, средствами, предоставляемыми Kaspersky Security Center для работы с образами дисков (см. раздел "Развертывание захватом и копированием образа устройства" на стр. 167)	✓	—	—
Установка методом клонирования образа жесткого диска администратора с операционной системой и Агентом администрирования сторонними средствами (см. раздел "Развертывание захватом и копированием образа устройства" на стр. 167)	✓	✓	✓
Установка приложений с помощью сторонних средств удаленной установки приложений (см. раздел "Развертывание при помощи сторонних средств удаленной установки приложений" на стр. 166)	✓	✓	✓
Установка вручную с помощью запуска инсталляторов приложений на устройствах (см. раздел "Возможности ручной установки приложений" на стр. 174)	✓	✓	✓
Установка Агента администрирования в тихом режиме (см. раздел "Установка в тихом режиме (с файлом ответов)" на стр. 179)	✓	✓	✓
Подключение клиентского устройства к Серверу администрирования вручную (см. раздел "Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover" на стр. 750)	✓	✓	✓
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center (на стр. 487)	✓	—	✓
Автоматическое распространение ключа (см. раздел "Автоматическое распространение лицензионного ключа." на стр. 398)	✓	✓	✓

Функция Агента администрирования	Windows	macOS	Linux
Принудительная синхронизация (см. раздел "О принудительной синхронизации" на стр. 764)	✓	✓	✓
Точка распространения			
Использование точки распространения (см. раздел "О точках распространения" на стр. 147)	✓	✓	✓
Автоматическое назначение точек распространения (см. раздел "Расчет количества и конфигурации точек распространения" на стр. 149)	✓	Без использования Network Location Awareness (NLA).	Без использования Network Location Awareness (NLA).
Опрос сети (см. раздел "Обнаружение устройств" на стр. 324)	✓ - Опрос сети Windows - Опрос IP-диапазонов - Опрос контроллеров домена (Microsoft Active Directory)	✓ - Опрос IP-диапазонов - Опрос Zeroconf - Опрос контроллеров домена (Microsoft Active Directory, Samba 4 Active Directory)	—
Запуск службы прокси-сервер KSN на стороне точки распространения (см. раздел "Назначение устройства точкой распространения вручную" на стр. 491)	✓	—	✓

Функция Агента администрирования	Windows	macOS	Linux
Загрузка обновлений через серверы обновлений "Лаборатории Касперского" в хранилища точек распространения, которые распространяют обновления на управляемые устройства (см. раздел "Создание задачи загрузки обновлений в хранилища точек распространения" на стр. 474)	✓	— Если устройств с операционной системой Linux или macOS находятся в области действия задачи Загрузка обновлений в хранилища точек распространения, задача завершится со статусом Сбой, даже если она успешно завершилась на всех устройствах с операционной системой Windows.	✓

Функция Агента администрирования	Windows	macOS	Linux
Принудительная установка приложений	✓	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой macOS.	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой Linux.
Использовать в качестве push-сервера (см. раздел "Использование точки распространения в качестве извещающего сервера" на стр. 697)	✓	—	✓
Работа с приложениями сторонних производителей			
Удаленная установка приложений на устройства (см. раздел "Удаленная установка приложений на устройства с установленным Агентом администрирования" на стр. 174)	✓	—	—
Обновления программного обеспечения (см. раздел "Установка обновлений приложений сторонних производителей" на стр. 498)	✓	—	—
Настройка обновлений операционной системы в политике Агента администрирования (см. раздел "Настройка обновлений Windows в политике Агента администрирования" на стр. 526)	✓	—	—
Просмотр информации об уязвимостях в приложениях (на стр. 533)	✓	—	—
Поиск уязвимостей в приложениях (на стр. 535)	✓	—	—

Функция Агента администрирования	Windows	macOS	Linux
Инвентаризация программного обеспечения, установленного на устройствах (см. раздел "Изменение времени начала инвентаризации программного обеспечения" на стр. 586)	✓	—	✓
Виртуальные машины			
Установка Агента администрирования на виртуальные машины (см. раздел "Виртуальная инфраструктура" на стр. 187)	✓	✓	✓
Оптимизация параметров для VDI (см. раздел "Рекомендации по снижению нагрузки на виртуальные машины" на стр. 188)	✓	✓	✓
Поддержка динамических виртуальных машин (на стр. 189)	✓	✓	✓
Другое			
Аудит действий на удаленном клиентском устройстве с помощью совместного доступа к рабочему столу Windows (см. раздел "Аудит действий на удаленном клиентском устройстве" на стр. 756)	✓	—	—
Мониторинг состояния антивирусной защиты (см. раздел "Отслеживание состояния антивирусной защиты с помощью информации в системном реестре" на стр. 682)	✓	✓	✓
Управление перезагрузкой устройств (см. раздел "Настройка перезагрузки клиентского устройства" на стр. 755)	✓	—	—
Поддержка отката файловой системы (см. раздел "Поддержка отката файловой системы для устройств с Агентом администрирования" на стр. 190)	✓	✓	✓
Использование Агента администрирования в качестве шлюза соединений (см. раздел "Об использовании точки распространения в качестве шлюза соединений" на стр. 695)	✓	✓	✓
Менеджер соединений (см. раздел "О расписании соединений" на стр. 765)	✓	✓	✓
Переключение Агента администрирования с одного Сервера администрирования на другой (автоматически по сетевому местоположению) (см. раздел "О переключении Агента администрирования на другой Сервер администрирования" на стр. 307)	✓	✓	—
Проверка соединения клиентского устройства с Сервером администрирования. Утилита klnagchk (см. раздел "Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита klnagchk" на стр. 757)	✓	✓	✓

Функция Агента администрирования	Windows	macOS	Linux
Удаленное подключение к рабочему столу клиентского устройства (на стр. 752)	✓	✓ С помощью системы Virtual Network Computing (VNC).	—
Загрузка автономного инсталляционного пакета с помощью мастера переноса данных	✓	✓	✓
Опрос Zeroconf (на стр. 331)	—	—	✓

См. также:

Развертывание Агента администрирования и приложения безопасности	163

Kaspersky Security Center Web Console.

В этом разделе описаны действия, которые вы можете выполнять с помощью Kaspersky Security Center Web Console.

В этом разделе

О Kaspersky Security Center Web Console.....	975
Аппаратные и программные требования Kaspersky Security Center Web Console	976
Схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console	979
Порты, используемые приложением Kaspersky Security Center Web Console	980
Интерфейс Kaspersky Security Center Web Console	982
Закрепление и отмена закрепления разделов главного меню.....	983
Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985
Установка.....	987
Перенос данных из Kaspersky Security Center Windows.....	999
Вход в приложение Kaspersky Security Center Web Console и выход из него	1006
Identity and Access Manager в Kaspersky Security Center Web Console.....	1008
Настройка доменной аутентификации с использованием протоколов NTLM и Kerberos	1015
Настройка Сервера администрирования	1016
Первоначальная настройка Kaspersky Security Center Web Console	1047
Мастер развертывания защиты	1076
Развертывание приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console	1084
Обнаружение устройств в сети.....	1109
Приложения "Лаборатории Касперского": лицензирование и активация	388
Настройка защиты сети	401
Сценарий: обновление Kaspersky Security Center и управляемых приложений безопасности.....	1333
Обновление баз и приложений "Лаборатории Касперского"	1335
Управление приложениями сторонних производителей на клиентских устройствах	1379
Мониторинг и отчеты	1466
Журнал активности Kaspersky Security Center Web Console	1563
Интеграция Kaspersky Security Center с другими решениями	1564
Удаленная диагностика клиентских устройств	1580
Изменение языка интерфейса Kaspersky Security Center Web Console	1590

О Kaspersky Security Center Web Console

Kaspersky Security Center Web Console представляет собой приложение (веб-приложение), предназначенное для контроля состояния системы безопасности сетей организации, находящихся под защитой приложений "Лаборатории Касперского".

С помощью приложения вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- устанавливать приложения "Лаборатории Касперского" на устройства вашей сети и управлять установленными приложениями;
- управлять политиками, сформированными для устройств вашей сети;
- управлять учетными записями пользователей;
- управлять задачами приложений, установленных на устройствах сети;
- просматривать отчеты о состоянии системы безопасности;
- управлять рассылкой отчетов заинтересованным лицам: системным администраторам и другим IT-специалистам.

Kaspersky Security Center Web Console предоставляет веб-интерфейс, который обеспечивает ваше взаимодействие с Сервером администрирования с помощью браузера. Сервер администрирования – это приложение, которое служит для управления приложениями "Лаборатории Касперского", установленными на устройства вашей сети. Сервер администрирования связывается с устройствами вашей сети через защищенные (SSL) каналы связи. Когда вы с помощью браузера подключаетесь к Kaspersky Security Center Web Console, браузер устанавливает с Сервером Kaspersky Security Center Web Console защищенное (HTTPS) соединение.

Kaspersky Security Center Web Console работает следующим образом:

1. Вы подключаетесь к Kaspersky Security Center Web Console с помощью браузера, в окне которого отображаются страницы веб-портала приложения.
2. С помощью элементов управления веб-портала вы выбираете команду, которую хотите выполнить. Kaspersky Security Center Web Console выполняет следующие действия:
 - Если вы выбрали команду, связанную с получением информации (например, просмотр списка устройств), Kaspersky Security Center Web Console формирует запрос на получение информации к Серверу администрирования, затем получает от него необходимые данные и передает их браузеру в удобном для отображения виде.
 - Если вы выбрали команду управления (например, удаленная установка приложения), Kaspersky Security Center Web Console получает команду от браузера и передает ее Серверу администрирования. Затем приложение получает результат выполнения команды от Сервера администрирования и передает результат браузеру в удобном для отображения виде.

Kaspersky Security Center Web Console представляет собой многоязыковое приложение. Вы можете изменить язык интерфейса в любое время без повторного открытия приложения. Если вы устанавливаете Kaspersky Security Center Web Console совместно с Kaspersky Security Center, Kaspersky Security Center Web Console имеет тот же язык интерфейса что и установочный файл. Если вы устанавливаете только Kaspersky Security Center Web Console, приложение имеет тот же язык что и операционная система. Если Kaspersky Security Center Web Console не поддерживает язык установочного файла или операционной системы, по умолчанию устанавливается английский язык.

Управление мобильными устройства не поддерживается в Kaspersky Security Center Web Console. Однако если вы добавили мобильные устройства в группу администрирования в Консоли администрирования, эти устройства также отображаются в Kaspersky Security Center Web Console.

Аппаратные и программные требования Kaspersky Security Center Web Console

Сервер Kaspersky Security Center Web Console

Минимальные аппаратные требования:

- Процессор: 4 ядра, частота от 2500 МГц.
- Оперативная память: 8 ГБ.
- Объем свободного места на диске: 40 ГБ.

Программные требования:

- Окружение Node.js 14.16.0

Одна из следующих операционных систем:

- Microsoft Windows (только 64-разрядные версии):
 - Microsoft Windows 10 20H2.
 - Microsoft Windows 10 20H1.
 - Microsoft Windows 10 Enterprise 2019 LTSC.
 - Microsoft Windows 10 Enterprise 2016 LTSCB.
 - Microsoft Windows 10 Enterprise 2015 LTSCB.
 - Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809).
 - Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809).
 - Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809).
 - Microsoft Windows 10 Education RS5 (October 2018 Update, 1809).
 - Microsoft Windows 10 Pro 19H1.
 - Microsoft Windows 10 Pro для рабочих станций 19H1.
 - Microsoft Windows 10 Enterprise 19H1.
 - Microsoft Windows 10 Education 19H1.
 - Microsoft Windows 10 Home 19H2.
 - Microsoft Windows 10 Pro 19H2.
 - Microsoft Windows 10 Pro для рабочих станций 19H2.
 - Microsoft Windows 10 Enterprise 19H2.
 - Microsoft Windows 10 Education 19H2.
 - Microsoft Windows 8.1 Pro.
 - Microsoft Windows 8.1 Enterprise.

- Windows Server® 2019 Standard.
- Windows Server 2019 Core.
- Windows Server 2019 Datacenter.
- Windows Server 2016 Server Standard RS3 (1709) (LTSB/CBB).
- Windows Server 2016 Server Datacenter RS3 (1709) (LTSB/CBB).
- Windows Server 2016 (вариант установки Server Core RS3 (1709) (LTSB/CBB).
- Windows Server 2016 Standard (LTSB).
- Windows Server 2016 (вариант установки Server Core) (LTSB).
- Windows Server 2016 Datacenter (LTSB).
- Windows Server 2012 R2 Standard.
- Windows Server 2012 R2 Server Core.
- Windows Server 2012 R2 Foundation.
- Windows Server 2012 R2 Essentials.
- Windows Server 2012 R2 Datacenter.
- Windows Server 2012 Standard.
- Windows Server 2012 Server Core.
- Windows Server 2012 Foundation.
- Windows Server 2012 Essentials.
- Windows Server 2012 Datacenter.
- Windows Storage Server 2016.
- Windows Storage Server 2012 R2.
- Windows Storage Server 2012.
- Linux (только 64-разрядные версии):
 - Debian GNU/Linux® 10.x (Buster).
 - Debian GNU/Linux 9.x (Stretch).
 - Ubuntu Server 20.04 LTS (Focal Fossa).
 - Ubuntu Server 18.04 LTS (Bionic Beaver).
 - CentOS 8.x.
 - CentOS 7.x;
 - Red Hat Enterprise Linux Server 8.x.
 - Red Hat Enterprise Linux Server 7.x.
 - SUSE Linux Enterprise Server 15 (все пакеты обновлений).
 - SUSE Linux Enterprise Server 12 (все пакеты обновлений).
 - Astra Linux Special, версия 1.6.
 - Astra Linux Special, версия 1.5.

- Astra Linux Common Edition, версия 2.12.
- ALT 9.1.
- ALT 8.3.
- ALT SE 8.

Клиентские устройства

Клиентскому устройству для работы с Kaspersky Security Center Web Console требуется только браузер.

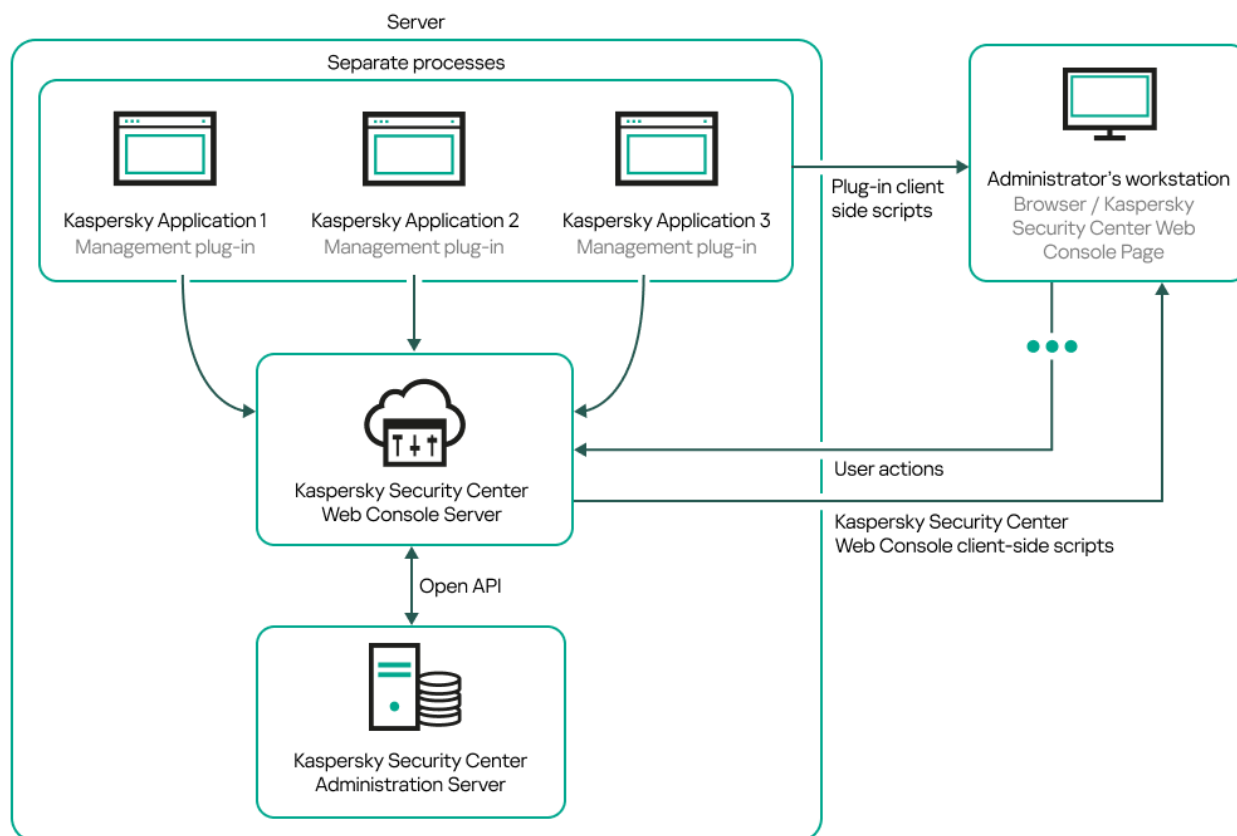
Требования к аппаратному и программному обеспечению устройства соответствуют требованиям браузера, который используется для работы с Kaspersky Security Center Web Console.

Браузер:

- Mozilla Firefox™ 78 Extended Support Release.
- Mozilla Firefox 78 и выше.
- Google Chrome™ 88 и выше.
- Safari 14 для macOS.

Схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console

На следующем рисунке приведена схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console.



Развертывание плагинов управления приложениями "Лаборатории Касперского", установленных на защищаемых устройствах (отдельный плагин для каждого приложения), происходит одновременно с развертыванием Сервера Kaspersky Security Center Web Console.

Как администратор, вы имеете доступ к Kaspersky Security Center Web Console через браузер на вашей рабочей станции.

Когда вы выполняете определенные действия в Kaspersky Security Center Web Console, Сервер Kaspersky Security Center Web Console взаимодействует с Сервером администрирования Kaspersky Security Center по OpenAPI. Сервер Kaspersky Security Center Web Console запрашивает необходимые данные у Сервера администрирования Kaspersky Security Center и отображает результаты ваших действий в Kaspersky Security Center Web Console.

Порты, используемые приложением Kaspersky Security Center Web Console

В таблице ниже перечислены порты, которые должны быть открыты на устройстве, на котором установлен Сервер Kaspersky Security Center Web Console (далее также просто Kaspersky Security Center Web Console).

Таблица 83. Порты, используемые приложением Kaspersky Security Center Web Console

Номер порта	Имя службы	Протокол	Назначение порта	Область
2001	Kaspersky Security Center Product Plugins Server	HTTP S	API-порт, который используется процессами плагина управления для приема запросов от службы Kaspersky Security Center Web Console Management Service	Запуск процессов node.exe плагинов управления.
1329, 2003	Kaspersky Security Center Web Console Management Service	HTTP S	API-порты, которые используются для получения запросов от службы Kaspersky Security Center Web Console Management Service, работающей на том же устройстве.	Обновление компонентов Kaspersky Security Center Web Console.
2005	Kaspersky Security Center Web Console	HTTP S	API-порт, который используется для получения запросов от службы "Kaspersky Security Center Web Console Management Service", работающей на том же устройстве.	Запуск установки Kaspersky Security Center Web Console.
3333	Kaspersky OSMP KAS Service	HTTP S	Порт конечной точки авторизации OAuth2.0.	Identity and Access Manager
4004	Kaspersky OSMP Facade Service	HTTP S	Порт провайдера идентификации OAuth2.0.	Identity and Access Manager
4444	Kaspersky OSMP KAS Service	HTTP S	Порт конечной точки самоанализа токена OAuth2.0	Identity and Access Manager

Номер порта	Имя службы	Протокол	Назначение порта	Область
8200	—	HTTP	API-порт, который используется для генерации сертификатов с помощью HashiCorp Vault (подробнее см. на сайте HashiCorp Vault https://www.vaultproject.io/).	Установка Kaspersky Security Center Web Console и обновление компонентов Kaspersky Security Center Web Console.
4150, 4151, 4152	Kaspersky Security Center Web Console Message Queue	HTTP S	API-порты Message Broker, которые используются для связи между Kaspersky Security Center Web Console и плагинами управления.	Взаимодействие между Kaspersky Security Center Web Console и плагинами управления

В таблице ниже перечислены порты, которые необязательно открывать на устройстве, на котором установлен Сервер Kaspersky Security Center Web Console. Однако Kaspersky Security Center Web Console использует эти порты для Identity and Access Manager (см. раздел "Identity and Access Manager в Kaspersky Security Center Web Console" на стр. [1008](#)).

Таблица 84. Порты, используемые Kaspersky Security Center Web Console для Identity and

Номер порта	Имя службы	Протокол	Назначение порта	Область
4445	Kaspersky OSMP KAS Service	HTTPS	Основной порт Identity and Access Manager, который получает конфигурацию от Kaspersky Security Center Web Console для порта конечной точки авторизации OAuth2.0 (подробнее о OAuth 2.0 см. веб-сайт OAuth https://www.oauth.com)	Identity and Access Manager
2444	Kaspersky OSMP Facade Service	HTTPS	Порт для настройки Identity and Access Manager	Identity and Access Manager
2445	Kaspersky OSMP Facade Service	HTTPS	Порт для подключения службы Kaspersky OSMP KAS Service к службе Kaspersky OSMP Facade Service	Identity and Access Manager

См. также:

Включение Identity and Access Manager: сценарий.....[1009](#)

Интерфейс Kaspersky Security Center Web Console

Управление Kaspersky Security Center осуществляется через интерфейс Kaspersky Security Center Web Console.

Окно приложения Kaspersky Security Center Web Console содержит следующие элементы:

- главное меню в левой части окна;
- рабочая область в правой части окна.

Главное меню

Главное меню содержит следующие разделы:

- **Сервер администрирования.** Отображает имя Сервера администрирования, к которому вы сейчас подключены. Нажмите на значок параметров () , чтобы открыть свойства Сервера администрирования (см. раздел "Настройка Сервера администрирования" см. стр. [1016](#)).
- **Мониторинг и отчеты.** Предоставляет сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

- **Активы (Устройства).** Содержит инструменты для активов, а также задачи (см. раздел "Задачи" см. стр. [1172](#)) и политики приложений "Лаборатории Касперского" (см. раздел "Политики и профили политик" см. стр. [431](#)).
- **Пользователи и роли.** Позволяет управлять пользователями и ролями, настраивать права пользователей, назначать пользователям роли и связывать профили политик с ролями (см. раздел "Пользователи и роли пользователей" на стр. [1273](#)).
- **Операции.** Содержит различные параметры, включая лицензирование приложений, просмотр и управление зашифрованными дисками и событиями шифрования (см. раздел "Шифрование и защита данных." на стр. [1268](#)), а также управление приложениями сторонних производителей (см. раздел "Управление запуском приложений на клиентских устройствах" см. стр. [1441](#)). Раздел также предоставляет вам доступ к хранилищам приложений (см. раздел "Загрузка и удаление файлов из Карантина и Резервного хранилища" см. стр. [1590](#)).
- **Обнаружение устройств и развертывание.** Позволяет опрашивать сеть (см. раздел "Обнаружение устройств в сети" см. стр. [1109](#)) для обнаружения клиентских устройств и распределять устройства по группам администрирования вручную или автоматически. Этот раздел содержит мастер первоначальной настройки и мастер развертывания защиты.
- **Marketplace.** Содержит информацию о бизнес-решениях "Лаборатории Касперского", позволяет выбрать нужные вам и перейти к приобретению этих решений на сайте "Лаборатории Касперского".
- **Параметры.** Позволяет создавать резервную копию данных текущего состояния веб-плагинов in (см. раздел "Загрузка плагинов для приложений "Лаборатории Касперского" на стр. [1086](#)), чтобы впоследствии можно было восстановить сохраненное состояние state (см. раздел "Резервное копирование и восстановление веб-плагинов" см. стр. [1366](#)). Содержит личные параметры, связанные с внешним видом интерфейса, такие как язык интерфейса или тема (см. раздел "Изменение языка интерфейса Kaspersky Security Center Web Console" см. стр. [1590](#)).
- **Меню вашей учетной записи.** Содержит ссылку на справку Kaspersky Security Center. Также вы можете выйти из Kaspersky Security Center и просмотреть версию Kaspersky Security Center Web Console и список установленных веб-плагинов управления.

Рабочая область

В рабочей области отображается выбранная вами информация для просмотра в разделах окна интерфейса Kaspersky Security Center Web Console. Она также содержит элементы управления, которые можно использовать для настройки отображения информации.

Закрепление и отмена закрепления разделов главного меню

Вы можете закрепить разделы Kaspersky Security Center Web Console, чтобы добавить их в избранное и быстро получить к ним доступ из раздела **Закрепленное** в главном меню.

Если закрепленных элементов нет, раздел **Закрепленное** не отображается в главном меню.

Вы можете закрепить разделы, в которых отображаются только страницы. Например, если вы перейдете в раздел **Активы (Устройства)** → **Управляемые устройства**, откроется страница с таблицей устройств, что

означает, что вы можете закрепить раздел **Управляемые устройства**. Если после выбора раздела в главном меню отображается окно или элемент не отображается, то закрепить такой раздел невозможно.

► *Чтобы закрепить раздел:*

1. В главном меню наведите курсор мыши на раздел, который вы хотите закрепить.

Отображается значок булавки (*).

2. Нажмите на значок булавки (*).

Раздел закреплен и отображается в разделе **Закрепленное**.

Максимальное количество элементов, которые вы можете закрепить, равно пяти.

Вы также можете удалить элементы из избранных, отменив их закрепление.

► *Чтобы отменить закрепление раздела:*

1. В главном окне приложения перейдите в раздел **Закрепленное**.

2. Наведите курсор мыши на раздел, для которого вы хотите отменить закрепление и нажмите на значок отмены закрепления (*).

Раздел удален из избранных.

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console

В этом разделе описана установка Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console, первоначальная настройка Сервера администрирования с помощью мастера первоначальной настройки, а также установка приложений "Лаборатории Касперского" на управляемые устройства с помощью мастера развертывания защиты.

Установка и первоначальная настройка Kaspersky Security Center Web Console состоит из следующих этапов:

а. Установка системы управления базами данных (СУБД)

Установите СУБД, используемую Kaspersky Security Center, или используйте существующую СУБД.

Сведения о том, как установить выбранную СУБД, см. в документации к ней.

б. Установка Сервера администрирования, Консоли администрирования и Агента администрирования

Вместе с Сервером администрирования устанавливаются также Консоль администрирования и серверная версия Агента администрирования.

Во время установки Сервера администрирования Kaspersky Security Center можно указать, требуется ли устанавливать на это же устройство Kaspersky Security Center Web Console. Если вы решили установить оба компонента на одно устройство, то вам не потребуется устанавливать отдельно приложение Kaspersky Security Center Web Console, так как оно будет установлено автоматически. Если вы хотите установить Kaspersky Security Center Web Console на другое устройство, то после установки Сервера администрирования Kaspersky Security Center перейдите к установке Kaspersky Security Center Web Console.

в. Установка Kaspersky Security Center Web Console

Если вы не выбрали на предыдущем шаге установку Kaspersky Security Center Web Console совместно с Сервером администрирования Kaspersky Security Center, установите Kaspersky Security Center Web Console (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)) на другом устройстве. Kaspersky Security Center Web Console можно установить отличном устройстве от устройства, на котором установлен Сервер администрирования.

г. Выполнение первоначальной настройки

После завершения установки Сервера администрирования при первом подключении к Серверу администрирования автоматически запускается Мастер первоначальной настройки (см. раздел "Мастер первоначальной настройки (Kaspersky Security Center Web Console)" см. стр. [1047](#)). Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики (см. раздел "О политиках и профилях политик" на стр. [1241](#)) и задачи (см. раздел "О задачах" см. стр. [1172](#)) с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач (см. раздел "Сценарий: настройка защиты сети" см. стр. [403](#)).

е. Лицензирование Kaspersky Security Center (если требуется)

Kaspersky Security Center с поддержкой базовой функциональности Консоли администрирования не требует лицензии. Вам необходима коммерческая лицензия, если вы хотите использовать одну или несколько дополнительных возможностей приложения, включая Системное администрирование, Управление мобильными устройствами и интеграции с SIEM-системами. Вы можете добавить файл ключ или код активации для этих возможностей на соответствующем шаге (см. раздел "Шаг 9.

Выбор способа активации приложения" см. стр. [1058](#)) мастера первоначальной настройки или вручную (см. раздел "Добавление лицензионного ключа в хранилище Сервера администрирования." см. стр. [1126](#)).

f. Обнаружение сетевых устройств

Этот этап обрабатывается мастером первоначальной настройки (см. раздел "Мастер первоначальной настройки (Kaspersky Security Center Web Console)" см. стр. [1047](#)). Обнаружение устройств можно также выполнить вручную. В результате Сервер администрирования Kaspersky Security Center получает адреса и имена всех устройств, зарегистрированных в сети. В дальнейшем вы можете с помощью Kaspersky Security Center устанавливать приложения "Лаборатории Касперского" и других производителей на обнаруженные устройства. Kaspersky Security Center запускает обнаружение устройств регулярно, поэтому, если в сети появятся новые устройства, они будут обнаружены автоматически.

g. Объединение устройств в группы администрирования

Этот этап обрабатывается мастером первоначальной настройки (см. раздел "Мастер первоначальной настройки (Kaspersky Security Center Web Console)" см. стр. [1047](#)), но вы также можете переместить обнаруженные устройства в группы администрирования вручную.

h. Установка Агента администрирования и приложений безопасности на устройства в сети

Развертывание защиты в сети организации подразумевает установку Агента администрирования и приложений безопасности (например, Kaspersky Endpoint Security для Windows (см. раздел "Сценарий: развертывание приложений "Лаборатории Касперского"" см. стр. [1084](#))) на устройства, найденные Сервером администрирования в процессе обнаружения устройств.

Чтобы выполнить удаленную установку приложения, запустите мастер развертывания защиты.

Приложения безопасности защищают устройства от вирусов и других приложений, представляющих угрозу. Агент администрирования обеспечивает связь устройства с Сервером администрирования. Параметры Агента администрирования автоматически настраиваются по умолчанию.

Перед тем как установить Агент администрирования и приложения безопасности на устройства в сети, убедитесь, что эти устройства доступны (включены).

i. Распространение лицензионных ключей на клиентские устройства

Распространите лицензионные ключи (см. раздел "Приложения "Лаборатории Касперского": лицензирование и активация" на стр. [388](#)) на клиентские устройства, чтобы активировать управляемые приложения безопасности на этих устройствах.

j. Установка Kaspersky Security для мобильных устройств (необязательно)

Если вы планируете управлять корпоративными мобильными устройствами, см. справку Kaspersky Security для мобильных устройств <https://support.kaspersky.com/KESMob/10SP4MR3/en-US/218256.htm> для получения информации о развертывании Kaspersky Endpoint Security для Android.

к. Настройка политик приложений "Лаборатории Касперского"

Чтобы на различных устройствах были применены разные параметры приложений, можно использовать управление безопасностью устройств или управление безопасностью, ориентированное на пользователей. Управление безопасностью устройств реализуется с помощью политик (см. раздел "О политиках и профилях политик" на стр. [1241](#)) и задач (см. раздел "О задачах" см. стр. [1172](#)). Задачи могут выполняться только на устройствах, которые соответствуют определенным условиям. Для создания условий отбора устройств используются выборки устройств (на стр. [1218](#)) и теги (см. раздел "Теги устройств" см. стр. [1231](#)).

l. Мониторинг состояния защиты сети

Вы можете организовывать мониторинг сети с помощью веб-виджетов на информационной панели (см. раздел "Использование панели мониторинга" на стр. [1469](#)), формировать отчеты (см. раздел "Использование отчетов" на стр. [1475](#)) о приложениях "Лаборатории Касперского", настраивать и просматривать выборки событий (см. раздел "Использование выборок событий" см. стр. [1484](#)), полученные от приложений на управляемых устройствах, и просматривать список уведомлений.

Установка

В этом разделе описана установка Kaspersky Security Center и Kaspersky Security Center Web Console.

Установка Kaspersky Security Center (Стандартная установка)

В этом разделе описана установка Kaspersky Security Center. Сначала необходимо установить систему управления базами данных.

► Чтобы установить Kaspersky Security Center:

1. Запустите исполняемый файл ksc_<номер сборки>_full_<язык локализации>.exe под учетной записью с правами администратора.
2. В открывшемся окне выбора приложений выберите пункт **Установить Kaspersky Security Center**.
Откроется окно мастера установки Сервера администрирования Kaspersky Security Center.
3. Начав с окна приветствия, пройдите шаги мастера, нажимая на кнопку **Далее**.
4. Установите Microsoft .NET Framework, если он не установлен.
5. Примите условия Лицензионного соглашения и Политики конфиденциальности.
6. Выберите тип установки. Для ознакомительных целей рекомендуется оставить указанный по умолчанию тип – **Стандартная**.
7. Если требуется установить Kaspersky Security Center Web Console на то же устройство, что и Kaspersky Security Center, установите флажок **Установить Kaspersky Security Center Web Console**.
Если этот флажок не установлен, вы можете установить Kaspersky Security Center Web Console (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)) отдельно на это же или другое устройство.
8. Укажите размер сети. Для ознакомительных целей рекомендуется оставить указанное по умолчанию значение – **Менее 100 устройств в сети**.
9. Выберите тип установленного ранее сервера базы данных.
10. Укажите параметры подключения к установленному ранее серверу баз данных.
11. Укажите параметры аутентификации для установленного ранее сервера баз данных.
12. Нажмите на кнопку **Установить**, чтобы запустить установку.
13. После успешного завершения установки укажите, требуется ли запустить Консоль администрирования сразу после завершения работы мастера.

Если вы выбрали открыть Kaspersky Security Center Web Console, откроется экран входа (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)). Затем вы можете выполнить первоначальную настройку Сервера администрирования с помощью мастера первоначальной

настройки (см. раздел "Мастер первоначальной настройки (Kaspersky Security Center Web Console)" см. стр. [1047](#)).

Вы можете запустить приложение Kaspersky Security Center Web Console, только если вы уже установили его. Вы не можете запустить приложение Kaspersky Security Center Web Console, если вы не установили его во время установки Kaspersky Security Center или отдельно.

14. В открывшемся окне Консоли администрирования выберите установленный Сервер администрирования.
15. Чтобы продолжить, в открывшемся окне с сертификатом Сервера администрирования нажмите на кнопку **Да**.

Запустится мастер первоначальной настройки Сервера администрирования, если он не был запущен в веб-версии Консоли администрирования.

Устранение неисправностей

Если окно с сертификатом Сервера администрирования не отображается и появляются сообщения об ошибках подключения:

1. В Windows откройте окно **Службы (Панель управления → Администрирования → Службы)**. Убедитесь, что запущены службы Агент администрирования Kaspersky Security Center и Сервер администрирования Kaspersky Security Center.
2. В Windows откройте окно **Просмотр событий (Панель управления → Администрирование → Просмотр событий)** и выберите **Журнал приложений и служб → Kaspersky Event Log**. Убедитесь, что в журнале событий отсутствуют записи об ошибках и присутствуют записи о событиях вида **Запущен Сервер администрирования <номер версии>**.

См. также:

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985
Сценарий: настройка защиты сети.....	403
Настройка и распространение политик: подход, ориентированный на устройства	405

Установка Kaspersky Security Center Web Console

В этом разделе описано как установить Сервер Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console) отдельно. Сначала необходимо установить СУБД и Сервер администрирования Kaspersky Security Center. Вы можете установить Kaspersky Security Center Web Console на том же устройстве, что и Kaspersky Security Center, или на другое.

► Чтобы установить Kaspersky Security Center Web Console:

1. Запустите файл установки ksc-web-console-<номер_версии>.<номер сборки>.exe под учетной записью с правами администратора.
Запускается мастер установки.
2. Выберите язык мастера установки.
3. В окне приветствия нажмите на кнопку **Далее**.

4. В окне **Лицензионное соглашение** прочитайте и примите условия Лицензионного соглашения. Установка продолжится после принятия Лицензионного соглашения, в противном случае кнопка **Далее** недоступна.
5. В окне **Папка назначения** выберите папку, в которую будет установлено приложение Kaspersky Security Center Web Console (по умолчанию %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Если такой папки нет, она будет создана автоматически в процессе установки.

Вы можете изменить папку назначения с помощью кнопки **Обзор**.

6. В окне **Параметры подключения Kaspersky Security Center Web Console** укажите следующую информацию:
 - адрес Kaspersky Security Center Web Console (по умолчанию 127.0.0.1);
 - порт, который Kaspersky Security Center Web Console будет использовать для входящих подключений, то есть порт, который дает доступ к Kaspersky Security Center Web Console из браузера (по умолчанию 8080).

Рекомендуется оставить значения адреса и порта по умолчанию.

Нажмите на кнопку **Проверить**, если хотите проверить, доступен ли выбранный порт.

Если вы хотите включить запись в журнал Kaspersky Security Center Web Console (см. раздел "Журнал активности Kaspersky Security Center Web Console" на стр. [1563](#)), выберите соответствующий параметр. Если этот параметр не выбран, файлы журнала Kaspersky Security Center Web Console не будут созданы.

7. В окне **Параметры учетной записи** укажите учетные записи и пароли.
Рекомендуется использовать значения учетных записей по умолчанию.
8. В окне **Клиентский сертификат** выберите один из следующих параметров:
 - **Сформировать новый**. Этот вариант рекомендуется использовать, если у вас нет сертификата браузера.
 - **Выбрать существующий сертификат**. Вы можете выбрать этот вариант, если у вас уже есть сертификат браузера. В этом случае укажите путь к сертификату.
 - Если вы выбрали создать сертификат, при открытии Kaspersky Security Center Web Console, браузер может информировать вас о том, что подключение к Kaspersky Security Center Web Console не является приватным и что сертификат Kaspersky Security Center Web Console недействителен. Это предупреждение появляется потому, что сертификат Kaspersky Security Center Web Console является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить это предупреждение, создайте сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам. Далее выберите параметр **Выбрать существующий сертификат** в окне **Клиентский сертификат** и укажите путь к вашему пользовательскому сертификату.

Сертификаты в формате PFX не поддерживаются приложением Kaspersky Security Center Web Console. Чтобы использовать такой сертификат, необходимо сначала преобразовать его в поддерживаемый формат PEM (см. раздел "Преобразование сертификата из формата PFX в формат PEM" см. стр. [997](#)) с помощью кроссплатформенной утилиты на основе OpenSSL, например, OpenSSL для Windows.

9. В окне **Доверенные Серверы администрирования** убедитесь, что ваш Сервер администрирования есть в списке, и нажмите на кнопку **Далее**, чтобы перейти к последнему окну мастера установки.

Если нужно добавить в список новый Сервер администрирования, нажмите на кнопку **Добавить**. В открывшемся окне укажите свойства нового доверенного Сервера администрирования:

- **Имя Сервера администрирования**

Имя Сервера администрирования, которое будет отображаться в окне входа в Kaspersky Security Center Web Console.

- **Адрес Сервера администрирования**

IP-адрес устройства, на которое вы устанавливаете Сервер администрирования.

- **Порт Сервера администрирования**

Порт OpenAPI, который Kaspersky Security Center Web Console, использует для подключения к Серверу администрирования (по умолчанию 13299).

- **Сертификат Сервера администрирования**

Файл сертификата хранится на устройстве, на котором установлен Сервер администрирования. Путь к сертификату Сервера администрирования по умолчанию:

- Для устройств с операционной системой Windows: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.
- Для устройств с операционной системой Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/.

Если вы устанавливаете Kaspersky Security Center Web Console на то же устройство, где установлен Сервер администрирования, используйте один из указанных выше путей. Или скопируйте файл сертификата с устройства, на котором установлен Сервер администрирования, на устройство, на котором вы устанавливаете Kaspersky Security Center Web Console, и укажите локальный путь к сертификату.

10. В окне **Identity and Access Manager (IAM)** укажите, хотите ли вы установить Identity and Access Manager (см. раздел "Identity and Access Manager в Kaspersky Security Center Web Console" на стр. [1008](#)) (далее также IAM). Если вы выбрали установку Identity and Access Manager, укажите следующие номера портов:

- **KAS-порт администратора.** По умолчанию порт 4445 используется для получения конфигурации от Kaspersky Security Center Web Console для порта конечной точки авторизации OAuth2.0.
- **Фасадный порт администратора.** По умолчанию порт 2444 используется для настройки Identity and Access Manager.
- **Фасадный порт взаимодействия.** По умолчанию порт 2445 используется для подключения Kaspersky OSMP KAS Service к Kaspersky OSMP Facade Service.

Вы можете изменить номера портов по умолчанию. В дальнейшем вы не сможете изменить их с помощью Kaspersky Security Center Web Console.

11. В последнем окне мастера установки нажмите на кнопку **Установить**, чтобы начать установку.

После успешного завершения установки на рабочем столе появляется ярлык и вы можете войти (см. раздел "Вход в приложение Kaspersky Security Center Web Console и выход из него" на стр. [1006](#)) в Kaspersky Security Center Web Console.

Запускается мастер первоначальной настройки Сервера администрирования (см. раздел "Мастер первоначальной настройки (Kaspersky Security Center Web Console)" см. стр. [1047](#)), если он не был запущен в Консоли администрирования, интегрированной в Microsoft Management Console.

Устранение неисправностей

► Если Kaspersky Security Center Web Console не отображается в вашем браузере по указанному вами адресу, попробуйте сделать следующее:

1. Проверьте правильность указанного имени или IP-адреса устройства, на котором установлено приложение Kaspersky Security Center Web Console.
2. Убедитесь, что устройство, на котором вы работаете, имеет доступ к устройству, на котором установлено приложение Kaspersky Security Center Web Console.
3. Убедитесь, что параметры сетевого экрана устройства, на котором установлено приложение Kaspersky Security Center Web Console, разрешают входящие подключения через порт 8080 и для приложения node.exe.
4. В Windows откройте окно **Службы**. Убедитесь, что запущена Kaspersky Security Center Web Console.
5. Убедитесь, что у вас есть доступ к Kaspersky Security Center с помощью Консоли администрирования.
6. В Windows откройте окно **Просмотр событий** и выберите **Журнал приложений и служб** → **Kaspersky Event Log**. Убедитесь, что в журнале событий отсутствуют записи об ошибках.

См. также:

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985
Обновление Kaspersky Security Center Web Console	992
Сценарий: настройка защиты сети.....	403
Настройка и распространение политик: подход, ориентированный на устройства	405
Identity and Access Manager в Kaspersky Security Center Web Console.....	1008

Установка Kaspersky Security Center Web Console, подключенной к Серверу администрирования, установленного на узлах отказоустойчивого кластера "Лаборатории Касперского"

В этом разделе описывается установка Сервера Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console), который подключается к Серверу администрирования, установленному на узлах отказоустойчивого кластера Kaspersky Security Center или узлах отказоустойчивого кластера Windows Server. Перед установкой Kaspersky Security Center Web Console установите СУБД и Сервер администрирования Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center или на узлы отказоустойчивого кластера Windows Server.

Если вы используете отказоустойчивый кластер Windows Server, не рекомендуется устанавливать Kaspersky Security Center Web Console на узел отказоустойчивого кластера. В случае сбоя узла вы потеряете доступ к Серверу администрирования.

► Чтобы установить Kaspersky Security Center Web Console, которая подключается к Серверу администрирования, установленному на узлах отказоустойчивого кластера:

1. Выполните шаги из раздела Установка Kaspersky Security Center Web Console (см. стр. [988](#)), начиная с шага 1 по шаг 8.
2. На шаге 9 в окне **Доверенные Серверы администрирования** нажмите на кнопку **Добавить**, чтобы добавить отказоустойчивый кластер в качестве доверенного Сервера администрирования.

В открывшемся окне укажите следующие параметры:

- **Имя Сервера администрирования**

Имя кластера, которое будет отображаться в окне входа в Kaspersky Security Center Web Console.

- **Адрес Сервера администрирования**

В зависимости от типа отказоустойчивого кластера укажите адрес кластера:

- **Отказоустойчивый кластер Kaspersky Security Center.** Укажите IP-адрес дополнительного сетевого адаптера в качестве адреса кластера, если вы создали адаптер при подготовке узлов кластера. В противном случае укажите IP-адрес стороннего балансировщика нагрузки, который вы используете.
- **Отказоустойчивый кластер Windows Server.** Укажите адрес кластера, который вы получили при создании отказоустойчивого кластера Windows Server.

- **Порт Сервера администрирования**

Порт OpenAPI, который Kaspersky Security Center Web Console, использует для подключения к Серверу администрирования (по умолчанию 13299).

- **Сертификат Сервера администрирования**

Сертификат Сервера администрирования находится в общем хранилище данных отказоустойчивого кластера Kaspersky Security Center или отказоустойчивого кластера Windows Server. Путь по умолчанию к файлу сертификата: <shared data folder>\1093\cert\klserver.cer. Скопируйте файл сертификата из общего хранилища данных на устройство, на котором вы устанавливаете Kaspersky Security Center Web Console. Укажите локальный путь к сертификату Сервера администрирования.

3. Продолжите стандартную установку (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)) Kaspersky Security Center Web Console.

После завершения установки на рабочем столе появляется ярлык и вы можете войти (см. раздел "Вход в приложение Kaspersky Security Center Web Console и выход из него" на стр. [1006](#)) в Kaspersky Security Center Web Console.

Если вы используете отказоустойчивый кластер Kaspersky Security Center, вы можете перейти в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**, чтобы просмотреть информацию об узлах кластера и о файловом сервере.

Обновление Kaspersky Security Center Web Console

Если вы хотите использовать новую версию Kaspersky Security Center Web Console, не удаляя установленный в данный момент экземпляр приложения, вы можете использовать стандартную процедуру обновления, предусмотренную в установщике Kaspersky Security Center Web Console.

► Чтобы обновить Kaspersky Security Center Web Console:

1. Под учетной записью с правами администратора запустите ksc-web-console-[<номер версии>.<номер сборки>.exe](#) исполняемый файл, где [<номер сборки>](#) означает номер сборки Kaspersky Security Center Web Console, номер которой больше, чем у установленного вами экземпляра.
2. В открывшемся окне мастера установки выберите язык и нажмите на кнопку **ОК**.
3. В окне приветствия выберите параметр **Обновить** и нажмите на кнопку **Далее**.
4. В окне **Лицензионное соглашение** прочитайте и примите условия Лицензионного соглашения. Установка продолжится после принятия Лицензионного соглашения, в противном случае кнопка **Далее** недоступна.
5. Выполните все шаги мастера установки, пока не завершите установку. В процессе установки вы также можете изменить параметры Kaspersky Security Center Web Console, которые вы указали при предыдущей установке (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)). Нажмите на кнопку **Обновить** на шаге **Все готово для изменения Kaspersky Security Center Web Console**. Дождитесь, пока новые параметры вступят в силу, и на следующем шаге мастера установки нажмите на кнопку **Готово**. Вы также можете перейти по ссылке **Запустить Kaspersky Security Center Web Console в вашем браузере** для немедленного запуска обновленного экземпляра Kaspersky Security Center Web Console.

Изменение параметров Kaspersky Security Center Web Console при обновлении доступно только в версии приложения Kaspersky Security Center 12.2 Web Console и выше.

Приложение Kaspersky Security Center Web Console установлено.

См. также

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console.....	985
Сценарий: обновление Kaspersky Security Center и управляемых приложений безопасности.....	1333

Сертификаты для работы с Kaspersky Security Center Web Console

В разделе описано, как выпустить и заменить сертификаты для Kaspersky Security Center Web Console, а также как обновить сертификат Сервера администрирования, если Сервер взаимодействует с Kaspersky Security Center Web Console.

В этом разделе

Перевыпуск сертификата для Kaspersky Security Center Web Console	994
Замена сертификата для Kaspersky Security Center Web Console.....	995
Указание сертификатов для доверенных Серверов администрирования в Kaspersky Security Center Web Console	996
Преобразование сертификата из формата PFX в формат PEM	997

Перевыпуск сертификата для Kaspersky Security Center Web Console

Большинство браузеров ограничивает срок действия сертификата. Чтобы попасть в это ограничение, срок действия сертификата в Kaspersky Security Center Web Console равен 397 дням. Вы можете заменить существующий сертификат, полученный от аккредитованного центра сертификации (CA), при выпуске вручную нового самоподписанного сертификата. Вы также можете повторно выпустить устаревший сертификат Kaspersky Security Center Web Console.

Автоматический перевыпуск сертификата для Kaspersky Security Center Web Console не поддерживается. Вам необходимо вручную перевыпустить сертификат.

Если вы уже используете самоподписанный сертификат, вы также можете перевыпустить его, обновив Kaspersky Security Center Web Console, используя стандартную процедуру в установщике (параметр **Обновить**).

Когда вы открываете Web Console, браузер может информировать вас о том, что подключение к Web Console не является приватным и что сертификат Web Console недействителен. Это предупреждение появляется потому, что сертификат Kaspersky Security Center Web Console является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить или предотвратить это предупреждение, можно выполнить одно из следующих действий:

- Укажите пользовательский сертификат при его повторном выпуске (рекомендуемый вариант). Создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам.
 - Добавьте сертификат Web Console в список доверенных сертификатов браузера после перевыпуска сертификата. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.
- *Чтобы выпустить новый сертификат при первой установке Kaspersky Security Center Web Console:*
1. Запустите установку Kaspersky Security Center Web Console (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)).
 2. Выберите параметр **Сформировать новый** на шаге мастера установки **Клиентский сертификат** и нажмите на кнопку **Далее**.
 3. Выполните все шаги мастера установки, пока не завершите установку.
Новый сертификат для Kaspersky Security Center Web Console выписан со сроком действия 397 дней.
- *Чтобы перевыпустить просроченный сертификат Kaspersky Security Center Web Console:*
1. Запустите исполняемый файл ksc-web-console-**<номер_версии>**.**<номер сборки>**.exe под учетной записью с правами администратора.
 2. В открывшемся окне мастера установки выберите язык и нажмите на кнопку **ОК**.
 3. В окне приветствия выберите параметр **Перевыпустить сертификат** и нажмите на кнопку **Далее**.
 4. На следующем шаге дождитесь завершения перенастройки Kaspersky Security Center Web Console и нажмите на кнопку **Готово**.
Сертификат Kaspersky Security Center Web Console перевыпущен со сроком действия 397 дней.

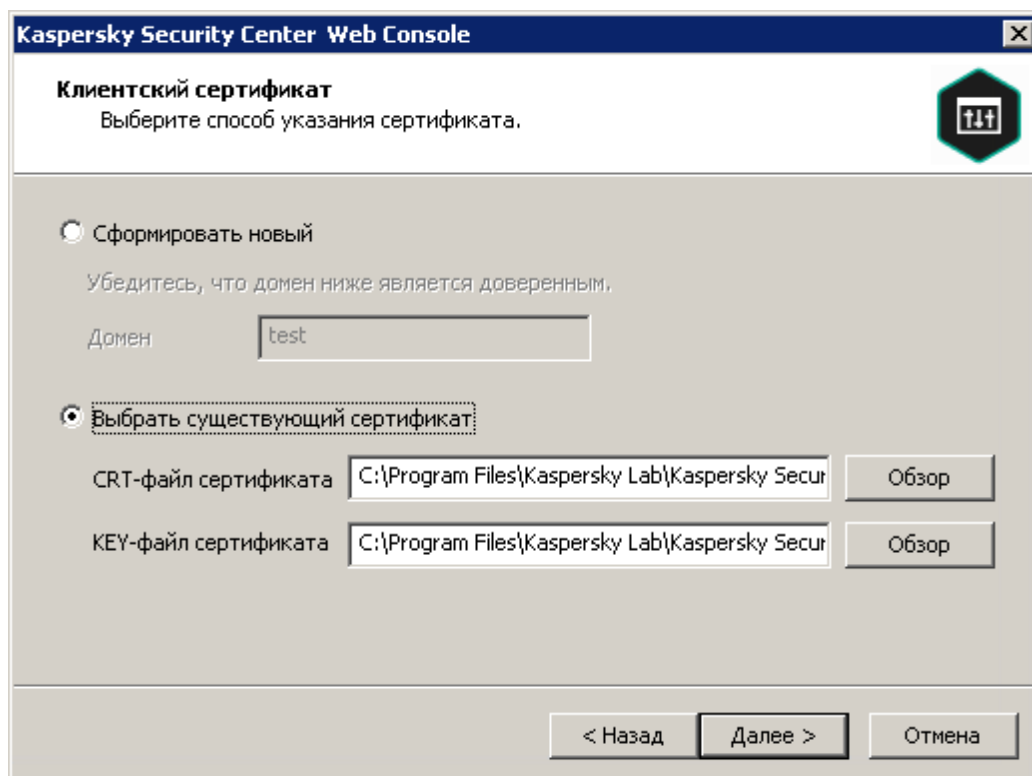
Если вы используете Identity and Access Manager (см. раздел "Identity and Access Manager в Kaspersky Security Center Web Console" на стр. [1008](#)), вы также должны повторно выпустить все TLS-сертификаты для портов, которые используют Identity and Access Manager (см. раздел "Порты, используемые приложением Kaspersky Security Center Web Console" на стр. [980](#)). В Kaspersky Security Center Web Console отображается уведомление об истечении срока действия сертификата. Следуйте инструкциям из уведомления.

Замена сертификата для Kaspersky Security Center Web Console

По умолчанию при установке Сервера Kaspersky Security Center Web Console сертификат браузера для приложения генерируется автоматически. Вы можете заменить автоматически сгенерированный сертификат на пользовательский.

► Чтобы заменить сертификат для Сервера Kaspersky Security Center Web Console на пользовательский сертификат:

1. Запустите на устройстве, на котором установлен Сервер Kaspersky Security Center Web Console, исполняемый файл ksc-web-console-*<номер версии>*.*<номер сборки>*.exe под учетной записью с правами администратора.
Запускается мастер установки.
2. На первой странице мастера выберите параметр **Обновить**.
3. На странице **Клиентский сертификат** выберите параметр **Выбрать существующий сертификат** и укажите путь к пользовательскому сертификату.



4. На последней странице мастера нажмите на кнопку **Изменить**, чтобы применить новые параметры.
5. После успешного завершения настройки приложения нажмите на кнопку **Готово**.

Kaspersky Security Center Web Console работает с указанным сертификатом.

Указание сертификатов для доверенных Серверов администрирования в Kaspersky Security Center Web Console

Существующий сертификат Сервера администрирования автоматически заменяется новым до истечения срока действия сертификата. Вы также можете заменить существующий сертификат Сервера администрирования пользовательским сертификатом. При каждом изменении сертификата новый сертификат должен быть указан в параметрах приложения Kaspersky Security Center Web Console. Иначе Kaspersky Security Center Web Console не сможет подключиться к Серверу администрирования.

► Чтобы задать новый сертификат для Сервера администрирования:

1. На устройстве, на котором установлен Сервер администрирования, скопируйте файл сертификата, например, на запоминающее устройство.

По умолчанию файл сертификата хранится в следующей папке:

- Для устройств с операционной системой Windows: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.
- Для устройств с операционной системой Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/.

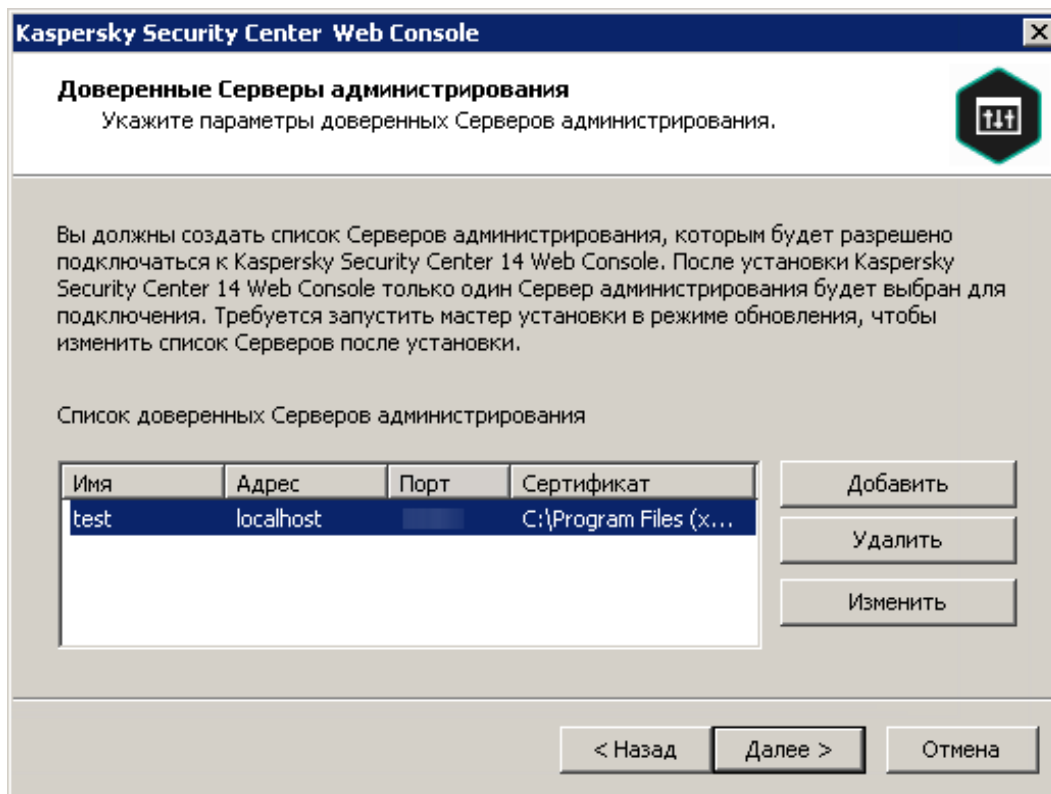
2. На устройстве, на котором установлено приложение Kaspersky Security Center Web Console, поместите файл сертификата в локальную папку.
3. Запустите установочный файл ksc-web-console-**<номер версии>.<номер сборки>.exe** под учетной записью с правами администратора.

Запускается мастер установки.

4. На странице мастера выберите параметр **Обновить**.

Следуйте далее указаниям мастера.

- На странице **Доверенные Серверы администрирования** выберите требуемый Сервер администрирования и нажмите на кнопку **Изменить**.



- В открывшемся окне **Изменить Сервер администрирования** нажмите на кнопку **Обзор**, укажите путь к новому файлу сертификата и нажмите на кнопку **Обновить**, чтобы применить изменения.
- На странице **Все готово для изменения Kaspersky Security Center Web Console** мастера нажмите на кнопку **Обновить**, чтобы начать обновление.
- После успешного завершения настройки приложения нажмите на кнопку **Готово**.
- Войдите (см. раздел "Вход в приложение Kaspersky Security Center Web Console и выход из него" на стр. [1006](#)) в Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console работает с указанным сертификатом.

Преобразование сертификата из формата PFX в формат PEM

Чтобы использовать сертификат формата PFX в Kaspersky Security Center Web Console, вам необходимо предварительно преобразовать его в формат PEM с помощью любой кроссплатформенной утилиты на основе OpenSSL.

- Чтобы преобразовать сертификат из формата PFX в формат PEM в операционной системе Windows:

- В кроссплатформенной утилите на основе OpenSSL выполните следующие команды:

```
openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out server.crt
openssl pkcs12 -in <filename.pfx> -nocerts -nodes -out key.pem
```

В результате вы получаете открытый ключ в виде файла .crt и закрытый ключ в виде защищенного парольной фразой файла .pem.

11. Убедитесь, что файлы .crt и .pem сгенерированы в той же папке, где хранится .pfx файл.
12. Если файл .crt или .pem содержит "пакет атрибутов", удалите эти атрибуты с помощью любого удобного текстового редактора и сохраните файл.
13. Перезапустите службу Windows.
14. Kaspersky Security Center Web Console не поддерживает сертификаты, защищенные парольной фразой. Поэтому выполните следующую команду в кроссплатформенной утилите на основе OpenSSL, чтобы удалить парольную фразу из файла .pem:

```
openssl rsa -in key.pem -out key-without-passphrase.pem
```

Не используйте одно и то же имя для входных и выходных файлов .pem.

В результате новый файл .pem не зашифрован. Вводить парольную фразу для его использования не нужно.

Файлы .crt и .pem готовы к использованию, поэтому вы можете указать их в мастере установки Kaspersky Security Center Web Console (см. раздел "Замена сертификата для Kaspersky Security Center Web Console" см. стр. [995](#)).

► *Чтобы преобразовать сертификат из формата PFX в формат PEM в операционной системе Linux:*

1. В кроссплатформенной утилите на основе OpenSSL выполните следующие команды:

```
openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN  
CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
```

```
openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN  
PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
```

2. Убедитесь, что файл сертификата и закрытый ключ сгенерированы в той же папке, где хранится файл PFX.
3. Kaspersky Security Center Web Console не поддерживает сертификаты, защищенные парольной фразой. Поэтому выполните следующую команду в кроссплатформенной утилите на основе OpenSSL, чтобы удалить парольную фразу из файла .pem:

```
openssl rsa -in key.pem -out key-without-passphrase.pem
```

Не используйте одно и то же имя для входных и выходных файлов .pem.

В результате новый файл .pem не зашифрован. Вводить парольную фразу для его использования не нужно.

Файлы .crt и .pem готовы к использованию, поэтому вы можете указать их в мастере установки Kaspersky Security Center Web Console (см. раздел "Замена сертификата для Kaspersky Security Center Web Console" см. стр. [995](#)).

Перенос данных из Kaspersky Security Center Windows

В этом разделе описан перенос данных управляемых устройств и связанных с ними объектов (политик, задач, групп, тегов и других объектов) из Kaspersky Security Center Windows.

- Kaspersky Security Center Cloud Console (см. раздел "О переносе данных в Kaspersky Security Center Cloud Console" см. стр. [999](#))
- Kaspersky Security Center Linux (см. раздел "О переносе данных в приложение Kaspersky Security Center Linux" см. стр. [1000](#))

В этом разделе

О переносе данных в Kaspersky Security Center Cloud Console	999
О переносе данных в приложение Kaspersky Security Center Linux.....	1000
Экспорт групповых объектов из Kaspersky Security Center Windows	1002
Импорт экспортного файла в Kaspersky Security Center Linux	1004
Переключение управляемых устройств под управление Kaspersky Security Center Linux	1005

О переносе данных в Kaspersky Security Center Cloud Console

Вы можете выполнить перенос данных из приложения Kaspersky Security Center Web Console в Kaspersky Security Center Cloud Console. После этого вы получаете доступ к Серверу администрирования и системе управления базами данных (СУБД), которые размещены в инфраструктуре "Лаборатории Касперского". Вам не нужен физический сервер или СУБД: и то, и другое обслуживается за вас специалистами "Лаборатории Касперского".

Вы можете перенести данные управляемых устройств с операционными системами Windows, Linux или macOS под управление Kaspersky Security Center Cloud Console. Если в вашей сети есть иерархия Серверов администрирования, вы можете сохранить ее в Kaspersky Security Center Cloud Console. Кроме того, вы можете перенести:

- Задачи и политики управляемых приложений.
- Глобальные задачи (см. раздел "О задачах" см. стр. [1172](#)).
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги, назначенные устройствам, данные которых вы переносите.

После завершения переноса данных вы сможете управлять устройствами с помощью Kaspersky Security Center Cloud Console. При этом переносимые объекты сохраняются, а Агент администрирования переустанавливается на все управляемые устройства.

Информацию о том, как выполнить перенос данных, и список предварительных требований см. в справке *Kaspersky Security Center Cloud Console*
https://click.kaspersky.com/?hl=en&link=online_help&pid=KSC&version=1.0.0&helpid=186799.

О переносе данных в приложение Kaspersky Security Center Linux

Следуя этому сценарию, вы можете переместить структуру групп администрирования, включая управляемые устройства и другие объекты группы (политики, задачи, глобальные задачи, теги и выборки устройств) из Kaspersky Security Center Windows под управление Kaspersky Security Center Linux.

Ограничения:

- Перенос данных возможен только из Kaspersky Security Center Windows версии 14.2 и выше в Kaspersky Security Center Linux версии 15 и выше.
- Вы можете выполнить этот сценарий только с помощью Kaspersky Security Center Web Console.

Прежде чем начать, узнайте больше о функциях и ограничениях Kaspersky Security Center Linux:

- Функциональные различия Kaspersky Security Center Windows и Kaspersky Security Center Linux
- Список приложений "Лаборатории Касперского" поддерживаемых приложением Kaspersky Security Center Linux

Этапы

Сценарий переноса данных состоит из следующих этапов:

а. Выберите способ переноса данных

Вы переносите данные в Kaspersky Security Center Linux с помощью мастера переноса данных. Действия мастера переноса данных зависят от того, организованы ли Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux в иерархию:

- Перенос данных с использованием иерархии Серверов администрирования
Выберите этот параметр, если Сервер администрирования Kaspersky Security Center Windows является подчиненным по отношению к Серверу администрирования Kaspersky Security Center Linux. Вы управляете процессом переноса данных и переключаетесь между Серверами в рамках одного экземпляра Kaspersky Security Center Web Console. Если вы предпочитаете этот вариант, вы можете организовать Серверы администрирования в иерархию, чтобы упростить процедуру переноса данных. Для этого создайте иерархию перед началом переноса данных.
- Перенос данных с помощью файла экспорта (ZIP-архив)
Выберите этот параметр, если Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux не организованы в иерархию. Вы управляете процессом переноса данных с помощью двух экземпляров Kaspersky Security Center Web Console, одного экземпляра Kaspersky Security Center Windows и другого Kaspersky Security Center Linux. В этом случае вы будете использовать файл экспорта, который вы создали и загрузили во время экспорта из Kaspersky Security Center Windows (см. раздел "Экспорт групповых объектов из Kaspersky Security Center Windows" см. стр. [1002](#)), и импортировать этот файл в Kaspersky Security Center Linux (см. раздел "Импорт экспортного файла в Kaspersky Security Center Linux" см. стр. [1004](#)).

Если на шаге 5 вы не хотите переустанавливать Агент администрирования, так как это может занять много времени, вы можете создать резервную копию сертификата и закрытый ключ Сервера администрирования Kaspersky Security Center Windows, запустив утилиту `klbackup` с параметром `-cert_only`. Затем на шаге 5 вам необходимо восстановить сертификат и закрытый ключ.

б. Экспорт данных из Kaspersky Security Center Windows

Откройте Kaspersky Security Center Windows и запустите мастер переноса данных (см. раздел "Экспорт групповых объектов из Kaspersky Security Center Windows" см. стр. [1002](#)).

с. Импорт данных в приложение Kaspersky Security Center Linux

Продолжите работу мастера переноса данных, чтобы импортировать экспортированные данные в Kaspersky Security Center Linux (см. раздел "Импорт экспортного файла в Kaspersky Security Center Linux" см. стр. [1004](#)). Если Серверы организованы в иерархию, импорт начинается автоматически после успешного экспорта в том же мастере. Если Серверы не выстроены в иерархию, вы продолжите работу мастера переноса данных после перехода на Kaspersky Security Center Linux.

д. Выполнение дополнительных действий для переноса объектов и параметров из Kaspersky Security Center Windows в Kaspersky Security Center Linux вручную (необязательный шаг)

Вы также можете перенести объекты и параметры, которые невозможно передать с помощью мастера переноса данных. Например, вы можете дополнительно сделать следующее:

- Перенести лицензионные ключи, используемые Сервером администрирования и управляемыми приложениями.
- Настроить глобальные задачи Сервера администрирования.
- Настроить параметры политики Агента администрирования (на стр. [1145](#)).
- Создать инсталляционные пакеты приложений (см. раздел "Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"" см. стр. [1087](#)).
- Создать виртуальные Серверы администрирования (см. раздел "Создание виртуального Сервера администрирования" см. стр. [1025](#)).
- Назначить и настроить точки распространения (см. раздел "Назначение точек распространения вручную" см. стр. [1370](#)).
- Создать правила перемещения устройств (см. раздел "Создание правил перемещения устройств" см. стр. [1197](#)).
- Настроить правила автоматического назначения тегов устройствам (см. раздел "Создание правил автоматического назначения тегов устройствам" см. стр. [1236](#)).
- Создать категории приложений (см. раздел "Использование компонента Контроль приложений для управления исполняемыми файлами" см. стр. [572](#)).

е. Переместить импортированные управляемые устройства под управление Kaspersky Security Center Linux

Завершите перенос данных, переместите импортированные управляемые устройства под управление Kaspersky Security Center Linux. В текущей версии Kaspersky Security Center Linux это можно сделать одним из следующих способов:

- С помощью утилиты klmover.
Используйте утилиту klmover и укажите параметры подключения для нового Сервера администрирования.
- С помощью установки или переустановки Агента администрирования на управляемые устройства.
Создайте инсталляционный пакет Агента администрирования и укажите параметры подключения для нового Сервера администрирования в свойствах инсталляционного пакета. Используя инсталляционный пакет, установите Агент администрирования на импортированные управляемые устройства с помощью задачи удаленной установки. Подробнее см. в разделе Переключение управляемых устройств под управление Kaspersky Security Center Linux (см. стр. [1005](#)).

Вы также можете создать и использовать автономный инсталляционный пакет (см. раздел "Создание автономного инсталляционного пакета" на стр. [1090](#)) для локальной установки Агента администрирования.

- С помощью восстановления сертификата и закрытого ключа Сервера администрирования из резервной копии.

Назначьте устройству с Сервером администрирования Kaspersky Security Center Linux тот же IP-адрес, что и у устройства с Сервером администрирования Kaspersky Security Center Windows.

Запустите утилиту kbackup с параметром `-cert_only`, чтобы восстановить сертификат Сервера администрирования и закрытый ключ из резервной копии, сохраненной на шаге 2.

Выполните следующую команду в командной строке:

```
/opt/kaspersky/ksc64/sbin/kbackup -path /путь к резервной копии
сертификата Сервера администрирования/ -restore -cert_only.
```

f. Обновите Агент администрирования до последней версии.

Рекомендуется обновить Агент администрирования для Linux (см. раздел "Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского" см. стр. [460](#)) до той же версии, что и Kaspersky Security Center.

g. Убедитесь, что управляемые устройства отображаются на новом Сервере администрирования.

На Сервере администрирования Kaspersky Security Center Linux откройте список управляемых устройств (**Активы (Устройства)** → **Управляемые устройства**) и проверьте значения в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Последнее подключение к Серверу администрирования**.

Другие способы переноса данных

Помимо мастера переноса данных, вы также можете переносить определенные задачи и политики:

- Экспортируйте задачи (см. раздел "Экспорт задачи" см. стр. [1184](#)) из Kaspersky Security Center Windows, а затем импортируйте задачи (см. раздел "Импорт задачи" см. стр. [1184](#)) в Kaspersky Security Center Linux.
- Экспортируйте определенные политики (см. раздел "Экспорт политики" см. стр. [1257](#)) из Kaspersky Security Center Windows, а затем импортируйте политики (см. раздел "Импорт политики" на стр. [1258](#)) в Kaspersky Security Center Linux. Связанные профили политик экспортируются и импортируются вместе с выбранными политиками.

См. также:

Экспорт групповых объектов из Kaspersky Security Center Windows[1002](#)

Экспорт групповых объектов из Kaspersky Security Center Windows

Для переноса структуры группы администрирования, которая включает управляемые устройства и другие объекты группы из Kaspersky Security Center Windows в Kaspersky Security Center Linux, вам сначала необходимо выбрать данные для экспорта и создать файл экспорта. Файл экспорта содержит информацию обо всех групповых объектах, которые вы хотите перенести. Файл экспорта будет использоваться для последующего импорта в Kaspersky Security Center Linux.

Вы можете экспортировать следующие объекты:

- Задачи и политики управляемых приложений.
- Глобальные задачи.
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги, назначенные устройствам, данные которых вы переносите.

Перед началом экспорта прочтите общую информация о переносе данных в Kaspersky Security Center Linux (см. раздел "Перенос данных из Kaspersky Security Center Windows" см. стр. [999](#)). Выберите способ переноса данных: с использованием или без использования иерархии Серверов администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux.

► *Чтобы экспортировать управляемые устройства и связанные групповые объекты с помощью мастера переноса данных:*

1. В зависимости от того, организованы ли в иерархию Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux, выполните одно из следующих действий:
 - Если Серверы выстроены в иерархию, откройте Kaspersky Security Center Web Console и переключитесь на Сервер администрирования Kaspersky Security Center Windows.
 - Если Серверы не организованы в иерархию, откройте Kaspersky Security Center Web Console, подключенную к Kaspersky Security Center Windows.
2. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.
3. Чтобы запустить мастер и следовать его шагам, выберите, куда вы хотите перенести свои данные и параметры.
 - Если вы хотите перенести свои данные и параметры в Kaspersky Security Center Cloud Console, выберите параметр **Перенос данных в Kaspersky Security Center Cloud Console**.
 - Если вы хотите перенести свои данные и параметры в Kaspersky Security Center Linux или Kaspersky XDR Expert, выберите параметр **Перенос данных в Kaspersky Security Center Linux или Open Single Management Platform**.
4. Выберите группу или подгруппу администрирования, которую вы хотите экспортировать. Обратите внимание, что в выбранной группе или подгруппе администрирования должно быть не более 10 000 устройств.
5. Выберите управляемые приложения, задачи и политики которых будут экспортированы. Выберите только те приложения, которые поддерживаются Kaspersky Security Center Linux. Объекты неподдерживаемых приложений все равно будут экспортированы, но не будут работать.
6. Используйте ссылки слева, чтобы выбрать глобальные задачи, выбранные устройства и отчеты для экспорта. Ссылка **Группировать объекты** позволяет исключить из экспорта роли пользователей, внутренних пользователей и группы безопасности, а также пользовательские категории приложений.

Файл экспорта (ZIP-архив) создан. В зависимости от того, выполняете ли вы перенос данных с поддержкой иерархии Сервера администрирования, файл экспорта сохраняется следующим образом:

- Если Серверы выстроены в иерархию, файл экспорта сохраняется во временную папку на Сервере Kaspersky Security Center Web Console.
- Если Серверы не организованы в иерархию, файл экспорта загружается на ваше устройство.

При переносе данных с поддержкой иерархии Сервера администрирования импорт начинается автоматически (см. раздел "Переключение управляемых устройств под управление Kaspersky Security Center Linux" см. стр. [1005](#)) после успешного экспорта. При переносе данных без поддержки иерархии Сервера администрирования вы можете вручную импортировать сохраненный файл экспорта в Kaspersky Security Center Linux (см. раздел "Переключение управляемых устройств под управление Kaspersky Security Center Linux" см. стр. [1005](#)).

Импорт экспортного файла в Kaspersky Security Center Linux

Чтобы передать информацию об управляемых устройствах, объектах и их параметрах, которые вы экспортировали из Kaspersky Security Center Windows (см. раздел "Экспорт групповых объектов из Kaspersky Security Center Windows" см. стр. [1002](#)), вам нужно импортировать ее в приложение Kaspersky Security Center Linux или Kaspersky SMP.

► *Чтобы импортировать управляемые устройства и связанные групповые объекты с помощью мастера переноса данных:*

1. В зависимости от того, организованы ли в иерархию Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux, выполните одно из следующих действий:
 - Если Серверы организованы в иерархию, переходите к следующему шагу мастера переноса данных после завершения экспорта. Импорт начнется автоматически после успешного экспорта (см. раздел "Экспорт групповых объектов из Kaspersky Security Center Windows" см. стр. [1002](#)) в этом мастере (см. шаг 2 этой инструкции).
 - Если Серверы не организованы в иерархию:
 - a. Откройте Kaspersky Security Center Web Console, подключенный к Kaspersky Security Center Linux или к Kaspersky XDR Expert.
 - b. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.
 - c. Выберите файл экспорта (ZIP-архив), который вы создали и загрузили при экспорте из Kaspersky Security Center Windows (см. раздел «Экспорт групповых объектов из Kaspersky Security Center Windows» см. стр. [1002](#)). Начнется загрузка файла экспорта.
2. После успешной загрузки файла экспорта вы можете продолжить импорт. Если вы хотите указать другой файл для экспорта, перейдите по ссылке **Изменить** и выберите нужный файл.
3. Отобразится вся иерархия групп администрирования Kaspersky Security Center Linux.

Установите флажок рядом с целевой группой администрирования, в которой необходимо восстановить объекты экспортированной группы администрирования (управляемые устройства, политики, задачи и другие объекты группы).
4. Начнется импорт объектов группы. Свернуть мастер переноса данных и выполнять любые параллельные операции во время импорта невозможно. Дождитесь, пока значки (🔄) рядом со всеми пунктами в списке объектов заменятся на зеленые флажки (✓) и импорт завершится.
5. Когда импорт завершится, экспортированная структура групп администрирования, включая сведения об устройствах, появится в целевой группе администрирования, которую вы выбрали. Если имя восстанавливаемого объекта совпадает с именем существующего объекта, к восстановленному будет добавлен дополнительный суффикс.

Если в перенесенной задаче указаны данные учетной записи, под которой она запускается (см. раздел "Общие параметры задач" см. стр. [1176](#)), вам нужно открыть задачу и ввести пароль еще раз после завершения импорта.

Если импорт завершился с ошибкой, вы можете выполнить одно из следующих действий:

- Для переноса данных с поддержкой иерархии Сервера администрирования вы можете импортировать файл экспорта еще раз.
- Для переноса данных без поддержки иерархии Сервера администрирования вы можете запустить мастер переноса данных, чтобы выбрать другой файл экспорта, а затем импортировать его снова.

Вы можете проверить, были ли объекты группы, входящие в область экспорта, успешно импортированы в Kaspersky Security Center Linux. Для этого перейдите в раздел **Активы (Устройства)** и убедитесь, что импортированные объекты отображаются в соответствующих подразделах.

Обратите внимание, что импортированные управляемые устройства отображаются в подразделе **Управляемые устройства**, но они не видны в сети и на них не установлен и не запущен Агент администрирования (значение *Нет* в столбцах **Видимо в сети**, **Агент администрирования установлен**, **Агент администрирования запущен**).

Для завершения переноса данных вам необходимо переключить управляемые устройства под управление Kaspersky Security Center Linux (см. раздел "Переключение управляемых устройств под управление Kaspersky Security Center Linux" см. стр. [1005](#)).

Переключение управляемых устройств под управление Kaspersky Security Center Linux

После успешного импорта информации об управляемых устройствах, объектах и их параметрах в Kaspersky Security Center Linux для завершения переноса данных вам необходимо переключить управляемые устройства под управление Kaspersky Security Center Linux.

В текущей версии Kaspersky Security Center Linux вы можете переместить управляемые устройства под управлением Kaspersky Security Center Linux одним из следующих способов:

- Используя утилиту `klmover`.
- Восстановив сертификат и закрытый ключ Сервера администрирования из резервной копии данных.
Подробнее см. шаг 5 основного сценария переноса данных (см. раздел "О переносе данных в приложение Kaspersky Security Center Linux" см. стр. [1000](#)).
- Установив Агент администрирования на управляемые устройства с помощью задачи удаленной установки.

► *Чтобы переключить управляемые устройства под управление Kaspersky Security Center Linux, установив Агент администрирования:*

1. Переключитесь на Сервер администрирования Kaspersky Security Center Windows.
2. Перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты** и откройте свойства существующего инсталляционного пакета Агента администрирования.

Если инсталляционный пакет Агента администрирования отсутствует в списке пакетов, загрузите новый (см. раздел "Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"" см. стр. [1087](#)).

3. На вкладке **Параметры** выберите раздел **Подключение**. Укажите параметры подключения Сервера администрирования Kaspersky Security Center Linux.
4. Создайте задачу удаленной установки для импортированных управляемых устройств, а затем укажите перенастроенный инсталляционный пакет Агента администрирования.

Вы можете установить Агент администрирования с помощью Сервера администрирования Kaspersky Security Center Windows или с помощью устройства под управлением Windows, которое выполняет роль точки распространения (см. раздел "Назначение точек распространения вручную" см. стр. [1370](#)). Если вы используете Сервер администрирования, включите параметр **Средствами операционной системы с помощью Сервера администрирования**. Если вы используете точку распространения, включите параметр **Средствами операционной системы с помощью точек распространения**.

5. Запустите задачу удаленной установки приложения.

После успешного завершения задачи удаленной установки перейдите на Сервер администрирования Kaspersky Security Center Linux и убедитесь, что управляемые устройства видны в сети и что на них установлен и запущен Агент администрирования (значение *Да* в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Агент администрирования запущен**).

Вход в приложение Kaspersky Security Center Web Console и выход из него

Вы можете войти в Kaspersky Security Center Web Console после установки Сервера администрирования и Kaspersky Security Center Web Console (см. раздел "Установка" см. стр. [987](#)). Вам нужно знать веб-адрес Сервера администрирования и номер порта, указанный во время установки (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)) (по умолчанию используется порт 8080). В вашем браузере JavaScript должен быть включен.

Войти в Kaspersky Security Center Web Console можно одним из следующих способов:

- Используя доменную аутентификацию (см. раздел "Настройка доменной аутентификации с использованием протоколов NTLM и Kerberos" на стр. [1015](#)).

Если вы выберете этот способ, убедитесь, что опрос контроллеров домена (см. стр. [1117](#)) активирован и доменные пользователи добавлены на Сервер администрирования.

- Указав имя учетной записи и пароль администратора.

Вход с использованием доменной аутентификации

► Чтобы войти в Kaspersky Security Center Web Console, используя доменную аутентификацию:

1. В браузере укажите <веб-адрес Сервера администрирования>:<номер порта>.

Отобразится страница входа в приложение.

2. Если вы добавили несколько доверенных Серверов администрирования, в списке выберите Сервер администрирования, к которому вы хотите подключиться.

Если вы добавили только один Сервер администрирования, список Серверов администрирования не отображается.

3. Выполните одно из следующих действий:

- Нажмите на кнопку **Использовать доменную аутентификацию**.
- Если на Сервере создан один или несколько виртуальных Серверов администрирования и вы хотите войти на виртуальный Сервер с использованием доменной аутентификации:
 - a. Нажмите на кнопку **Показать параметры виртуального Сервера**.
 - b. Введите имя виртуального Сервера администрирования, которое вы указали при создании виртуального Сервера (см. раздел «Создание виртуального Сервера администрирования» см. стр. [1025](#)).
 - c. Нажмите на кнопку **Использовать доменную аутентификацию**.

4. Если для вашей учетной записи включена двухэтапная проверка (см. раздел "Включение двухэтапной проверки для вашей учетной записи" на стр. [1036](#)), укажите код безопасности, сгенерированный приложением для аутентификации на мобильном устройстве.

При необходимости вы можете вернуться на страницу входа.

После входа в систему информационная панель отображается с языком и темой, которые вы использовали в последний раз. Вы можете перемещаться по Kaspersky Security Center Web Console и использовать ее для работы с Kaspersky Security Center.

Вход с указанием имени учетной записи и пароля администратора

- Чтобы войти в Kaspersky Security Center Web Console, указав имя учетной записи и пароль администратора:

1. В браузере укажите <веб-адрес Сервера администрирования>:<номер порта>.

Отобразится страница входа в приложение.

2. Если вы добавили несколько доверенных Серверов администрирования, в списке выберите Сервер администрирования, к которому вы хотите подключиться.

Если вы добавили только один Сервер администрирования, список Серверов администрирования не отображается.

3. Выполните одно из следующих действий:

- Для входа на Сервер администрирования:
 - a. Введите имя пользователя и пароль локального администратора.
 - b. Нажмите на кнопку **Войти**.
- Если на Сервере создан один или несколько виртуальных Серверов администрирования и вы хотите войти на виртуальный Сервер:
 - a. Нажмите на кнопку **Показать параметры виртуального Сервера**.
 - b. Введите имя виртуального Сервера администрирования, которое вы указали при создании виртуального Сервера (см. раздел «Создание виртуального Сервера администрирования» см. стр. [1025](#)).

- c. Введите имя пользователя и пароль администратора, имеющего права на виртуальном Сервере администрирования.
- d. Нажмите на кнопку **Войти**.
4. Если для вашей учетной записи включена двухэтапная проверка (см. раздел "Включение двухэтапной проверки для вашей учетной записи" на стр. [1036](#)), укажите код безопасности, сгенерированный приложением для аутентификации на мобильном устройстве.
При необходимости вы можете вернуться на страницу входа.
5. Если для вашей учетной записи включено принудительное изменение пароля (см. раздел "Изменение пароля учетной записи пользователя" см. стр. [1314](#)) или срок действия пароля истек, отобразится окно изменения пароля. Установите новый пароль для входа в Kaspersky Security Center Web Console.

После входа в систему информационная панель отображается с языком и темой, которые вы использовали в последний раз. Вы можете перемещаться по Kaspersky Security Center Web Console и использовать ее для работы с Kaspersky Security Center.

Выход

- Чтобы выйти из Kaspersky Security Center Web Console,

в главном меню перейдите в параметры своей учетной записи и выберите **Выход**.

Приложение Kaspersky Security Center Web Console закрыто, отображается страница входа в приложение.

Identity and Access Manager в Kaspersky Security Center Web Console

В этом разделе представлена информация о Identity and Access Manager (далее также IAM).

О компоненте Identity and Access Manager

Identity and Access Manager (далее также IAM) – это компонент Kaspersky Security Center Web Console, позволяющий использовать единый вход (Single Sign-on, SSO) между Kaspersky Security Center Web Console и веб-интерфейсом Kaspersky Industrial CyberSecurity for Networks. IAM использует протокол OAuth 2.0 для авторизации Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console.

В этом случае приложение Kaspersky Industrial CyberSecurity for Networks, доступ к которому вы получаете через Kaspersky Security Center Web Console, называется *сервером ресурсов*, Kaspersky Security Center Web Console и веб-интерфейс Kaspersky Industrial CyberSecurity for Networks называются *клиенты OAuth 2.0*. Сервер ресурсов – это приложение, которое работает с несколькими пользователями и требует авторизации. Клиент использует *токен* для авторизации на сервере ресурсов. Токен – это уникальная последовательность байтов. По истечении срока действия токена он автоматически перевыпускается. IAM действует как единый сервер авторизации для нескольких клиентов OAuth 2.0.

Вы можете установить IAM при установке Kaspersky Security Center Web Console. Вы можете включить его позже в любой момент в параметрах Kaspersky Security Center Web Console. Если Сервер Kaspersky Industrial CyberSecurity или веб-интерфейс Kaspersky Industrial CyberSecurity установлены на устройстве, управляемым тем же Сервером администрирования, IAM обнаруживает это приложение, и в Kaspersky

Security Center Web Console отображается уведомление об этом. Вы можете зарегистрировать Kaspersky Industrial CyberSecurity for Networks, а затем использовать SSO как для Kaspersky Security Center Web Console, так и для веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Если вы выйдете из Kaspersky Security Center Web Console, ваш сеанс в веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks завершится, и вам придется снова войти в Kaspersky Security Center Web Console.

См. также:

Включение Identity and Access Manager: сценарий.....	1009
Настройка Identity and Access Manager в Kaspersky Security Center Web Console	1011
Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console	1011
Время жизни токенов и время ожидания авторизации для Identity and Access Manager	1013
Загрузка и распространение IAM-сертификатов.....	1014
Отключение Identity and Access Manager	1015
Установка Kaspersky Security Center Web Console	988
Порты, используемые приложением Kaspersky Security Center Web Console	980

Включение Identity and Access Manager: сценарий

Предварительные требования

Перед началом работы убедитесь, что у вас есть доступ к Kaspersky Industrial CyberSecurity for Networks версии 3.1 или новее.

Этапы

Включение Identity and Access Manager (также называемого IAM) происходит поэтапно:

а. Проверка необходимых портов

Убедитесь, что на устройстве, на котором установлено приложение Kaspersky Security Center Web Console, открыты порты 3333, 4004 и 4444. Эти порты необходимы для использования OAuth 2.0. Вы можете изменить номера портов по умолчанию в окне параметров Kaspersky Security Center Web Console (см. раздел "Настройка Identity and Access Manager в Kaspersky Security Center Web Console" на стр. [1011](#)).

Кроме портов 3333, 4004 и 4444, Kaspersky Security Center Web Console также использует порты 4445, 2444 и 2445 для различных целей (см. раздел "Порты, используемые приложением Kaspersky Security Center Web Console" на стр. [980](#)).

б. Установка Identity and Access Manager

Во время установки (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)) Kaspersky Security Center Web Console укажите, что вы хотите установить Identity and Access Manager. Если вы этого не сделали, запустите еще раз мастер установки Kaspersky Security Center Web Console.

c. Настройка Identity and Access Manager

В окне параметров Kaspersky Security Center Web Console (см. раздел "Настройка Identity and Access Manager в Kaspersky Security Center Web Console" на стр. [1011](#)) убедитесь, что переключатель **Identity and Access Manager (IAM)** включен. Также укажите DNS-имя устройства, на котором установлено приложение Kaspersky Security Center Web Console: клиентские приложения будут подключаться к этому устройству.

d. Указание параметров токена

В окне параметров Kaspersky Security Center Web Console (см. раздел "Настройка Identity and Access Manager в Kaspersky Security Center Web Console" на стр. [1011](#)) укажите время жизни токенов и время ожидания авторизации, которые будет использовать Identity and Access Manager. Вы можете использовать значения по умолчанию или указать свои значения в соответствии с вашими требованиями.

e. Предоставление сертификатов

Если вы предпочитаете использовать сертификаты, сгенерированные Сервером администрирования, то в окне параметров Kaspersky Security Center Web Console (см. раздел "Настройка Identity and Access Manager в Kaspersky Security Center Web Console" на стр. [1011](#)) загрузите корневые сертификаты для портов, используемых IAM, и раздайте их рабочим станциям пользователей Kaspersky Security Center Web Console. В противном случае браузеры пользователей будут отображать сообщения об ошибках при попытке подключения к Kaspersky Security Center Web Console.

f. Регистрация Серверов Kaspersky Industrial CyberSecurity for Networks и веб-интерфейсов Kaspersky Industrial CyberSecurity for Networks

При установке IAM в Kaspersky Security Center Web Console отображается сообщение о том, что Сервер Industrial CyberSecurity for Networks (или несколько Серверов) и один или несколько веб-интерфейсов Kaspersky Industrial CyberSecurity for Networks ожидают регистрации. Нажмите на это сообщение, чтобы зарегистрировать (см. раздел "Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console" на стр. [1011](#)) Сервер Kaspersky Industrial CyberSecurity for Networks Server (или Серверы) и веб-интерфейс (или веб-интерфейсы).

Результаты

После завершения этого сценария вы сможете использовать SSO и IAM <https://support.kaspersky.com/KICSforNetworks/3.1/en-US/110348.htm> для Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center Web Console.

Настройка Identity and Access Manager в Kaspersky Security Center Web Console

► Чтобы настроить Identity and Access Manager в соответствии с вашими требованиями:

1. В главном меню перейдите в раздел **Параметры** → **Identity and Access Manager**.
2. В разделе **Identity and Access Manager** убедитесь, что Identity and Access Manager включен.
3. Перейдите по ссылке **Параметры** в блоке **Сетевое имя устройства Identity and Access Manager**.
4. Укажите DNS-имя устройства, на котором вы установили Identity and Access Manager. Клиентские приложения будут подключаться к этому устройству.
5. Если хотите, измените параметры токена по умолчанию (см. раздел "Время жизни токенов и время ожидания авторизации для Identity and Access Manager" на стр. [1013](#)), параметры сертификата (см. раздел "Загрузка и распространение IAM-сертификатов" на стр. [1014](#)), а также номера портов (см. раздел "Порты, используемые приложением Kaspersky Security Center Web Console" на стр. [980](#)) нажав на ссылку **Параметры** под соответствующей группой параметров.

Identity and Access Manager включен и работает в соответствии с вашими требованиями.

См. также:

Включение Identity and Access Manager: сценарий.....[1009](#)

Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console

Чтобы начать работу с приложением Kaspersky Industrial CyberSecurity for Networks через Kaspersky Security Center Web Console, необходимо предварительно зарегистрировать его в Kaspersky Security Center Web Console.

Чтобы зарегистрировать приложение Kaspersky Industrial CyberSecurity for Networks:

1. Убедитесь, что сделано следующее:
 - Вы загрузили и установили веб-плагин Kaspersky Industrial CyberSecurity for Networks.
Также можно сделать это позже, ожидая синхронизацию Сервера Kaspersky Industrial CyberSecurity for Networks с Сервером администрирования.
 - Вы завершили сценарий подготовки к использованию технологии единого входа (SSO).
 - Необходимые параметры в веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks заданы на странице Kaspersky Security Center. Подробную информацию см. в онлайн-справке Kaspersky Industrial CyberSecurity for Networks.
 - Вы вошли в Kaspersky Security Center Web Console под учетной записью администратора.
 - IAM настроен (см. раздел "Настройка Identity and Access Manager в Kaspersky Security Center Web Console" на стр. [1011](#)).
2. Переместите устройство, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks, из группы Нераспределенные устройства в группу Управляемые устройства:

- a. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
 - b. Установите флажок рядом с устройством, на котором установлен Kaspersky Industrial CyberSecurity for Networks Server.
 - c. Нажмите на кнопку **Переместить в группу**.
 - d. В иерархии групп администрирования установите флажок рядом с группой **Управляемые устройства**.
 - e. Нажмите на кнопку **Переместить**.
3. Перейдите к свойствам устройства, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks.
 4. На странице свойств устройства в разделе **Общие**, выберите параметр **Не разрывать соединение с Сервером администрирования**, а затем нажмите на кнопку **Сохранить**.
 5. В окне свойств устройства выберите раздел **Приложения**.
 6. В разделе **Приложения** выберите Агент администрирования.
 7. Если текущий статус приложения *Остановлено*, подождите, пока он не изменится на *Выполняется*.
Это может занять до 15 минут. Если вы еще не установили веб-плагин Kaspersky Industrial CyberSecurity for Networks, вы можете сделать это сейчас, пока ждете.
 8. В главном меню перейдите в раздел **Параметры** → **Identity and Access Manager**.
В поле **Запросы на регистрацию**, отображается один ожидающий запрос.
 9. Перейдите по ссылке **Параметры**, расположенной ниже поля **Запросы на регистрацию**.
 10. В открывшемся списке зарегистрированных клиентов установите флажок рядом с названием того Сервера Kaspersky Industrial CyberSecurity for Networks, который имеет статус *Ожидает применения*, а затем нажмите на кнопку **Одобрить**.

Если вы не хотите регистрировать Сервер Kaspersky Industrial CyberSecurity for Networks, вы можете нажать на кнопку **Отклонить** и вернуться к этому списку позже.

После того, как вы нажмете на кнопку **Одобрить**, статус меняется на *Одобрено*, а затем на *Готов*. Если статус не поменялся, вы можете нажать на кнопку **Обновить**.
 11. Закройте список зарегистрированных клиентов и убедитесь, что значение в поле **Зарегистрированные клиенты** увеличилось.
 12. Чтобы добавить веб-виджет Kaspersky Industrial CyberSecurity for Networks на панель управления:
 - a. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
 - b. В панели управления нажмите на кнопку **Добавить или восстановить веб-виджет**.
 - c. В появившемся веб-виджете нажмите на кнопку **Другое**.
 - d. Выберите виджет Kaspersky Industrial CyberSecurity for Networks.
 Теперь вы можете перейти в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks по ссылке в веб-виджете.

После завершения процедуры регистрации появится новая кнопка **Kaspersky Security Center**, которая отображается на странице входа в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks. Вы можете нажать на эту кнопку, чтобы войти в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks под своими учетными данными Kaspersky Security Center.

Время жизни токенов и время ожидания авторизации для Identity and Access Manager

При настройке компонента Identity and Access Manager (далее также IAM) необходимо указать параметры времени жизни токена и время ожидания авторизации. Параметры по умолчанию разработаны с учетом одновременно и стандартов безопасности, и нагрузки на Сервер. Вы можете менять эти параметры в соответствии с политиками вашей организации.

IAM автоматически повторно выпускает токен, когда срок его действия истекает.

В таблице ниже перечислены параметры времени жизни токена по умолчанию.

Таблица 85. Параметры времени жизни токена

Токен	Время жизни по умолчанию (в секундах)	Описание
Идентификационный токен (id_token)	86400	Идентификационный токен, используемый клиентом OAuth 2.0 (то есть Kaspersky Security Center Web Console или веб-интерфейсом Kaspersky Industrial CyberSecurity). IAM отправляет идентификатор токена, который содержит информацию о пользователе (то есть профиль пользователя) клиенту.
Токен доступа (access_token)	86400	Токен доступа, используемый клиентом OAuth 2.0 для доступа к серверу ресурсов от имени владельца ресурса, определенного IAM.
Обновить токен (refresh_token)	172800	Клиент OAuth 2.0 использует этот токен для повторной выдачи идентификационного токена и токена доступа.

В таблице ниже приведено время ожидания для auth_code и login_consent_request.

Таблица 86. Параметры времени ожидания авторизации

Параметр	Время ожидания по умолчанию (в секундах)	Описание
Код авторизации (auth_code)	3600	Время ожидания обмена кода токена. Клиент OAuth 2.0 отправляет этот код на сервер ресурсов и взамен получает токен доступа.
Время ожидания запроса на вход (login_consent_request)	3600	Время ожидания для делегирования прав пользователя клиенту OAuth 2.0.

Для получения дополнительной информации о токенах см. веб-сайт OAuth <https://www.oauth.com>.

► *Чтобы настроить время ожидания для клиентов, у которых не обнаружена активность мыши или клавиатуры:*

1. В папке установки Kaspersky Security Center Web Console найдите и откройте файл config.json. Файл содержит параметры для настройки времени ожидания бездействия клиентов.
2. Используйте параметр `clientIdleTimeout`, чтобы указать время в миллисекундах, по истечении которого неактивному клиенту отобразится всплывающее окно с предупреждением.
3. Используйте параметр `clientLogoutTimeout`, чтобы указать время в миллисекундах, по истечении которого IAM-авторизация для неактивного клиента завершается. Значение параметра `ClientLogoutTimeout` отсчитывается последовательно после параметра `clientIdleTimeout`.

См. также:

Включение Identity and Access Manager: сценарий.....[1009](#)

Загрузка и распространение IAM-сертификатов

По умолчанию Identity and Access Manager использует сертификаты, созданные Сервером администрирования, для предоставления доступа браузерам к Kaspersky Security Center Web Console. Вы также можете использовать пользовательские сертификаты. Какой бы сертификат вы ни использовали, вам нужно убедиться, что все рабочие станции, с которых пользователи Kaspersky Security Center Web Console обращаются к Kaspersky Security Center Web Console, доверяют этому сертификату.

► *Чтобы загрузить и распространить сертификаты:*

1. В главном меню перейдите в раздел **Параметры** → **Identity and Access Manager**.
2. Для каждого сертификата нажмите на ссылку **Настройки** под соответствующей группой параметров, и выполните одно из следующих действий:
 - Если вы хотите использовать сертификат, сгенерированный Сервером администрирования при установке Kaspersky Security Center Web Console:
 1. Выберите **Сертификат, созданный Сервером администрирования** в открывшемся окне свойств сертификата.
 2. Нажмите на кнопку **Загрузить**, чтобы загрузить сертификат.
 3. Распространите загруженный сертификат на все рабочие станции, с которых пользователи Kaspersky Security Center Web Console получают доступ к Kaspersky Security Center Web Console.
 - Если у вас есть сертификат, который вы хотите использовать:
 1. Выберите **Пользовательский TLS-сертификат** в открывшемся окне свойств сертификата.
 2. Выберите файл сертификата и закрытый ключ.
 3. Нажмите на кнопку **ОК**.
 4. Распространите сертификат на все рабочие станции, с которых пользователи получают доступ к Kaspersky Security Center Web Console или веб-интерфейсу Kaspersky Industrial CyberSecurity.

Сертификаты предоставляют пользователям доступ к Kaspersky Security Center Web Console и веб-интерфейсу Kaspersky Industrial CyberSecurity.

Вам необходимо своевременно перевыпустить все сертификаты. Сертификаты, сгенерированные Сервером администрирования, необходимо заново сгенерировать вручную. Сертификаты, сгенерированные установщиком (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)) Kaspersky Security Center Web Console, необходимо повторно сгенерировать с помощью установщика.

См. также:

Включение Identity and Access Manager: сценарий.....[1009](#)

Отключение Identity and Access Manager

Вы можете выключить Identity and Access Manager (IAM).

► Чтобы отключить IAM,

1. В главном окне приложения перейдите в раздел **Параметры** → **Интеграция**.
2. В разделе **Identity and Access Manager** установите переключатель **Identity and Access Manager** в положение выключено.

Вы можете включить IAM позже в любое время.

Если вы обновите Kaspersky Security Center Web Console через установщик и укажете, что вы не хотите устанавливать IAM, то Kaspersky Security Center Web Console будет обновлен, а IAM не будет установлен. С вашего устройства будут удалены: вся информация об интеграции с Kaspersky Industrial CyberSecurity for Networks, файлы конфигурации IAM и файлы журналов событий.

См. также:

Включение Identity and Access Manager: сценарий.....[1009](#)

Настройка доменной аутентификации с использованием протоколов NTLM и Kerberos

Kaspersky Security Center позволяет использовать доменную аутентификацию в OpenAPI по протоколам NTLM и Kerberos. Использование доменной аутентификации позволяет пользователю Windows включить безопасную аутентификацию в Kaspersky Security Center Web Console без повторного ввода пароля в корпоративной сети (единый вход).

Доменная аутентификация в OpenAPI по протоколу Kerberos имеет следующие ограничения:

- Пользователь Kaspersky Security Center Web Console должен пройти аутентификацию в Active Directory по протоколу Kerberos. У пользователя должен быть действующий мандат на выдачу мандатов Kerberos (далее также TGT). TGT выдается автоматически при аутентификации в домене.
- Вам нужно настроить аутентификацию Kerberos в браузере. Подробнее см. в документации используемого вами браузера.

Если вы хотите использовать доменную аутентификацию с использованием протоколов Kerberos, ваша сеть должна соответствовать следующим условиям:

- Сервер администрирования должен запускаться под доменной учетной записью.
- Сервер Kaspersky Security Center Web Console установлен на том же устройстве, что и Сервер администрирования.
- Для учетной записи Сервера администрирования необходимо указать следующие имена субъектов службы (SPN):
 - "http/<server.fqnd.name>"
 - "http/<server>"

Здесь <server> – сетевое имя устройства Сервера администрирования, <server.fqnd.name> – полное доменное имя устройства Сервера администрирования.

- При подключении через Консоль администрирования или Kaspersky Security Center Web Console необходимо указывать адрес Сервера администрирования точно так же, как адрес, для которого зарегистрировано имя субъекта-службы (SPN). Вы можете указать или <server.fqnd.name> или <server>.
- Для входа без пароля процесс браузера, в котором открыта Kaspersky Security Center Web Console, должен работать под доменной учетной записью.

Протоколы Kerberos и NTLM поддерживаются только в OpenAPI для Kaspersky Security Center. Эти протоколы не поддерживаются в OpenAPI для Kaspersky Security Center Linux.

Настройка Сервера администрирования

В этом разделе описан процесс настройки и свойства Сервера администрирования Kaspersky Security Center.

В этом разделе

Настройка параметров подключения Kaspersky Security Center Web Console к Серверу администрирования	1017
Настройка журнала событий подключения к Серверу администрирования	1018
Настройка количества событий в хранилище событий	1018
Параметры подключения устройств с защитой на уровне UEFI	1019
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования	1020
Просмотр списка подчиненных Серверов администрирования	1022
Удаление иерархии Серверов администрирования	1023
Обслуживание Сервера администрирования	1023
Настройка интерфейса	1024
Управление виртуальными Серверами администрирования	1025
Включение защиты учетной записи от несанкционированного изменения	1031
Двухэтапная проверка	1031
Резервное копирование и восстановление данных Сервера администрирования	723
Создание задачи резервного копирования данных	1043
Перенос Сервера администрирования на другое устройство	1044

Настройка параметров подключения Kaspersky Security Center Web Console к Серверу администрирования

► Чтобы задать порты подключения к Серверу администрирования:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Порты подключения**.

Будут отображены основные параметры подключения к выбранному Серверу Администрирования.

Приложение Kaspersky Security Center Web Console подключено к Серверу администрирования по SSL-порту TCP 13299. Этот же порт может использоваться объектами автоматизации klakaut.

Порт TCP 14000 может использоваться для подключения Kaspersky Security Center Web Console, точек распространения, подчиненных Серверов администрирования и объектов автоматизации утилиты klakaut, а также для получения данных с клиентских устройств.

Как правило, SSL-порт TCP 13000 могут использовать только Агент администрирования, подчиненный Сервер и главный Сервер администрирования, размещенный в демилитаризованной зоне. В некоторых

случаях может быть необходимо подключение Kaspersky Security Center Web Console по SSL-порту 13000:

- если предпочтительно использовать один и тот же SSL-порт как для Kaspersky Security Center Web Console, так и для других активностей (для получения данных с клиентских устройств, подключения точек распространения, подключения подчиненных Серверов администрирования);
- если объект автоматизации утилиты klakaut подключается к Серверу администрирования не напрямую, а через точку распространения, размещенную в демилитаризованной зоне.

Настройка журнала событий подключения к Серверу администрирования

Можно сохранить в файл журнала историю подключений и попыток подключения к Серверу администрирования в процессе его работы. Информация в файле позволит отследить не только подключения внутри инфраструктуры сети, но и попытки несанкционированного доступа к серверам.

► *Чтобы настроить регистрацию событий подключения к Серверу администрирования:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Порты подключения**.
3. Включите параметр **Записывать события соединения с Сервером администрирования в журнал**.

Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл
%ProgramData%\KasperskyLab\admindkit\logs\sc.syslog.

Настройка количества событий в хранилище событий

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

- Чтобы ограничить количество событий, которые можно сохранить в хранилище событий на Сервере администрирования:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Хранилище событий**. Укажите максимальное количество событий, хранящихся в базе данных.
3. Нажмите на кнопку **Сохранить**.

Также можно изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи. Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

См. также:

О блокировке частых событий	1536
Сценарий: настройка защиты сети.....	403

Параметры подключения устройств с защитой на уровне UEFI

Устройство с защитой на уровне UEFI – это устройство со встроенным на уровне BIOS решением или приложением "Лаборатории Касперского" для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска приложения безопасности. Kaspersky Security Center поддерживает управление такими устройствами.

- Чтобы изменить параметры подключения устройств с защитой на уровне UEFI:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Дополнительные порты**.
3. Измените требуемые параметры:
 - **Открыть порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**
Если флажок установлен, то устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.
По умолчанию флажок установлен.
 - **Порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**
Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию используется порт 13294.

4. Нажмите на кнопку **Сохранить**.

Устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Добавление подчиненного Сервера администрирования (выполняется с будущим главным Сервером администрирования)

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер".

- *Чтобы добавить Сервер администрирования, доступный для подключения через Kaspersky Security Center Web Console, в качестве подчиненного Сервера:*

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.

2. На будущем главном Сервере администрирования нажмите на значок параметров ().

3. На открывшейся странице свойств перейдите на вкладку **Серверы администрирования**.

4. Установите флажок рядом с именем группы администрирования, в которую вы хотите добавить Сервер администрирования.

5. В меню выберите пункт **Подключить подчиненный Сервер администрирования**.

Запустится мастер добавления подчиненного Сервера администрирования. Для продолжения работы мастера нажмите на кнопку **Далее**.

6. Заполните следующие поля:

- **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**

Выберите этот параметр, если подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ).

Если выбран этот параметр, необходимо указать **Адрес подчиненного Сервера**.

Если выбран этот параметр, главный Сервер администрирования инициирует подключение к подчиненному Серверу администрирования. Иначе подчиненный Сервер администрирования инициирует подключение к главному Серверу администрирования.

- **Имя подчиненного Сервера администрирования**

Имя подчиненного Сервера администрирования, которое будет отображаться в иерархии Серверов. Вы можете ввести IP-адрес в качестве имени или использовать такое имя, как, например, "Подчиненный Сервер для группы 1".

- **Адрес подчиненного Сервера администрирования (необязательно)**

Укажите IP-адрес или доменное имя подчиненного Сервера администрирования.

Этот параметр необходим, если включен параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

- **SSL-порт Сервера администрирования**

Укажите номер SSL-порта главного Сервера администрирования. По умолчанию установлен порт 13000.

- **API-порт Сервера администрирования**

Укажите номер порта главного Сервера администрирования для получения соединений через OpenAPI. По умолчанию установлен порт 13299.

7. Укажите сертификат подчиненного Сервера администрирования. Если вы указали параметр **Адрес подчиненного Сервера**, чтобы получить сертификат, нажмите на кнопку **Получить с подчиненного Сервера администрирования**. Или нажмите на кнопку **Выбрать файл сертификата** и найдите файл сертификата.

8. Задайте параметры подключения:

- Введите адрес будущего главного Сервера администрирования.
- Если будущий подчиненный Сервер администрирования использует прокси-сервер, введите адрес прокси-сервера и учетные данные пользователя для подключения к прокси-серверу.

9. Введите учетные данные пользователя, имеющего права доступа на будущий подчиненный Сервер администрирования.

10. Если двухэтапная проверка включена и настроена, укажите код безопасности, сгенерированный приложением для аутентификации.

Если двухэтапная проверка включена, но не настроена для учетной записи, которую вы указали, создайте иерархию только из будущего подчиненного Сервера (см. инструкции ниже).

Если параметры соединения верны, устанавливается соединение с будущим подчиненным Сервером и строится иерархия "главный/подчиненный". Если подключение не удалось, проверьте параметры подключения или укажите сертификат будущего подчиненного Сервера вручную.

Соединение между главным и подчиненным Серверами администрирования устанавливается через порт 13000. Задачи и политики главного Сервера администрирования получены и применены.

Подчиненный Сервер администрирования отображается на главном Сервере администрирования, в группе администрирования, в которую он был добавлен.

Добавление подчиненного Сервера администрирования (выполняется с будущим подчиненным Сервером администрирования)

Если вы не можете подключиться к будущему подчиненному Серверу администрирования (например, потому что он был временно отключен или недоступен), вы все равно можете добавить подчиненный Сервер администрирования.

► *Чтобы добавить Сервер администрирования, недоступный для подключения через Kaspersky Security Center Web Console, в качестве подчиненного Сервера:*

1. Отправьте файл сертификата будущего главного Сервера администрирования системному администратору офиса, в котором находится будущий подчиненный Сервер администрирования. (Например, вы можете записать файл на внешнее устройство или отправить его по электронной почте.)

Файл сертификата находится на будущем главном Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\admindkit\1093\cert\klserver.cer.

2. Предложите системному администратору, ответственному за будущий подчиненный Сервер администрирования, следующее:

- a. Нажмите на значок параметров (.
- b. На открывшейся странице свойств перейти в раздел **Иерархия Серверов администрирования** на вкладке **Общие**.
- c. Выберите параметр **Данный Сервер администрирования является подчиненным в иерархии**.
- d. В поле **Адрес главного Сервера администрирования** введите сетевое имя будущего главного Сервера администрирования.
- e. Выбрать ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.
- f. Если необходимо, установить флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.
- g. Если подключение к будущему подчиненному Серверу администрирования выполняется с помощью прокси-сервера, выберите параметр **Использовать прокси-сервер** и задайте параметры подключения.
- h. Нажмите на кнопку **Сохранить**.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Главный Сервер начинает принимать подключение от подчиненного Сервера, используя порт 13000. Задачи и политики главного Сервера администрирования получены и применены. Подчиненный Сервер администрирования отображается на главном Сервере администрирования, в группе администрирования, в которую он был добавлен.

Просмотр списка подчиненных Серверов администрирования

- Чтобы просмотреть список подчиненных (включая виртуальные) Серверов администрирования:

в главном меню нажмите на имя Сервера администрирования, которое находится рядом со значком параметров (.

Отобразится раскрывающийся список подчиненных (включая виртуальные) Серверов администрирования.

Вы можете перейти на любой из этих Серверов администрирования, нажав на его имя.

Группы администрирования тоже отображаются, но они неактивны и недоступны для управления в этом меню.

Если вы подключены к главному Серверу администрирования в Kaspersky Security Center Web Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- Измените существующую установку Kaspersky Security Center Web Console, добавив подчиненный Сервер в список доверенных Серверов администрирования. После этого вы сможете подключиться к виртуальному Серверу администрирования в Kaspersky Security Center Web Console.
- Используйте Kaspersky Security Center Web Console, чтобы напрямую подключиться к подчиненному Серверу администрирования (см. раздел "Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования" см. стр. [1020](#)), на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center Web Console.
- Используйте Консоль администрирования на основе MMC для прямого подключения к виртуальному Серверу.

Удаление иерархии Серверов администрирования

Если вам больше не нужна иерархия Серверов администрирования, вы можете отключить их от этой иерархии.

► *Чтобы удалить иерархию Серверов администрирования:*

1. В главном меню нажмите на значок параметров () рядом с именем главного Сервера администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. В группе администрирования, в которой вы хотите удалить подчиненный Сервер администрирования, выберите подчиненный Сервер администрирования.
4. В меню выберите пункт **Удалить**.
5. В открывшемся окне нажмите на кнопку **ОК** для подтверждения удаления подчиненного Сервера администрирования.

Бывший главный и бывшие подчиненные Серверы администрирования теперь независимы друг от друга. Иерархии Серверов больше не существует.

Обслуживание Сервера администрирования

Обслуживание Сервера администрирования позволяет освободить место в папке Сервера администрирования и уменьшить объем базы данных за счет удаления ненужных объектов. Это поможет вам повысить производительность и надежность работы приложения. Рекомендуется обслуживать Сервер администрирования не реже раза в неделю.

Обслуживание Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания Сервера администрирования приложение выполняет следующие действия:

- Удаляет ненужные папки и файлы из папки хранилища.

- Удаляет ненужные записи из таблиц (также известные как "висячие указатели").
- Очищает кеш.
- Обслуживает базу данных (если вы используете SQL Server или PostgreSQL в качестве СУБД):
 - проверяет базу данных на наличие ошибок (доступно только для SQL Server);
 - перестраивает индексы базы данных;
 - обновляет статистику базы данных;
 - сжимает базу данных (если необходимо).

Задача Обслуживание Сервера администрирования поддерживает MariaDB версии 10.3 и выше. Если используется MariaDB версии 10.2 или ниже, администраторам следует обслуживать базу данных самостоятельно.

Задача Обслуживание Сервера администрирования создается автоматически при установке Kaspersky Security Center. Если задача Обслуживание Сервера администрирования удалена, вы можете создать ее вручную.

► *Чтобы создать задачу Обслуживание Сервера администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи.
3. В окне мастера **Параметры новой задачи** выберите тип задачи **Обслуживание Сервера администрирования** и нажмите на кнопку **Далее**.
4. Следуйте дальнейшим шагам мастера.

В результате созданная задача отобразится в списке задач. Для одного Сервера администрирования может выполняться только одна задача Обслуживание Сервера администрирования. Если задача Обслуживание Сервера администрирования для Сервера администрирования уже создана, создание еще одной задачи Обслуживание Сервера администрирования невозможно.

Настройка интерфейса

Вы можете настроить интерфейс Kaspersky Security Center Web Console на отображение и скрытие разделов и элементов интерфейса в зависимости от используемых функций.

► *Чтобы настроить интерфейс Kaspersky Security Center Web Console в соответствии с используемым в настоящее время набором функций:*

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса**.
2. В появившемся окне **Параметры интерфейса** включите или выключите необходимые параметры.
3. Нажмите на кнопку **Сохранить**.

После этого в консоли отображаются разделы в главном меню в соответствии с включенными параметрами. Например, если включить **Показать EDR-алерты**, раздел **Мониторинг и отчеты** → **Алерты** появится в главном меню.

Управление виртуальными Серверами администрирования

В этом разделе описываются следующие действия, как управлять виртуальными Серверами администрирования:

- создание виртуальных Серверов администрирования (см. раздел "Создание виртуального Сервера администрирования" на стр. [1025](#));
- включение и выключение виртуальных Серверов администрирования (см. раздел "Включение и выключение виртуального Сервера администрирования" на стр. [1026](#));
- назначение администратора виртуального Сервера администрирования (см. раздел "Назначение администратора виртуального Сервера администрирования" см. стр. [1027](#));
- смена Сервера администрирования для клиентских устройств (см. раздел "Смена Сервера администрирования для клиентских устройств" на стр. [1029](#));
- удаление виртуальных Серверов администрирования (см. раздел "Удаление виртуального Сервера администрирования" на стр. [1030](#)).

В этом разделе

Создание виртуального Сервера администрирования	1025
Включение и выключение виртуального Сервера администрирования	1026
Назначение администратора виртуального Сервера администрирования	1027
Смена Сервера администрирования для клиентских устройств	1029
Удаление виртуального Сервера администрирования	1030

Создание виртуального Сервера администрирования

Можно создать виртуальные Серверы администрирования и добавить их в группы администрирования.

► *Чтобы создать и добавить виртуальный Сервер администрирования:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. Выберите группу администрирования, в которую вы хотите добавить виртуальный Сервер администрирования.
Виртуальный Сервер администрирования будет управлять устройствами из выбранной группы (включая подгруппы).
4. В меню выберите пункт **Новый виртуальный Сервер администрирования**.
5. На открывшейся странице задайте свойства нового виртуального Сервера администрирования:

- **Имя виртуального Сервера администрирования.**
- **Адрес подключения Сервера администрирования**

Вы можете указать имя или IP-адрес Сервера администрирования.

- Из списка пользователей выберите администратора виртуального Сервера администрирования. Существующую учетную запись при необходимости можно изменить перед тем, как назначить ей роль администратора; можно также создать новую учетную запись.
- Нажмите на кнопку **Сохранить**.

Новый виртуальный Сервер администрирования создан, добавлен в группу администрирования и отображается на вкладке **Серверы администрирования**.

Если вы подключены к главному Серверу администрирования в Kaspersky Security Center Web Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- Измените существующую установку Kaspersky Security Center Web Console, добавив подчиненный Сервер в список доверенных Серверов администрирования. После этого вы сможете подключиться к виртуальному Серверу администрирования в Kaspersky Security Center Web Console.
- Используйте Kaspersky Security Center Web Console, чтобы напрямую подключиться к подчиненному Серверу администрирования (см. раздел "Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования" см. стр. [1020](#)), на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center Web Console.
- Используйте Консоль администрирования на основе MMC для прямого подключения к виртуальному Серверу.

Включение и выключение виртуального Сервера администрирования

Когда вы создаете виртуальный Сервер администрирования, он по умолчанию включается. Вы можете выключить или снова включить его в любое время. Выключение или включение виртуального Сервера администрирования равносильно выключению или включению физического Сервера администрирования.

► *Чтобы включить или выключить виртуальный Сервер администрирования:*

- В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
- На открывшейся странице перейдите на вкладку **Серверы администрирования**.
- Выберите виртуальный Сервер администрирования, который вы хотите включить или выключить.
- В меню нажмите на кнопку **Подключить / отключить виртуальный Сервер администрирования**.

Состояние виртуального Сервера администрирования изменяется на включено или выключено в зависимости от его предыдущего состояния. Обновленное состояние отображается рядом с именем Сервера администрирования.

См. также:

Удаление виртуального Сервера администрирования [1030](#)

Назначение администратора виртуального Сервера администрирования

Если вы используете в своей организации виртуальные Серверы администрирования, вам может потребоваться назначить отдельного администратора для каждого виртуального Сервера администрирования. Например, это может быть полезно, когда вы создаете виртуальные Серверы администрирования для управления отдельными офисами или отделами вашей организации или если вы являетесь поставщиком услуг (MSP) и управляете своими тенантами с помощью виртуальных Серверов администрирования.

При создании виртуального Сервера администрирования он наследует список пользователей и все права пользователей главного Сервера администрирования. Если пользователь имеет права доступа к главному Серверу, этот пользователь также имеет права доступа к виртуальному Серверу. После создания вы самостоятельно настраиваете права доступа к Серверам. Если вы хотите назначить администратора только для виртуального Сервера администрирования, убедитесь, что у администратора нет прав доступа на главном Сервере администрирования.

Вы назначаете администратора виртуального Сервера администрирования, предоставляя права доступа администратору к виртуальному Серверу администрирования. Вы можете предоставить требуемые права доступа одним из следующих способов:

- Настройте права доступа для администратора вручную.
- Назначьте одну или несколько пользовательских ролей администратору.

Чтобы войти в Kaspersky Security Center Web Console (см. раздел "Вход в приложение Kaspersky Security Center Web Console и выход из него" на стр. [1006](#)), администратор виртуального Сервера администрирования указывает имя виртуального Сервера администрирования, имя пользователя и пароль. Kaspersky Security Center Web Console выполняет аутентификацию администратора и открывает виртуальный Сервер администрирования, к которому у администратора есть права доступа. Администратор не может переключаться между Серверами администрирования.

Предварительные требования

Убедитесь, что выполнены следующие условия:

- Виртуальный Сервер администрирования создан (см. раздел "Создание виртуального Сервера администрирования" на стр. [1025](#)).
- На главном Сервере администрирования у вас создана учетная запись для администратора, которого вы хотите назначить для виртуального Сервера администрирования.
- У вас есть право **Изменение списков управления доступом объектов** (см. раздел "**Настройка прав доступа к функциям приложения Управление доступом на основе ролей**" см. стр. [1275](#)) в функциональной области **Общие функции** → **Права пользователей**.

Настройка прав доступа вручную

► *Чтобы назначить администратора виртуального Сервера администрирования:*

1. В главном меню переключитесь на требуемый виртуальный Сервер администрирования:

- a. Нажмите на значок шеврона () справа от текущего имени Сервера администрирования.
 - b. Выберите требуемый Сервер администрирования.
2. В главном меню нажмите на значок параметров () рядом с именем Сервера администрирования.
Откроется окно свойств Сервера администрирования.
 3. На вкладке **Права доступа** нажмите на кнопку **Добавить**.
Откроется единый список пользователей главного Сервера администрирования и текущего виртуального Сервера администрирования.
 4. В списке пользователей выберите учетную запись администратора, которого вы хотите назначить для виртуального Сервера администрирования, и нажмите на кнопку **ОК**.
Приложение добавляет выбранного пользователя в список пользователей на вкладку **Права доступа**.
 5. Установите флажок рядом с добавленной учетной записью и нажмите на кнопку **Права доступа**.
 6. Настройте права администратора на виртуальном Сервере администрирования.
Для успешной аутентификации администратор должен иметь следующие права:
 - право **Чтение** в функциональной области **Общие функции** → **Базовая функциональность**.
 - право **Чтение** в функциональной области **Общие функции** → **Виртуальные Серверы администрирования**.

Приложение сохраняет измененные права пользователя в учетной записи администратора.

Настройка прав доступа с помощью назначения пользовательских ролей

Также вы можете предоставить права доступа администратору виртуального Сервера администрирования через пользовательскую роль. Например, это может быть полезно, если вы хотите назначить несколько администраторов на один и тот же виртуальный Сервер администрирования. В этом случае вы можете назначить учетным записям администраторов одну или несколько пользовательских ролей вместо того, чтобы настраивать одни и те же права для нескольких администраторов.

► *Чтобы назначить администратора виртуального Сервера администрирования, назначив ему пользовательские роли:*

1. На главном Сервере администрирования создайте пользовательскую роль (см. раздел "Создание роли пользователя" см. стр. [1316](#)) и укажите все необходимые права доступа, которыми должен обладать администратор на виртуальном Сервере администрирования. Вы можете создать несколько ролей, например, если хотите разделить доступ к разным функциональным областям.
2. В главном меню переключитесь на требуемый виртуальный Сервер администрирования:
 - a. Нажмите на значок шеврона () справа от текущего имени Сервера администрирования.
 - b. Выберите требуемый Сервер администрирования.
3. Назначьте новую роль или несколько ролей учетной записи администратора.

Приложение назначает роль учетной записи администратора.

Настройка прав доступа на уровне объекта

В дополнение к назначению прав доступа на уровне функциональной области (см. раздел "Права доступа к функциям приложения" на стр. [1276](#)), вы можете настроить доступ к определенным объектам (см. раздел "Назначение прав доступа к набору объектов" см. стр. [1305](#)) на виртуальном Сервере администрирования, например, к определенной группе администрирования или задаче. Для этого переключитесь на виртуальный Сервер администрирования, а затем настройте права доступа в свойствах объекта.

См. также:

Удаление виртуального Сервера администрирования[1030](#)

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи **Смена Сервера администрирования**. После завершения задачи выбранные клиентские устройства будут под управлением указанного Сервера администрирования.

► *Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center выберите тип задачи **Смена Сервера администрирования**.
4. Укажите имя задачи, которую вы создаете.
Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\":|).
5. Выберите устройства, которым будет назначена задача.
6. Выберите Сервер администрирования, который вы хотите использовать для управления выбранными устройствами.
7. Задайте параметры учетной записи:
 - **Учетная запись по умолчанию**
Задача будет запускаться под той же учетной записью, под которой была установлено и запущено приложение, выполняющее эту задачу.
По умолчанию выбран этот вариант.
 - **Задать учетную запись**
Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.
 - **Учетная запись**
Учетная запись, от имени которой будет запускаться задача.
 - **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

8. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
9. Нажмите на кнопку **Готово**.
Задача будет создана и отобразится в списке задач.
10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
11. В окне свойств задачи укажите общие параметры задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)) в соответствии с вашими требованиями.
12. Нажмите на кнопку **Сохранить**.
Задача создана и настроена.
13. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Если Сервер администрирования поддерживает управление шифрованием и защитой данных, то при создании задачи *Смена Сервера администрирования* отображается предупреждение. Предупреждение содержит информацию о том, что при наличии на устройствах зашифрованных данных после переключения устройств под управлением другого Сервера пользователям будет предоставлен доступ только к тем зашифрованным данным, с которыми они работали ранее. В остальных случаях доступ к зашифрованным данным предоставлен не будет. Подробное описание сценариев, в которых доступ к зашифрованным данным не будет предоставлен, приведено в справке Kaspersky Endpoint Security для Windows.

См. также:

Управление виртуальными Серверами администрирования.....	1025
Сценарий: настройка защиты сети.....	403

Удаление виртуального Сервера администрирования

При удалении виртуального Сервера администрирования все объекты, созданные на Сервере администрирования, включая политики и задачи, также будут удалены. Управляемые устройства из групп администрирования, которыми управлял виртуальный Сервер администрирования, будут удалены из групп администрирования. Чтобы вернуть устройства под управление Kaspersky Security Center, выполните опрос сети, а затем переместите найденные устройства из группы Нераспределенные устройства в группы администрирования.

► Чтобы удалить виртуальный Сервер администрирования:

1. В главном меню нажмите на значок параметров () рядом с именем Сервера администрирования.
 2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
 3. Выберите виртуальный Сервер администрирования, который вы хотите удалить.
 4. В строке меню нажмите на кнопку **Удалить**.
- Виртуальный Сервер администрирования удален.

См. также:

Включение и выключение виртуального Сервера администрирования.....[1026](#)

Включение защиты учетной записи от несанкционированного изменения

Вы можете дополнительно включить защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, изменение параметров учетной записи пользователя требует авторизации пользователя с правами на изменение.

► Чтобы включить или выключить защиту учетной записи от несанкционированного изменения:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на учетную запись внутреннего пользователя, для которой вы хотите настроить защиту учетной записи от несанкционированного изменения.
3. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.
4. На вкладке **Защита учетной записи** выберите параметр **Запросить аутентификацию для проверки разрешения на изменение учетных записей пользователей**, если вы хотите запрашивать учетные данные каждый раз при изменении параметров учетной записи. В противном случае выберите **Разрешить пользователям изменять эту учетную запись без дополнительной аутентификации**.
5. Нажмите на кнопку **Сохранить**.

Для учетной записи пользователя включена защита от несанкционированного изменения.

Двухэтапная проверка

В этом разделе описывается использование двухэтапной проверки для снижения риска несанкционированного доступа к Kaspersky Security Center Web Console.

В этом разделе

Сценарий: настройка двухэтапной проверки для всех пользователей	1032
О двухэтапной проверке	1035
Включение двухэтапной проверки для вашей учетной записи	1036
Включение обязательной двухэтапной проверки для всех пользователей	1037
Выключение двухэтапной проверки для учетной записи пользователя	1038
Выключение обязательной двухэтапной проверки для всех пользователей	1039
Исключение учетных записей из двухэтапной проверки.	1039
Генерация нового секретного ключа	1040
Изменение имени издателя кода безопасности	1041
Настройка двухэтапной проверки для вашей учетной записи	1041

Сценарий: настройка двухэтапной проверки для всех пользователей

В этом сценарии описывается, как включить двухэтапную проверку для всех пользователей и как исключить учетные записи пользователей из двухэтапной проверки. Если вы не включили двухэтапную проверку для своей учетной записи, прежде чем включить ее для других пользователей, приложение сначала откроет окно включения двухэтапной проверки для вашей учетной записи. В этом сценарии также описано, как включить двухэтапную проверку для вашей учетной записи.

Если вы включили двухэтапную проверку для своей учетной записи, вы можете перейти к включению двухэтапной проверки для всех пользователей.

Предварительные требования

Прежде чем начать:

- Убедитесь, что ваша учетная запись имеет право Изменение списков управления доступом объектов в функциональной области **Общий функционал: Права пользователей** для изменения параметров безопасности учетных записей других пользователей.
- Убедитесь, что другие пользователи Сервера администрирования установили на свои устройства приложение для аутентификации.

Этапы

Включение двухэтапной проверки для всех пользователей состоит из следующих этапов:

а. Установка приложения для аутентификации на устройство

Вы можете установить любое приложение проверки подлинности, которое поддерживает алгоритм формирования одноразового пароля на основе времени (TOTP), такие как:

- Google Authenticator.
- Microsoft Authenticator.

- Bitrix24 OTP.
- Яндекс ключ.
- Avapost Authenticator.
- Aladdin 2FA.

Чтобы проверить, поддерживает ли Kaspersky Security Center приложение для аутентификации, которое вы хотите использовать, включите двухфакторную проверку для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением для аутентификации. В случае успеха Kaspersky Security Center поддерживает выбранное приложение проверки подлинности.

Категорически не рекомендуется устанавливать приложение для аутентификации на том же устройстве, с которого выполняется подключение к Серверу администрирования.

b. Синхронизация времени приложения для аутентификации и время устройства, на котором установлен Сервер администрирования

Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени. Иначе возможны сбои при аутентификации и активации двухэтапной проверки.

c. Включение двухэтапной проверки и получение секретного ключа для своей учетной записи

Инструкции:

- Для Консоли администрирования на основе MMC: Включение двухэтапной проверки для вашей учетной записи.
- Для Kaspersky Security Center Web Console: Включение двухэтапной проверки для вашей учетной записи (на стр. [1036](#)).

После включения двухэтапной проверки для своей учетной записи вы можете включить двухэтапную проверку для всех пользователей.

d. Включение двухэтапной проверки для всех пользователей

Пользователи с включенной двухэтапной проверкой должны использовать ее для входа на Сервер администрирования.

Инструкции:

- Для Консоли администрирования на основе MMC: Включение двухэтапной проверки для всех пользователей.
- Для Kaspersky Security Center Web Console: Включение двухэтапной проверки для всех пользователей (см. раздел "Включение обязательной двухэтапной проверки для всех пользователей" на стр. [1037](#)).

e. Изменение имени издателя кода безопасности

Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности для лучшего распознавания разных Серверов администрирования.

Инструкции:

- Для Консоли администрирования на основе MMC: Изменение имени издателя кода безопасности.
- Для Kaspersky Security Center Web Console: Изменение имени издателя кода безопасности (на стр. [1041](#)).

f. Исключение учетных записей пользователей, для которых не требуется включать двухэтапную проверку

При необходимости исключите учетные записи пользователей из двухэтапной проверки. Пользователям с исключенными учетными записями не нужно использовать двухэтапную проверку для входа на Сервер администрирования.

Инструкции:

- Для Консоли администрирования на основе MMC: Исключение учетных записей из двухэтапной проверки.
- Для Kaspersky Security Center Web Console: Исключение учетных записей из двухэтапной проверки (см. раздел "Исключение учетных записей из двухэтапной проверки." на стр. [1039](#)).

g. Настройка двухэтапной проверки для вашей учетной записи

Если пользователи не исключены из двухэтапной проверки и двухэтапная проверка еще не настроена для их учетных записей, им необходимо настроить ее в окне, открываемом при входе в Kaspersky Security Center. Иначе они не смогут получить доступ к Серверу администрирования в соответствии со своими правами.

Инструкции:

- Для Консоли администрирования на основе MMC: Настройка двухэтапной проверки для вашей учетной записи.
- Для Kaspersky Security Center Web Console: Настройка двухэтапной проверки для вашей учетной записи (на стр. [1041](#)).

Результаты

После выполнения этого сценария:

- Двухэтапная проверка для вашей учетной записи включена.
- Двухэтапная проверка включена для всех учетных записей пользователей Сервера администрирования, кроме исключенных учетных записей пользователей.

См. также:

О двухэтапной проверке	1035
Включение двухэтапной проверки для вашей учетной записи	1036
Включение обязательной двухэтапной проверки для всех пользователей	1037
Выключение двухэтапной проверки для учетной записи пользователя	1038
Выключение обязательной двухэтапной проверки для всех пользователей	1039
Исключение учетных записей из двухэтапной проверки.	1039

О двухэтапной проверке

Если для учетной записи включена двухэтапная проверка, для входа в Консоль администрирования или Kaspersky Security Center Web Console, помимо имени пользователя и пароля, требуется одноразовый код безопасности. Если доменная аутентификация включена (см. раздел "Настройка доменной аутентификации с использованием протоколов NTLM и Kerberos" на стр. [1015](#)), пользователю достаточно ввести одноразовый код безопасности.

Чтобы использовать двухэтапную проверку, установите на мобильное устройство или компьютер приложение для аутентификации, которое генерирует одноразовые коды безопасности. Вы можете использовать любое приложение проверки подлинности, которое поддерживает алгоритм формирования одноразового пароля на основе времени (TOTP), такие как:

- Google Authenticator.
- Microsoft Authenticator.
- Bitrix24 OTP.
- Яндекс ключ.
- Avanpost Authenticator.
- Aladdin 2FA.

Чтобы проверить, поддерживает ли Kaspersky Security Center приложение для аутентификации, которое вы хотите использовать, включите двухфакторную проверку для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением для аутентификации. В случае успеха Kaspersky Security Center поддерживает выбранное приложение проверки подлинности.

Настоятельно рекомендуется сохранить секретный ключ или QR-код и хранить его в надежном месте. Это поможет вам восстановить доступ к Kaspersky Security Center Web Console в случае потери доступа к мобильному устройству.

Чтобы обезопасить использование Kaspersky Security Center, вы можете включить двухэтапную проверку для своей учетной записи и включить двухэтапную проверку для всех пользователей.

Вы можете исключить (см. раздел "Исключение учетных записей из двухэтапной проверки." на стр. [1039](#)) учетные записи из двухэтапной проверки. Это может быть необходимо для служебных учетных записей, которые не могут получить защитный код для аутентификации.

Правила и ограничения

Чтобы иметь возможность активировать двухэтапную проверку для всех пользователей и деактивировать двухэтапную проверку для отдельных пользователей:

- Убедитесь, что вашей учетной записи есть право Изменение списков управления доступом объектов (см. раздел "Права доступа к функциям приложения" на стр. [1276](#)) в функциональной области **Общий функционал: Права пользователей**.

- Включите двухэтапную проверку для вашей учетной записи.

Чтобы выключить двухэтапную проверку для всех пользователей:

- Убедитесь, что вашей учетной записи есть право Изменение списков управления доступом объектов (см. раздел "Права доступа к функциям приложения" на стр. [1276](#)) в функциональной области **Общий функционал: Права пользователей**.
- Войдите в Kaspersky Security Center Web Console с помощью двухэтапной проверки.

Если для учетной записи на Сервере администрирования Kaspersky Security Center версии 13 или выше включена двухэтапная проверка, то пользователь не сможет войти в приложение Kaspersky Security Center Web Console версий 12, 12.1 или 12.2.

Перевыпуск секретного ключа

Любой пользователь может повторно выпустить секретный ключ, используемый для двухэтапной проверки. Когда пользователь входит на Сервер администрирования с перевыпущенным секретным ключом, новый секретный ключ сохраняется для учетной записи пользователя. Если пользователь неправильно вводит новый секретный ключ, новый секретный ключ не сохраняется, а текущий секретный ключ остается действительным.

Код безопасности имеет идентификатор, называемый также *имя издателя*. Имя издателя кода безопасности используется в качестве идентификатора Сервера администрирования в приложении для аутентификации. Имя издателя кода безопасности имеет значение по умолчанию, такое же, как имя Сервера администрирования. Вы можете изменить имя издателя кода безопасности. Если вы изменили имя издателя кода безопасности, необходимо выпустить новый секретный ключ и передать его приложению для аутентификации.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей	1032
Исключение учетных записей из двухэтапной проверки.	1039

Включение двухэтапной проверки для вашей учетной записи

Вы можете включить двухэтапную проверку только для своей учетной записи.

Перед тем как включить двухэтапную проверку для своей учетной записи, убедитесь, что на мобильном устройстве установлено приложение для аутентификации. Убедитесь, что время, установленное в приложении для аутентификации, синхронизировано со временем устройства, на котором установлен Сервер администрирования.

► Чтобы включить двухэтапную проверку для учетной записи пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на имя вашей учетной записи.

3. В открывшемся окне свойств пользователя выберите вкладку **Дополнительные настройки безопасности**.
4. На вкладке **Дополнительные настройки безопасности**:
 - a. Выберите параметр **Запрашивать только имя пользователя, пароль и код безопасности (двухэтапная проверка)**. Нажмите на кнопку **Сохранить**.
 - b. В открывшемся окне двухэтапной проверки нажмите **Узнайте, как настроить двухэтапную проверку**.
 Введите секретный ключ в приложении для аутентификации или нажмите **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.
 - c. В окне двухэтапной проверки укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **Проверить и применить**.
5. Нажмите на кнопку **Сохранить**.

Двухэтапная проверка для вашей учетной записи включена.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей	1032
Включение обязательной двухэтапной проверки для всех пользователей	1037

Включение обязательной двухэтапной проверки для всех пользователей

Вы можете включить двухэтапную проверку для всех пользователей Сервера администрирования, если у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общий функционал: Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки.

► Чтобы включить двухэтапную проверку для всех пользователей:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
 Откроется окно свойств Сервера администрирования.
2. На вкладке **Дополнительные настройки безопасности** окна свойств включите **двухэтапную проверку для всех пользователей**.
3. Если вы не включили двухэтапную проверку для своей учетной записи (см. раздел "Включение двухэтапной проверки для вашей учетной записи" на стр. [1036](#)), приложение откроет окно включения двухэтапной проверки для вашей учетной записи.
 - a. В открывшемся окне двухэтапной проверки нажмите **Узнайте, как настроить двухэтапную проверку**.

- b. Введите секретный ключ вручную в приложении для аутентификации или нажмите **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.
- c. В окне двухэтапной проверки укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **Проверить и применить**.

Двухэтапная проверка для всех пользователей включена. Пользователям Сервера администрирования, включая пользователей, которые были добавлены после включения двухэтапной проверки для всех пользователей, необходимо настроить двухэтапную проверку для своих учетных записей, за исключением пользователей, учетные записи которых исключены (см. раздел "Исключение учетных записей из двухэтапной проверки." на стр. [1039](#)) из двухэтапной проверки.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей	1032
Включение двухэтапной проверки для вашей учетной записи	1036
Исключение учетных записей из двухэтапной проверки.	1039

Выключение двухэтапной проверки для учетной записи пользователя

Вы можете выключить двухэтапную проверку для своей учетной записи, а также для учетной записи любого другого пользователя.

Вы можете выключить двухэтапную проверку для другой учетной записи пользователя, если у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общий функционал: Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки.

► Чтобы выключить двухэтапную проверку для учетной записи пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на учетную запись внутреннего пользователя, для которой вы хотите выключить двухэтапную проверку. Это может быть ваша собственная учетная запись или учетная запись любого другого пользователя.
3. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.
4. На вкладке **Защита учетной записи** выберите параметр **Запрашивать только имя пользователя и пароль**, если вы хотите выключить двухэтапную проверку для учетной записи пользователя.
5. Нажмите на кнопку **Сохранить**.

Двухэтапная проверка для вашей учетной записи выключена.

Если вы хотите восстановить доступ пользователя, который не может войти в Kaspersky Security Center Web Console с помощью двухэтапной проверки, выключите двухэтапную проверку для этой учетной записи пользователя и выберите параметр **Запрашивать только имя пользователя и пароль** как описано выше. После этого войдите в Kaspersky Security Center Web Console под учетной записью пользователя, для которого вы выключили двухэтапную проверку и снова включите проверку (см. раздел "Включение двухэтапной проверки для вашей учетной записи" на стр. [1036](#)).

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей[1032](#)

Выключение обязательной двухэтапной проверки для всех пользователей

Вы можете выключить обязательную двухэтапную проверку для всех пользователей, если двухэтапная проверка включена для вашей учетной записи и у вашей учетной записи есть право Изменение списков ACL объекта в разделе **Общий функционал: Права пользователей**. Если двухэтапная проверка не включена для вашей учетной записи, вам нужно включить двухэтапную проверку для своей учетной (см. раздел "Включение двухэтапной проверки для вашей учетной записи" на стр. [1036](#)) записи, прежде чем выключить ее для всех пользователей.

► *Чтобы выключить двухэтапную проверку для всех пользователей:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
2. На вкладке **Дополнительные настройки безопасности** окна свойств выключите переключатель **двухэтапной проверки для всех пользователей**.
3. Введите учетные данные своей учетной записи в окне аутентификации.

Двухэтапная проверка для всех пользователей выключена. Выключение двухэтапной проверки для всех пользователей не применяется к конкретным учетным записям, для которых двухэтапная проверка ранее была включена отдельно.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей[1032](#)

Включение двухэтапной проверки для вашей учетной записи[1036](#)

Исключение учетных записей из двухэтапной проверки.

Вы можете исключить учетные записи пользователей из двухэтапной проверки, если у вас есть право Изменение списков ACL объекта в функциональной области **Общий функционал: Права пользователей**.

Если учетная запись пользователя исключена из списка двухэтапной проверки для всех пользователей, этому пользователю не нужно использовать двухэтапную проверку.

Исключение учетных записей из двухэтапной проверки может быть необходимо для служебных учетных записей, которые не могут передать код безопасности во время аутентификации.

► Если вы хотите исключить некоторые учетные записи пользователей из двухэтапной проверки:

1. Вам нужно выполнить опрос контроллера домена Microsoft Active Directory (см. раздел "Опрос контроллеров домена" см. стр. [1117](#)), чтобы обновить список пользователей Сервера администрирования, если вы хотите исключить учетные записи Active Directory.
2. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
3. На вкладке **Дополнительные настройки безопасности** окна свойств в таблице исключений для двухэтапной проверки нажмите на кнопку **Добавить**.
4. В открывшемся окне:
 - a. Выберите учетную запись пользователя, которую вы хотите исключить.
 - b. Нажмите на кнопку **ОК**.

Выбранные учетные записи пользователей исключены из двухэтапной проверки.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей	1032
О двухэтапной проверке	1035

Генерация нового секретного ключа

Вы можете сгенерировать новый секретный ключ для двухэтапной проверки своей учетной записи, только если вы авторизованы с помощью двухэтапной проверки.

► Чтобы сгенерировать новый секретный ключ для учетной записи пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на учетную запись пользователя, для которой вы хотите сгенерировать новый секретный ключ для двухэтапной проверки.
3. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.
4. На вкладке **Защита учетной записи** перейдите по ссылке **Сгенерировать секретный ключ**.
5. В открывшемся окне двухэтапной проверки укажите новый ключ безопасности, сгенерированный приложением для аутентификации.

6. Нажмите на кнопку **Проверить и применить**.

Новый секретный ключ для пользователя создан.

Если вы потеряете мобильное устройство, можно установить приложение для аутентификации на другое мобильное устройство и сгенерировать новый секретный ключ для восстановления доступа к Kaspersky Security Center Web Console.

Изменение имени издателя кода безопасности

У вас может быть несколько идентификаторов (также их называют издателями) для разных Серверов администрирования. Вы можете изменить имя издателя кода безопасности, например, если Сервер администрирования уже использует аналогичное имя издателя кода безопасности для другого Сервера администрирования. По умолчанию имя издателя кода безопасности совпадает с именем Сервера администрирования.

После изменения имени издателя кода безопасности необходимо повторно выпустить новый секретный ключ и передать его приложению для аутентификации.

- Чтобы указать новое имя издателя кода безопасности:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
2. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.
3. На вкладке **Защита учетной записи**, перейдите по ссылке **Редактировать**.
Откроется раздел **Изменить издателя кода безопасности**.
4. Укажите новое имя издателя кода безопасности.
5. Нажмите на кнопку **ОК**.

Для Сервера администрирования указано новое имя издателя кода безопасности.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей[1032](#)

Настройка двухэтапной проверки для вашей учетной записи

При первом входе в Kaspersky Security Center после включения двухэтапной проверки открывается окно настройки двухэтапной проверки для вашей учетной записи.

Перед тем как настроить двухэтапную проверку для своей учетной записи, убедитесь, что на мобильном устройстве установлено приложение для аутентификации. Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени.

► *Чтобы настроить двухэтапную проверку для учетной записи:*

1. Сгенерируйте одноразовый код безопасности с помощью приложения для аутентификации на мобильном устройстве. Для этого выполните одно из следующих действий:
 - Введите секретный ключ в приложение для аутентификации вручную.
 - Нажмите на кнопку **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации.

Код безопасности отобразится на мобильном устройстве.

2. В окне настройки двухэтапной проверки укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **Проверить и применить**.

Двухэтапная проверка для вашей учетной записи настроена. У вас есть доступ к Серверу администрирования в соответствии со своими правами.

Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование данных позволяет переносить Сервер администрирования с одного устройства на другое без потерь информации. С помощью резервного копирования вы можете восстанавливать данные при переносе информационной базы Сервера администрирования на другое устройство или при переходе на более позднюю версию Kaspersky Security Center.

Обратите внимание, что резервные копии установленных плагинов управления не сохраняются. После восстановления данных Сервера администрирования из резервной копии необходимо загрузить и переустановить плагины управляемых программ.

Прежде чем создавать резервную копию данных Сервера администрирования, проверьте, добавлен ли виртуальный Сервер администрирования в группу администрирования. Если виртуальный Сервер администрирования добавляется перед резервным копированием, убедитесь, что этому виртуальному Серверу назначен администратор (см. раздел "Назначение администратора виртуального Сервера администрирования" см. стр. [1027](#)). Вы не можете предоставить права администратора к виртуальному Серверу администрирования после резервного копирования. Обратите внимание, если учетные данные администратора утеряны, вы не сможете назначить нового администратора виртуальному Серверу администратора.

Вы можете создать резервную копию данных Сервера администрирования одним из следующих способов:

- Создать и запустить задачу резервного копирования данных через Консоль администрирования.
- Запустить утилиту kbackup на устройстве, где установлен Сервер администрирования. Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке приложения.

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- база данных Сервера администрирования (политики, задачи, параметры приложений, сохраненные на Сервере администрирования события);
- конфигурационная информация о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки;
- сертификат Сервера администрирования.

Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup.

Создание задачи резервного копирования данных

Задача резервного копирования является задачей Сервера администрирования и создается мастером первоначальной настройки. Если задача резервного копирования, созданная мастером первоначальной настройки, была удалена, вы можете создать ее вручную.

► *Чтобы создать задачу резервного копирования данных Сервера администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи.
3. В окне мастера **Параметры новой задачи** выберите тип задачи **Резервное копирование данных Сервера администрирования**.
4. Следуйте дальнейшим шагам мастера.

Задачу **Резервное копирование данных Сервера администрирования** можно создать только в одном экземпляре. Если задача резервного копирования данных Сервера администрирования уже создана для Сервера администрирования, то она не отображается в окне выбора типа задачи мастера создания задачи резервного копирования.

► *Чтобы настроить задачу резервного копирования данных Сервера администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи** и выберите задачу **Резервное копирование данных Сервера администрирования**.
2. Нажмите на имя задачи **Резервное копирование данных Сервера администрирования**.
Откроется окно свойств задачи.
3. При необходимости укажите общие параметры задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)) в соответствии с вашими требованиями.
4. В разделе **Параметры приложения** укажите путь к папке для хранения резервных копий данных Сервера администрирования, установите защиту паролем резервного копирования и количество резервных копий, если это необходимо.

5. Нажмите на кнопку **Сохранить**, чтобы применить изменения.

Задача Резервное копирование данных Сервера администрирования настроена.

Перенос Сервера администрирования на другое устройство

Если вам нужно использовать Сервер администрирования на новом устройстве, вы можете перенести его одним из следующих способов:

- Переместить Сервер администрирования и сервер баз данных на новое устройство.
- Оставить сервер баз данных на старом устройстве и перенести на новое устройство только Сервер администрирования.

Чтобы перенести Сервер администрирования и сервер баз данных на новое устройство:

1. На предыдущем устройстве создайте резервную копию данных Сервера администрирования.

Для этого запустите задачу резервного копирования данных (см. раздел "Создание задачи резервного копирования данных" на стр. [1043](#)) с помощью Kaspersky Security Center Web Console или запустите утилиту kbackup.

Если вы используете SQL Server в качестве СУБД для Сервера администрирования, можно перенести данные с SQL Server на СУБД MySQL или MariaDB. Для создания резервной копии данных запустите утилиту kbackup в интерактивном режиме. Включите параметр **Перенос данных в формате MySQL/MariaDB** в окне **Параметры резервного копирования** мастера резервного копирования и восстановления данных. Kaspersky Security Center создаст резервную копию данных, совместимую с MySQL и MariaDB. После этого вы можете восстановить данные из резервной копии в MySQL или MariaDB. Также можно включить параметр **Перенести в формат Azure**, если вы хотите перенести данные из SQL Server в СУБД Azure SQL.

2. Выберите новое устройство, на которое будет установлен Сервер администрирования. Убедитесь, что аппаратное и программное обеспечение на выбранном устройстве соответствует требованиям (см. раздел "Аппаратные и программные требования Kaspersky Security Center Web Console" на стр. [976](#)) для Сервера администрирования, Kaspersky Security Center Web Console и Агента администрирования. Проверьте, что порты, используемые на Сервере администрирования (см. раздел "Порты, используемые приложением Kaspersky Security Center Web Console" на стр. [980](#)) доступны.
3. На новом устройстве установите СУБД, которую будет использовать Сервер администрирования. При выборе СУБД учитывайте количество устройств, которые обслуживает Сервер администрирования.
4. Запустите выборочную установку Сервера администрирования на новом устройстве.

5. Установите компоненты Сервера администрирования в ту же папку, где Сервер администрирования установлен на предыдущем устройстве. Нажмите на кнопку **Обзор**, чтобы указать путь к файлу.

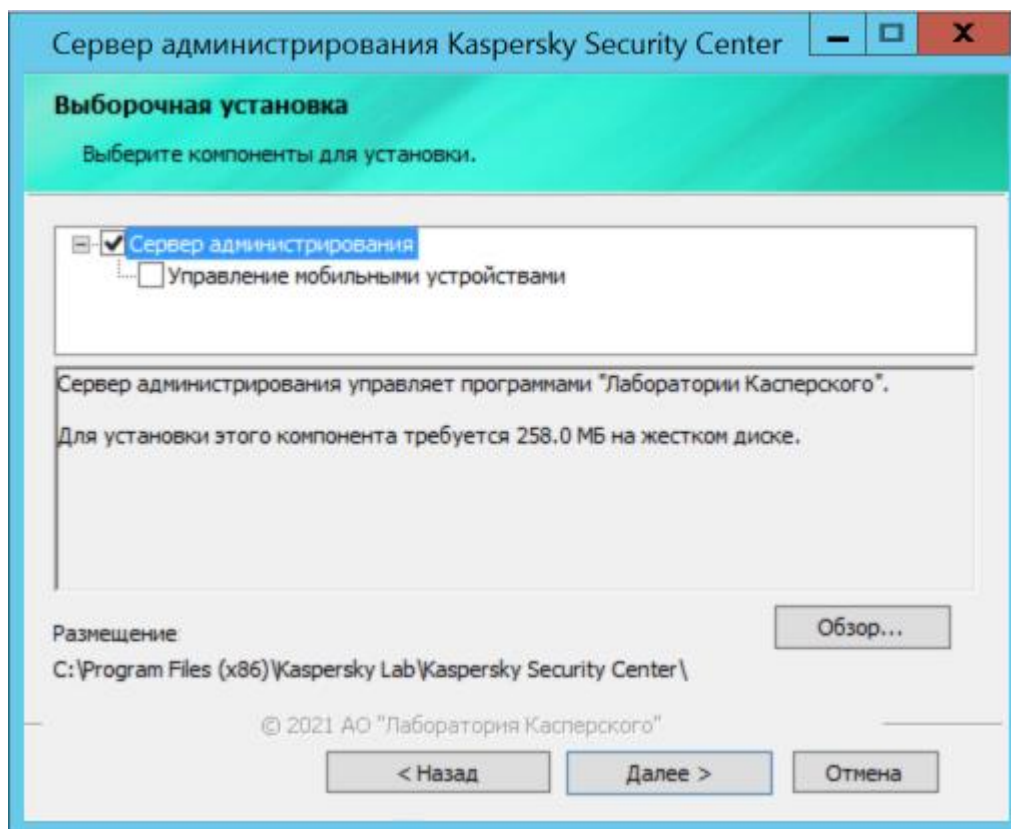


Рисунок 14. Окно выборочной установки

- Настройте параметры подключения к серверу базы данных.

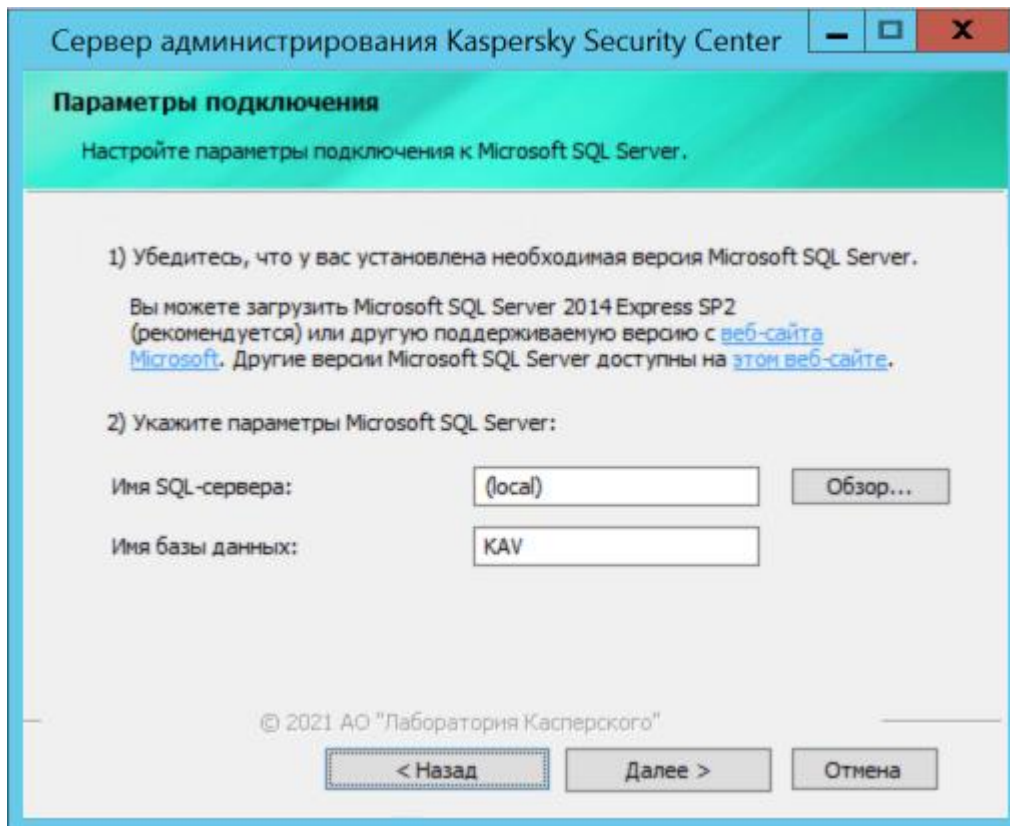


Рисунок 15. Окно параметров подключения

В зависимости от того, где вам нужно разместить сервер базы данных, выполните одно из следующих действий:

- Переместите сервер базы данных на новое устройство.
 - Оставьте сервер базы данных на предыдущем устройстве.
- После завершения установки восстановите данные Сервера администрирования на новом устройстве с помощью утилиты klbackup.

Если вы используете SQL Server в качестве СУБД на предыдущем и новом устройствах, обратите внимание, что версия SQL Server, установленная на новом устройстве, должна быть такой же или выше, чем версия SQL Server, установленная на предыдущем устройстве. Иначе вы не сможете восстановить данные Сервера администрирования на новом устройстве.

- Откройте Kaspersky Security Center Web Console и подключитесь к Серверу администрирования (см. раздел "Вход в приложение Kaspersky Security Center Web Console и выход из него" на стр. [1006](#)).
- Убедитесь, что все клиентские устройства подключены к Серверу администрирования.
- Удалите Сервер администрирования и сервер баз данных с предыдущего устройства.

Также можно использовать Консоль администрирования, чтобы перенести Сервер администрирования и сервер базы данных на другое устройство.

См. также:

Резервное копирование и восстановление данных Сервера администрирования.....[723](#)

Первоначальная настройка Kaspersky Security Center Web Console

В этом разделе описаны шаги, которые необходимо выполнить после установки Kaspersky Security Center Web Console для первоначальной настройки.

Мастер первоначальной настройки (Kaspersky Security Center Web Console)

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

Мастеру требуется доступ в интернет. Если Сервер администрирования не имеет доступа в интернет, рекомендуется выполнять все шаги мастера вручную через интерфейс Kaspersky Security Center Web Console.

Приложение Kaspersky Security Center позволяет настроить минимальный набор параметров, необходимых для построения централизованной системы управления, обеспечивающей защиту сети от угроз безопасности. Эта настройка выполняется в мастере первоначальной настройки. В процессе работы мастера вы можете внести в приложение следующие изменения:

- Добавить файлы ключей или ввести коды активации, которые можно автоматически распространять на устройства в группах администрирования.
- Настроить взаимодействие с Kaspersky Security Network (KSN). При разрешении использования KSN мастер включает службу прокси-сервера KSN, которая обеспечивает взаимодействие между KSN и устройствами.
- Настроить рассылку по электронной почте оповещений о событиях в работе Сервера администрирования и управляемых приложений (чтобы уведомление прошло успешно, на Сервере администрирования и на всех устройствах-получателях должна быть запущена служба сообщений Messenger).
- Сформировать политику защиты рабочих станций и серверов, а также задачи поиска вредоносного ПО, получения обновлений и резервного копирования данных для верхнего уровня иерархии управляемых устройств.

Мастер первоначальной настройки создает политики только для приложений, для которых еще нет созданных политик в папке **Управляемые устройства**. Мастер первоначальной настройки не создает задачи, если задачи с такими именами уже созданы для верхнего уровня иерархии управляемых устройств.

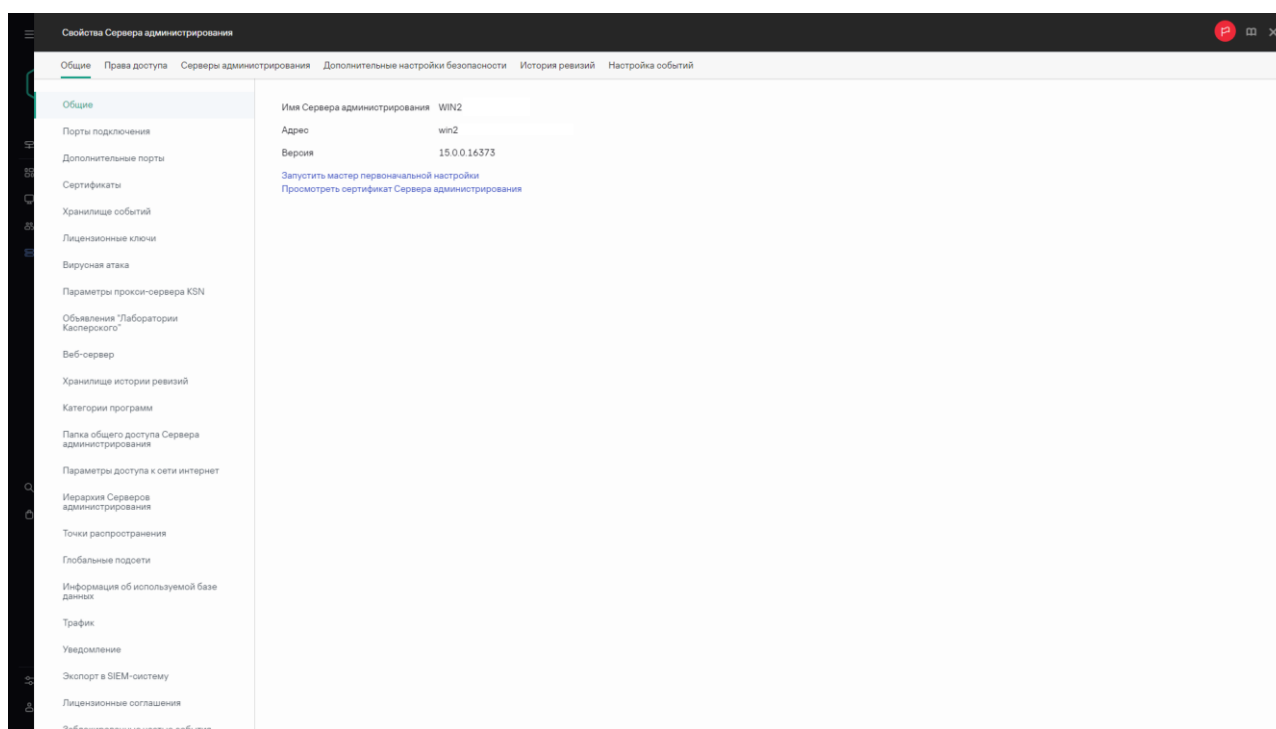
Приложение автоматически предлагает запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к Серверу. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

► Чтобы запустить мастер первоначальной настройки вручную:

1. В главном меню нажмите на значок параметров () рядом с именем Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Общие**.



3. Нажмите на кнопку **Запустить мастер первоначальной настройки**.

Мастер предложит произвести первоначальную настройку Сервера администрирования. Следуйте далее указаниям мастера. Для продолжения работы мастера нажмите на кнопку **Далее**.

См. также:

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985
Сценарий: развертывание приложений "Лаборатории Касперского"	1084
Сценарий: настройка защиты сети.....	403

В этом разделе

Шаг 1. Указание параметров подключения к интернету	1050
Шаг 2. Загрузка требуемых обновлений	1051
Шаг 3. Выбор активов для защиты	1051
Шаг 4. Выбор шифрования	1053
Шаг 5. Настройка установки плагинов для управляемых приложений	1054
Шаг 6. Установка выбранных плагинов	1056
Шаг 7. Загрузка дистрибутивов и создание инсталляционных пакетов	1056
Шаг 8. Настройка Kaspersky Security Network	1058
Шаг 9. Выбор способа активации приложения.....	1058
Шаг 10. Указание параметров управления обновлениями приложений сторонних производителей	1060
Шаг 11. Создание базовой конфигурации защиты сети	1061
Шаг 12. Настройка параметров отправки уведомлений по электронной почте	1062
Шаг 13. Выполнение опроса сети.....	1063
Шаг 14. Завершение работы мастера первоначальной настройки.....	1063

Шаг 1. Указание параметров подключения к интернету

Укажите параметры доступа Сервера администрирования к интернету. Доступ к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Kaspersky Security Center и управляемых приложений "Лаборатории Касперского".

Мастер первоначальной настройки

Шаг 1 Настройка мастера может занять около 15 минут.

Параметры подключения к интернету

Серверу администрирования требуется подключение к интернету для проверки текущих версий установленных плагинов и создания установочных пакетов.

☐ Прямое подключение

☒ Использовать прокси-сервер

Адрес

Номер порта

☒ Не использовать прокси-сервер для локальных адресов

☒ Аутентификация на прокси-сервере

Имя пользователя

Пароль

Включите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр включен, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

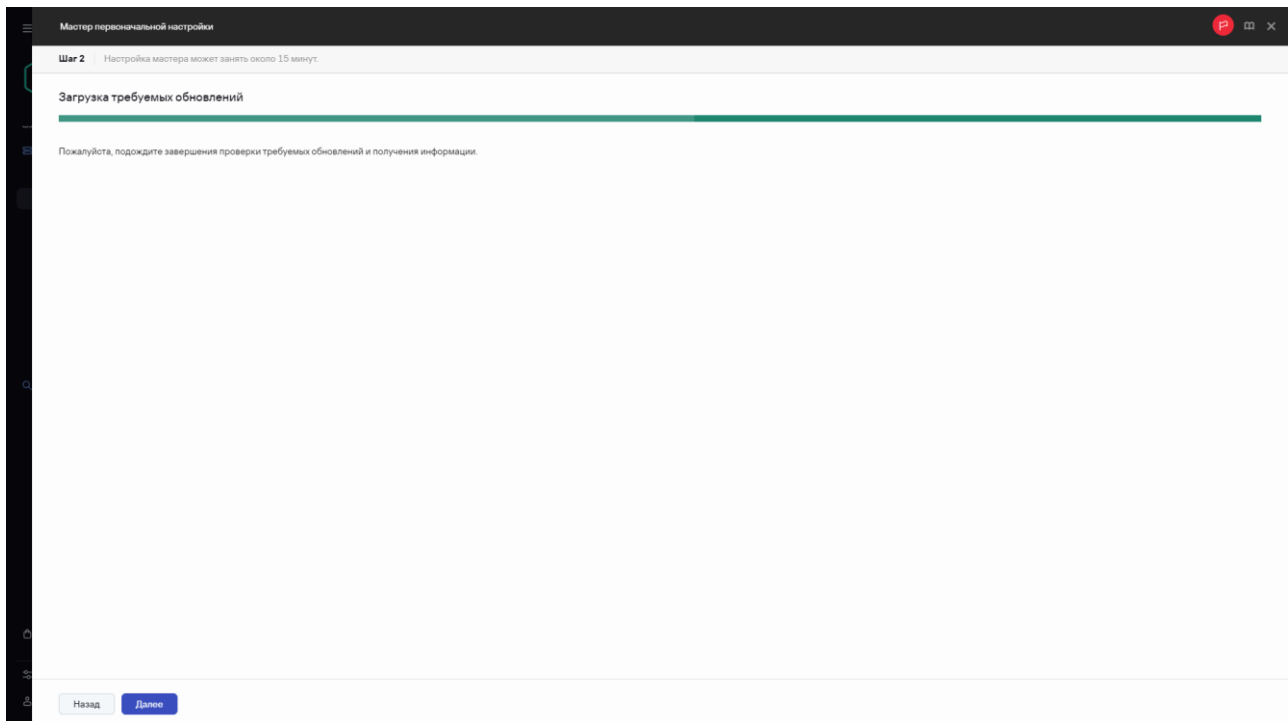
- **Адрес**
Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.
- **Номер порта**
Номер порта, по которому будет выполняться подключение Kaspersky Security Center к прокси-серверу.
- **Не использовать прокси-сервер для локальных адресов**
При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.
- **Аутентификация на прокси-сервере**
Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере. Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.
- **Имя пользователя**
Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.
- **Пароль**

Пароль пользователя, через учетную запись которого выполняется подключение к прокси-серверу.

Вы можете настроить доступ в интернет позднее без запуска мастера первоначальной настройки.

Шаг 2. Загрузка требуемых обновлений

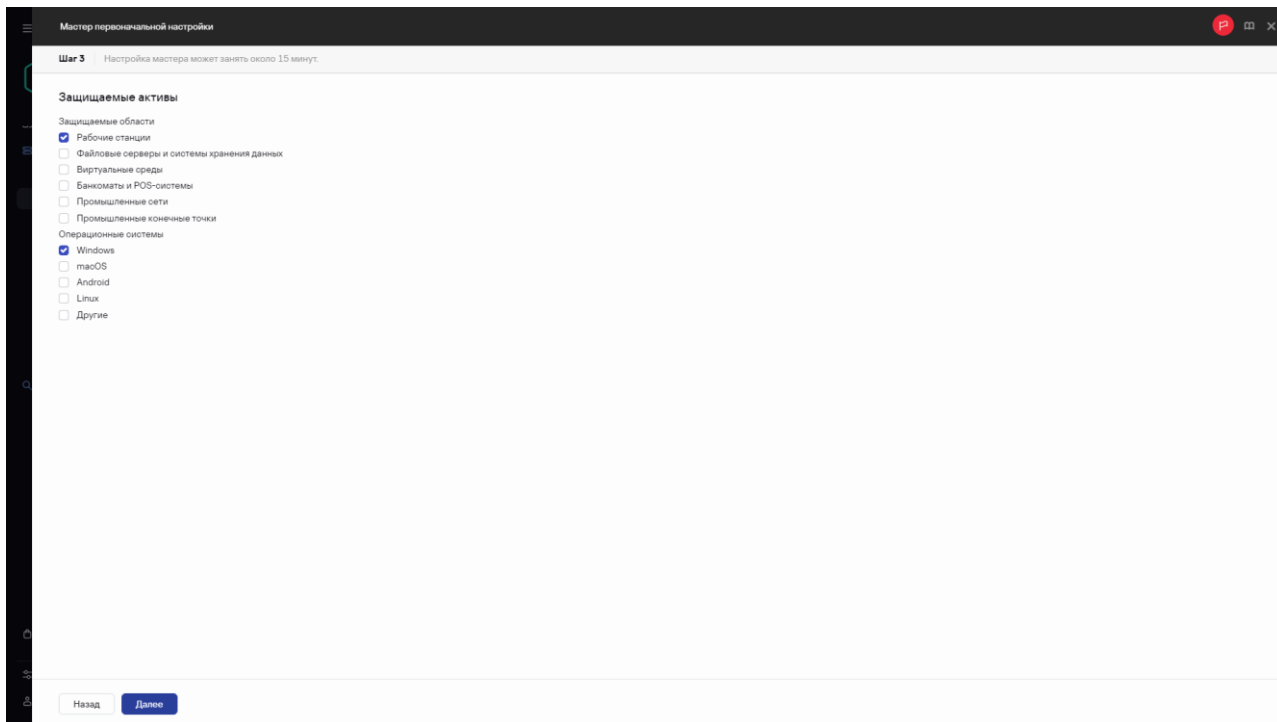
Необходимые обновления загружаются с серверов "Лаборатории Касперского" автоматически.



Шаг 3. Выбор активов для защиты

Выберите области защиты и операционные системы, которые используются в вашей сети. При выборе этих параметров вы указываете фильтры для плагинов управления приложениями и дистрибутивов на серверах

"Лаборатории Касперского", которые вы можете загрузить для установки на клиентские устройства в вашей сети.



Выберите следующие параметры:

- **Области**

Вы можете выбрать одну из следующих областей защиты:

- **Рабочие станции.** Выберите этот параметр, если вы хотите защитить рабочие станции в вашей сети. По умолчанию выбран параметр Рабочая станция.
- **Файловые серверы и системы хранения данных.** Выберите этот параметр, если вы хотите защитить файловые серверы в вашей сети.
- **Мобильные устройства.** Выберите этот параметр, если вы хотите защитить мобильные устройства, принадлежащие организации или сотрудникам организации. Если вы выбрали этот параметр, но не предоставили лицензию с возможностью Управление мобильными устройствами, отобразится сообщение о необходимости предоставить лицензию с возможностью Управление мобильными устройствами. Без этой лицензии использование возможностей Управления мобильными устройствами невозможно.
- **Виртуальные среды.** Выберите этот параметр, если вы хотите защитить виртуальные машины в вашей сети.
- **Анти-Спам.** Выберите этот параметр, если вы хотите защитить почтовые серверы вашей организации от спама, мошенничества и доставки вредоносных приложений.
- **Банкоматы и POS-системы.** Выберите этот параметр, если вы хотите защитить встроенные системы с операционной системой Windows, например банкоматы (АТМ).
- **Промышленные сети.** Выберите этот параметр, если вы хотите контролировать данные безопасности в промышленной сети и с конечных устройств сети, защищенных приложениями "Лаборатории Касперского".
- **Промышленные конечные точки.** Выберите этот параметр, если вы хотите

защитить отдельные узлы промышленной сети.

- **Операционные системы**

Вы можете выбрать одну из следующих платформ:

- Microsoft Windows
- macOS
- Android
- Linux
- Другое

Дополнительные сведения о поддерживаемых версиях операционных систем см. в разделе Аппаратные и программные требования Kaspersky Security Center Web Console (см. стр. [976](#)).

Можно выбрать инсталляционные пакеты приложений "Лаборатории Касперского" (см. раздел "Загрузка дистрибутивов для приложений "Лаборатории Касперского"" на стр. [1089](#)) из списка доступных инсталляционных пакетов позднее без запуска мастера первоначальной настройки. Для упрощения поиска необходимых инсталляционных пакетов вы можете фильтровать список доступных инсталляционных пакетов различным критериям.

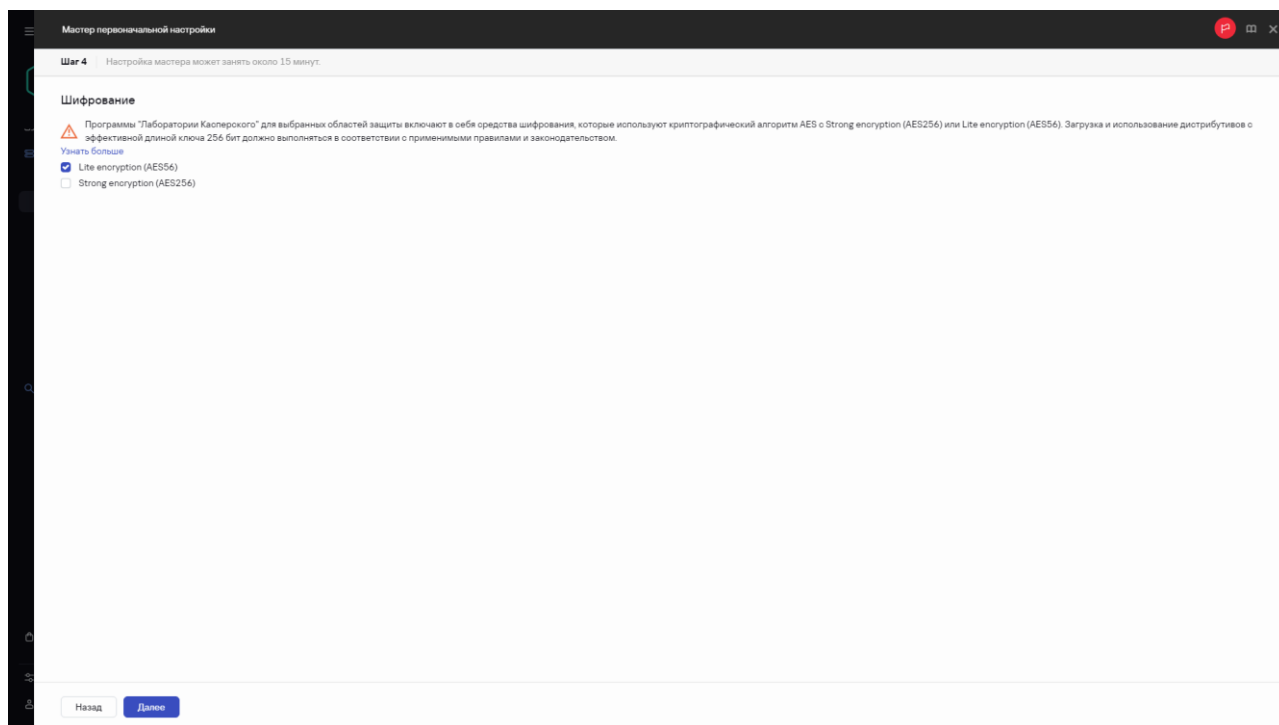
Шаг 4. Выбор шифрования

Окно **Шифрование** отображается, только если в качестве области защиты выбран вариант **Рабочие станции**.

Kaspersky Endpoint Security для Windows включает инструменты шифрования информации, хранящейся на клиентских устройствах в операционной системой Windows. Эти инструменты шифрования имеют расширенный стандарт шифрования (AES), реализованный с длиной ключа 256 бит или 56 бит.

Загрузка и использование дистрибутива с длиной ключа 256 бит должна выполняться в соответствии с действующими законами и правилами. Чтобы загрузить дистрибутив Kaspersky Endpoint Security для

Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.



В окне **Шифрование** выберите один из следующих типов шифрования:

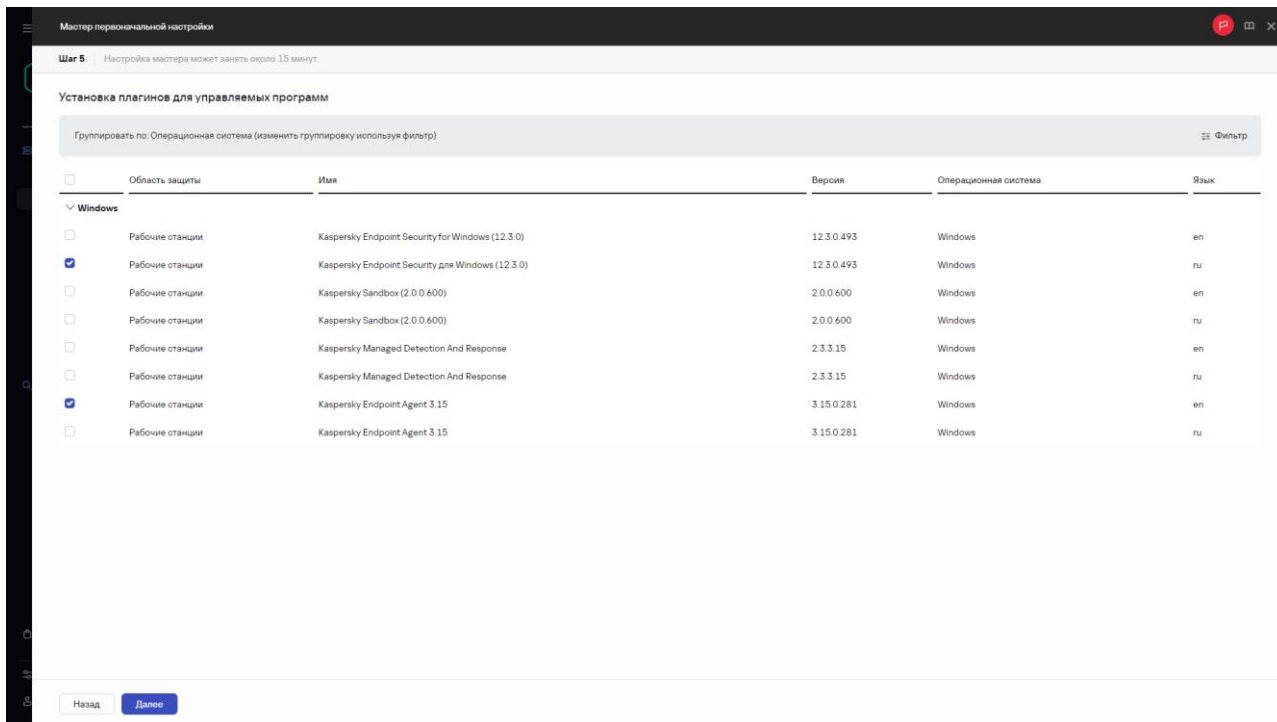
- Быстрое шифрование. Для этого типа шифрования используется 128-разрядный ключ.
- Стойкое шифрование. Для этого типа шифрования используется 256-разрядный ключ.

Вы можете выбрать дистрибутив (см. раздел "Загрузка дистрибутивов для приложений "Лаборатории Касперского"" на стр. [1089](#)) для Kaspersky Endpoint Security для Windows с необходимым типом шифрования позднее без запуска мастера первоначальной настройки.

Шаг 5. Настройка установки плагинов для управляемых приложений

Выберите плагины для управляемых приложений для установки. Отображается список плагинов, расположенных на серверах "Лаборатории Касперского". Список отфильтрован в соответствии с

параметрами, выбранными на предыдущем шаге мастера. По умолчанию в полный список включены плагины всех языков. Чтобы отображался только плагин на выбранном языке, используйте фильтр.



Список плагинов включает в себя следующие столбцы:

- **Область защиты**
- **Тип**
- **Имя**

Выбраны подключаемые модули в зависимости от областей защиты и платформ, выбранных на предыдущем шаге.

- **Версия**

В список включены плагины всех версий, размещенных на серверах "Лаборатории Касперского". По умолчанию выбраны плагины последних версий.

- **Последняя версия**
- **Операционная система**
- **Язык**

По умолчанию язык локализации плагина зависит от языка Kaspersky Security Center, который вы выбрали при установке. Другие языки можно выбрать в раскрывающемся списке **Отображать язык Консоли администрирования или**.

После выбора подключаемых модулей нажмите на кнопку **Далее**, чтобы начать установку.

Вы можете установить плагины управления для программ "Лаборатории Касперского" вручную позднее без запуска мастера первоначальной настройки.

Мастер первоначальной настройки автоматически установит выбранные плагины. Для установки некоторых плагинов вам нужно принять условия Лицензионного соглашения. Ознакомьтесь с текстом Лицензионного соглашения, который отображается на экране, установите флажок **Я принимаю условия использования**

Kaspersky Security Network и нажмите на кнопку **Установить**. Если вы не согласны с условиями Лицензионного соглашения, плагин не установится.

Когда все выбранные плагины будут установлены, мастер первоначальной настройки автоматически перейдет к следующему шагу.

Шаг 6. Установка выбранных плагинов

Мастер первоначальной настройки автоматически устанавливает плагины, выбранные на предыдущем шаге (см. раздел "Шаг 5. Настройка установки плагинов для управляемых приложений" см. стр. [1054](#)). Для установки некоторых плагинов вам нужно принять условия Лицензионного соглашения. Ознакомьтесь с текстом Лицензионного соглашения, который отображается на экране, установите флажок **Я принимаю условия использования Kaspersky Security Network** и нажмите на кнопку **Установить**. Если вы не согласны с условиями Лицензионного соглашения, плагин не установится.

Когда все выбранные плагины будут установлены, мастер первоначальной настройки автоматически перейдет к следующему шагу.

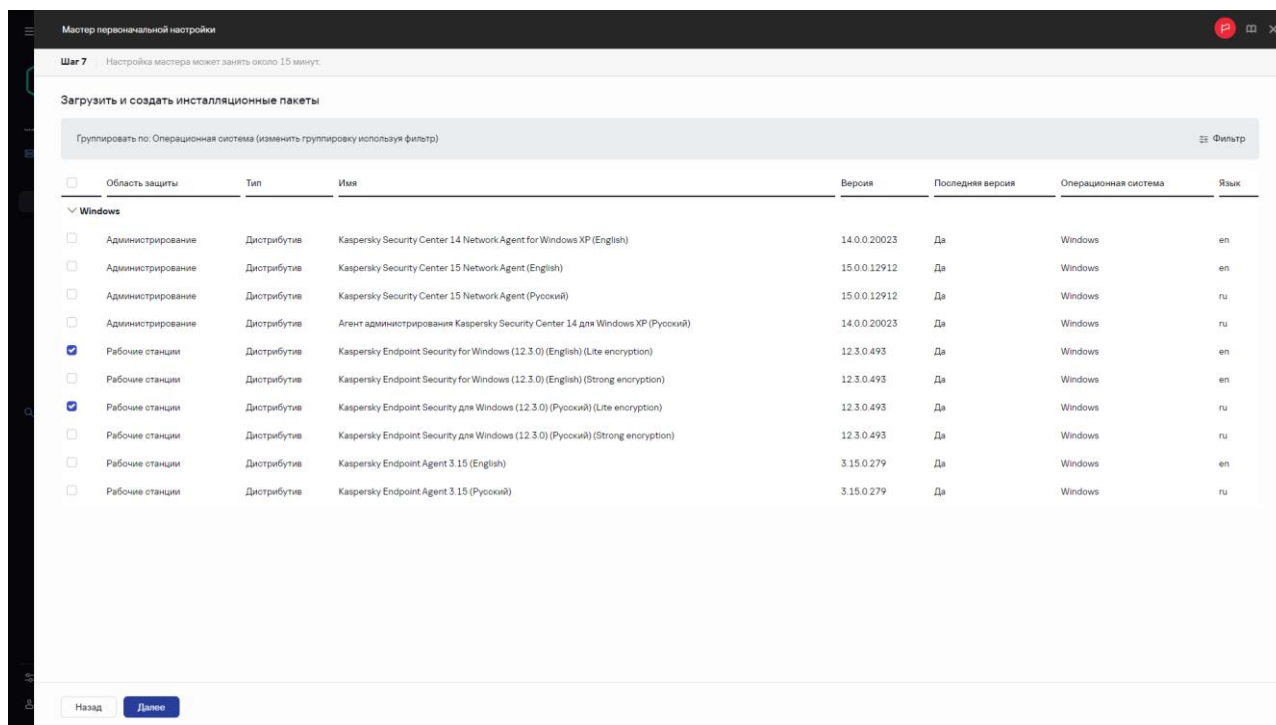
Шаг 7. Загрузка дистрибутивов и создание инсталляционных пакетов

Выберите дистрибутив для загрузки.

Для дистрибутивов управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center.

После того, как вы выбрали тип шифрования для Kaspersky Endpoint Security для Windows, отобразится список дистрибутивов для обоих типов шифрования. В списке выбран дистрибутив с выбранным типом шифрования. Вы можете выбрать дистрибутив для любого типа шифрования. Язык дистрибутива

соответствует языку Kaspersky Security Center. Если дистрибутив Kaspersky Endpoint Security для Windows для языка Kaspersky Security Center не существует, выбирается дистрибутив на английском языке.



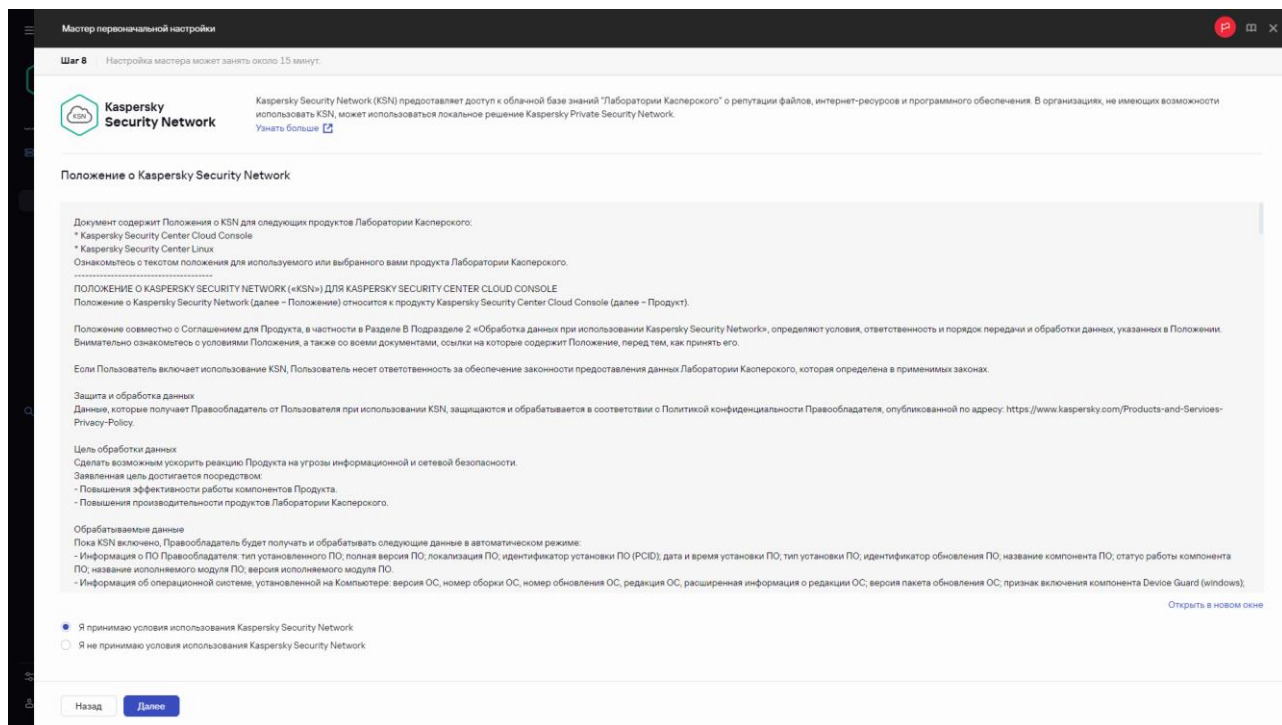
Чтобы завершить загрузку некоторых дистрибутивов вам нужно принять Лицензионное соглашение. При нажатии кнопки **Принять** отображается текст Лицензионного соглашения. Чтобы перейти к следующему шагу мастера, вам нужно принять положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского". Если вы не принимаете положения и условия, загрузка пакета отменяется.

После того, как вы приняли положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского", загрузка дистрибутивов продолжается. В дальнейшем инсталляционные пакеты можно использовать для развертывания приложений "Лаборатории Касперского" на клиентских устройствах.

Вы можете загрузить дистрибутивы и создать инсталляционные пакеты (см. раздел "Загрузка дистрибутивов для приложений "Лаборатории Касперского"" на стр. [1089](#)) позднее без запуска мастера первоначальной настройки.

Шаг 8. Настройка Kaspersky Security Network

Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network.



Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

Клиентские устройства под управлением Kaspersky Security Center в автоматическом режиме будут предоставлять "Лаборатории Касперского" информацию о работе установленных на них приложений "Лаборатории Касперского". Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия использования Kaspersky Security Network**

Клиентские устройства под управлением Kaspersky Security Center не будут предоставлять "Лаборатории Касперского" информацию о работе установленных на них приложений "Лаборатории Касперского".

Вы можете настроить доступ к Kaspersky Security Network (KSN) (см. раздел "Настройка доступа к KSN" см. стр. [1328](#)) позднее без запуска мастера первоначальной настройки.

Шаг 9. Выбор способа активации приложения

Выберите один из следующих вариантов активации Kaspersky Security Center:

- Введите ваш код активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security Center. Вы получаете код активации по указанному вами адресу

электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

- Укажите файл ключа

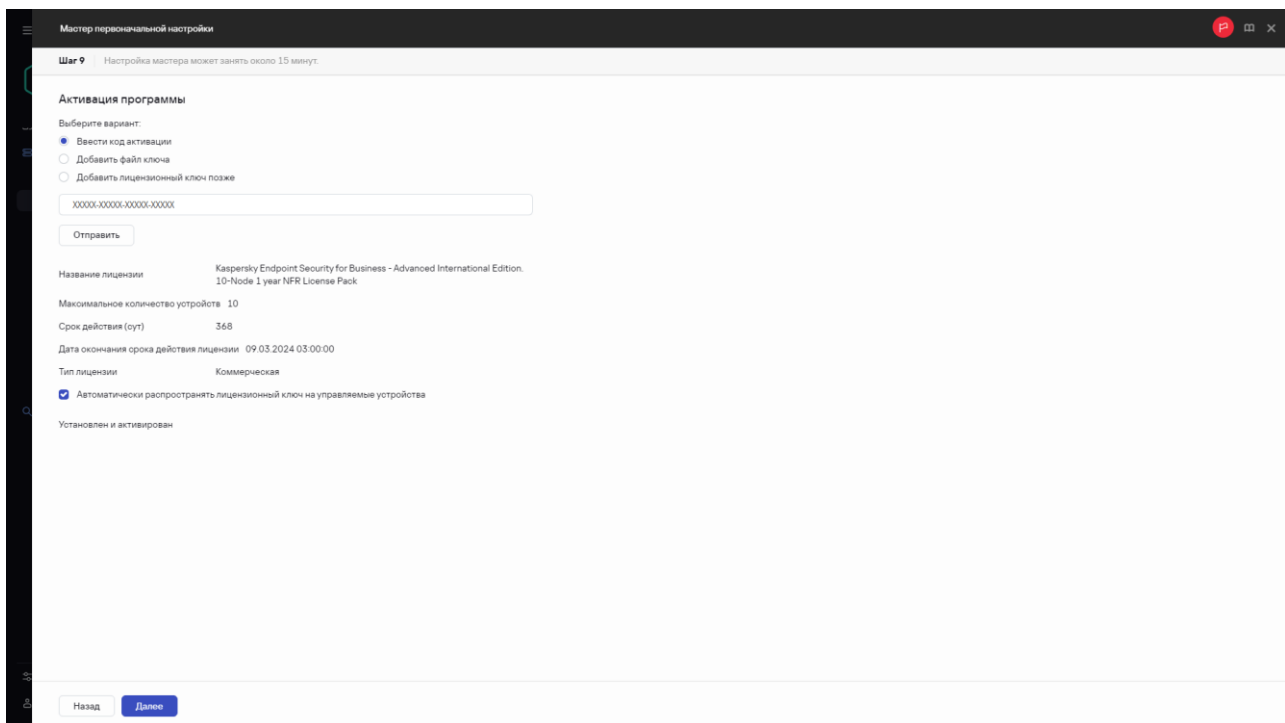
Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего приложение.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

- Отложите активацию приложения

Приложение будет работать в ограниченном режиме, без поддержки мобильных устройств и без функциональности системного администрирования.



Если вы отложили активацию приложения, вы можете добавить ключ позже в любое время, выбрав **Операции** → **Лицензирование**.

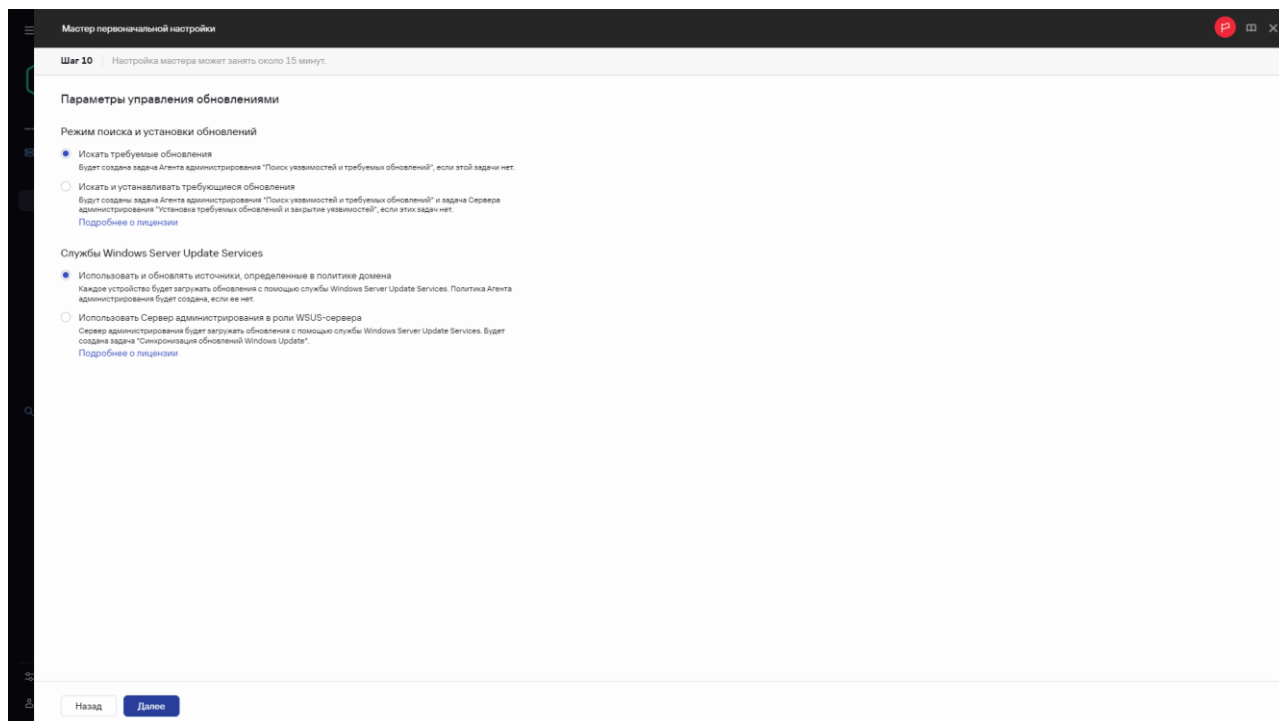
При работе с Kaspersky Security Center, развернутым из платного образа AMI или с использованием ежемесячных счетов за использование SKU, вы не можете указать файл ключа или ввести код активации.

См. также:

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console.....[985](#)

Шаг 10. Указание параметров управления обновлениями приложений сторонних производителей

Этот шаг не отображается, если у вас нет лицензии на Системное администрирование, а задача *Поиск уязвимостей и требуемых обновлений* уже существует.



Для обновлений приложений сторонних производителей выберите один из следующих вариантов:

- **Искать требуемые обновления**

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически, если она еще не создана.

По умолчанию этот вариант выбран.

- **Искать и устанавливать требующиеся обновления**

Задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* создаются автоматически, если они не были созданы ранее.

Этот параметр доступен при наличии лицензии на Системное администрирование.

Для обновлений Центра обновления Windows выберите один из следующих вариантов:

- **Использовать источники обновлений, определенные в политике домена**
- **Использовать Сервер администрирования в роли WSUS-сервера**

Создается задача **Синхронизация обновлений Windows Update**.

Этот параметр доступен при наличии лицензии на Системное администрирование.

Вы можете создать (см. раздел "Создание задачи" на стр. [1174](#)) задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* позднее без запуска мастера

первоначальной настройки. Чтобы использовать Сервер администрирования в качестве WSUS-сервера, вам нужно создать задачу *Синхронизация обновлений Windows Update* (см. раздел "*Создание задачи Синхронизация обновлений Windows Update*." см. стр. [1413](#)) и выбрать параметр **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования.

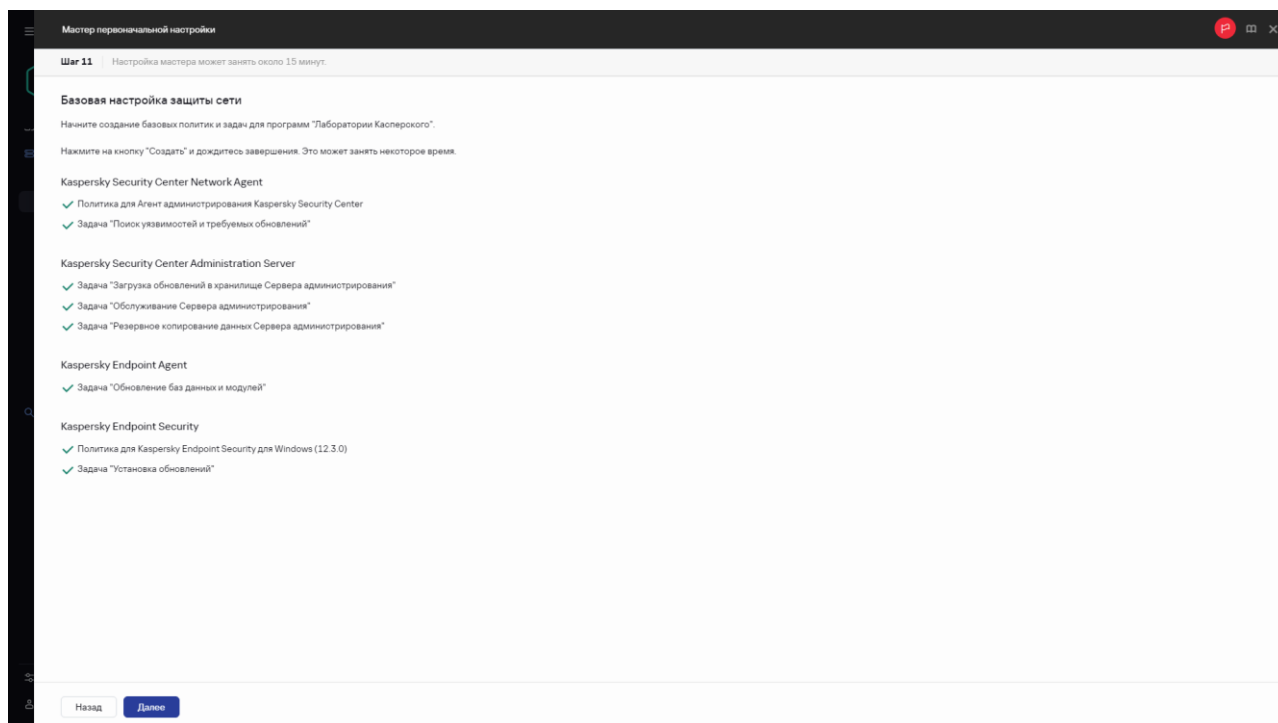
См. также:

Сценарий: обновление приложений сторонних производителей	499
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....	529
Создание задачи Поиск уязвимостей и требуемых обновлений.....	1393
Создание задачи Установка требуемых обновлений и закрытие уязвимостей.....	1399
Создание задачи Синхронизация обновлений Windows Update.	1413

Шаг 11. Создание базовой конфигурации защиты сети

Вы можете проверить список созданных политик и задач.

Для перехода на следующий шаг мастера дождитесь окончания создания политик и задач.



Можно создать необходимые задачи (см. раздел "*Создание задачи*" на стр. [1174](#)) и политики (см. раздел "*Создание политики*" на стр. [1251](#)) позднее без запуска мастера первоначальной настройки.

Шаг 12. Настройка параметров отправки уведомлений по электронной почте

Настройте параметры рассылки оповещений о событиях, регистрируемых при работе приложений "Лаборатории Касперского" на клиентских устройствах. Эти параметры будут использоваться в качестве значений по умолчанию в политиках приложений.

The screenshot shows the 'Шаг 12' (Step 12) configuration screen in the Kaspersky Security Center Web Console. The title bar reads 'Мастер первоначальной настройки' (Initial Setup Wizard). The step indicator shows 'Шаг 12' and a note: 'Настройка мастера может занять около 15 минут.' (The wizard configuration may take about 15 minutes). The main instruction is: 'Укажите один или несколько адресов электронной почты для получения уведомлений об ошибках' (Specify one or more email addresses for receiving error notifications). The form contains the following fields and controls:

- Получатели (адреса электронной почты)** (Recipients (email addresses)): A text area containing 'test_recipient@test.com'.
- Адрес SMTP-сервера** (SMTP server address): A text field containing 'smtp.test.com'.
- Порт SMTP-сервера** (SMTP server port): A text field with a blue border.
- ☐ **Использовать ESMTP-аутентификацию** (Use ESMTP authentication): An unchecked checkbox.
- Имя пользователя** (Username): A text field.
- Пароль** (Password): A text field with a 'Показать' (Show) button next to it.
- Отправить тестовое сообщение** (Send test message): A button.
- Используемый протокол TLS и его версия** (Used TLS protocol and its version): A dropdown menu.
- Использовать TLS** (Use TLS): A dropdown menu with the selected option 'Использовать TLS, если поддерживается SMTP-сервером' (Use TLS if supported by the SMTP server).

At the bottom, there are 'Назад' (Back) and 'Далее' (Next) buttons.

Для настройки рассылки оповещений о возникающих событиях приложений "Лаборатории Касперского" доступны следующие параметры:

- **Получатели (адреса электронной почты)**

Адреса электронной почты пользователей, которым приложение будет отправлять уведомления.

- **Адрес SMTP-сервера**

Адреса почтовых серверов вашей организации, введенные через точку с запятой. В качестве адреса может использоваться IP-адрес или имя устройства в сети Windows (NetBIOS-имя).

- **Порт SMTP-сервера**

Номер коммуникационного порта SMTP-сервера. По умолчанию указан порт 25.

- **Использовать ESMTP-аутентификацию**

Включение поддержки ESMTP-аутентификации. После установки флажка в полях **Имя пользователя** и **Пароль** можно указать параметры ESMTP-аутентификации. По умолчанию флажок снят, параметры ESMTP-аутентификации недоступны.

- **Использовать TLS**

Вы можете проверить параметры уведомления о сообщениях электронной почты с помощью кнопки **Отправить тестовое сообщение**.

Вы можете настроить уведомления о событии (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)) позднее без запуска мастера первоначальной настройки.

Шаг 13. Выполнение опроса сети

Сервер администрирования выполняет первоначальный опрос сети. Во время опроса отображается ход его выполнения. После завершения опроса ссылка **Просмотреть обнаруженные устройства** становится доступной. Вы можете перейти по ссылке, чтобы просмотреть устройства сети, обнаруженные Сервером администрирования. Чтобы вернуться в мастер первоначальной настройки, нажмите на кнопку **ESCAPE**.

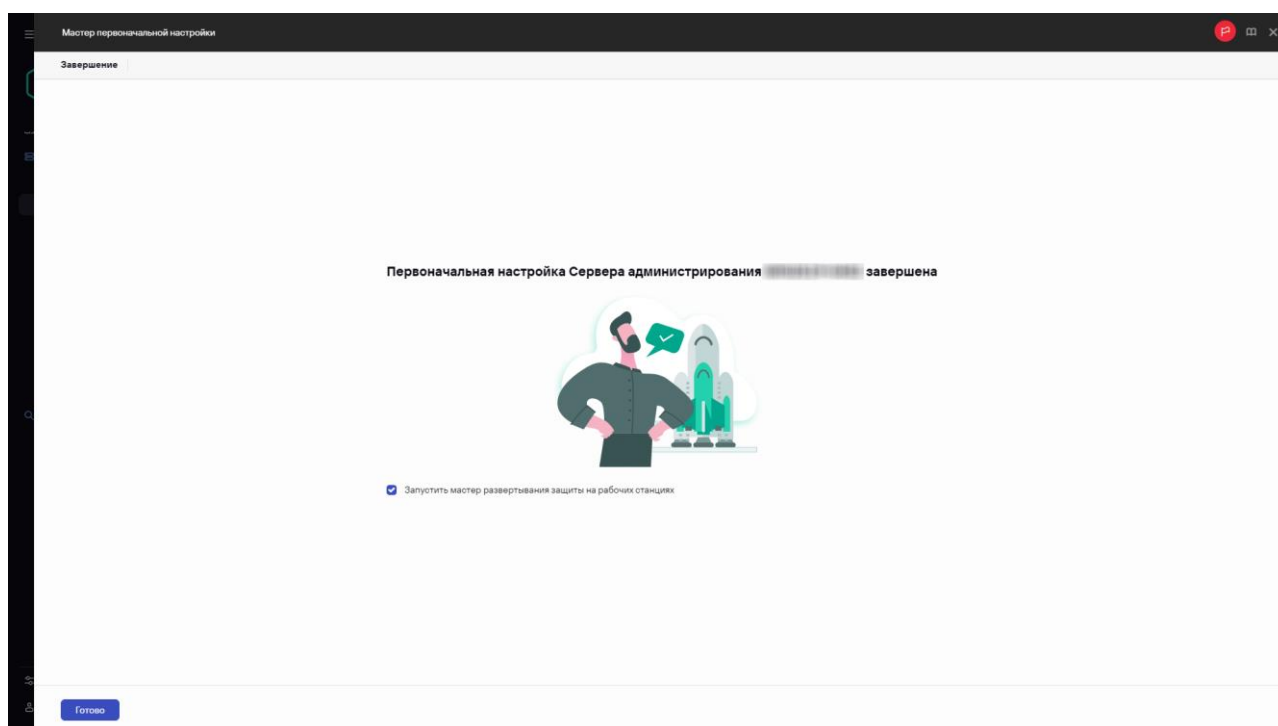
Вы можете выполнить опрос сети позднее без запуска мастера первоначальной настройки. С помощью Kaspersky Security Center Web Console настройте опрос контроллеров домена (см. раздел "Опрос контроллеров домена" см. стр. [1117](#)), Windows-доменов (см. раздел "Опрос сети Windows" см. стр. [1111](#)), IP-диапазонов (см. раздел "Опрос IP-диапазонов" см. стр. [1113](#)) и IPv6-сетей (см. раздел "Опрос Zeroconf" на стр. [1116](#)).

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Шаг 14. Завершение работы мастера первоначальной настройки

На странице завершения работы мастера первоначальной настройки установите флажок **Запустить мастер развертывания защиты на рабочих станциях**, если вы хотите запустить автоматическую установку (см. раздел "Мастер развертывания защиты" см. стр. [1076](#)) антивирусных приложений или Агента администрирования на устройства в вашей сети.



Для завершения работы мастера нажмите на кнопку **Готово**.

Подключение автономных устройств

В этом разделе описано, как подключить автономные устройства к Серверу администрирования (то есть управляемые устройства, находящиеся вне основной сети).

В этом разделе

Сценарий: подключение автономных устройств через шлюз соединения	1064
Сценарий: подключение автономных устройств через подчиненный Сервер администрирования в демилитаризованной зоне	1066
О подключении автономных устройств	300
Подключение внешних настольных компьютеров к Серверу администрирования	1069
О профилях соединения для автономных пользователей	1069
Создание профиля соединения для автономных пользователей	1070
О переключении Агента администрирования на другой Сервер администрирования	1073
Создание правила переключения Агента администрирования по сетевому местоположению.....	1074

Сценарий: подключение автономных устройств через шлюз соединения

В этом сценарии описано, как подключить к Серверу администрирования управляемые устройства, находящиеся вне основной сети.

Предварительные требования

Сценарий имеет следующие предварительные требования:

- В сети вашей организации организована демилитаризованная зона (DMZ).
- Сервер администрирования Kaspersky Security Center развернут в корпоративной сети.

Этапы

Этот сценарий состоит из следующих этапов:

а. Выбор клиентского устройства в демилитаризованной зоне

Это устройство будет использоваться в качестве шлюза соединения. Выбранное устройство должно соответствовать требованиям для шлюзов соединения.

б. Установка Агента администрирования в роли шлюза соединения

Для установки Агента администрирования на выбранное устройство рекомендуем использовать локальную установку.

По умолчанию установочный файл находится по адресу: \\<Имя Сервера>\KLSHARE\PkgInst\NetAgent_<номер версии>.

В окне **Шлюз соединения** мастера установки Агента администрирования выберите параметр **Использовать в качестве шлюза соединения в демилитаризованной зоне**. Этот режим одновременно активирует роль шлюза соединения и предписывает Агенту администрирования ждать соединений от Сервера администрирования, а не устанавливать соединения с Сервером администрирования.

Также вы можете установить Агент администрирования на устройство под управлением Linux и настроить Агент администрирования для работы в качестве шлюза соединения. Обратите внимание на список ограничений Агента администрирования, работающего на устройствах под управлением Linux.

с. Разрешение соединения на сетевом экране шлюза соединения

Чтобы Сервер администрирования мог подключаться к шлюзу соединения в демилитаризованной зоне, разрешите подключения к TCP-порту 13000 во всех сетевых экранов между Сервером администрирования и шлюзом соединения.

Если шлюз соединения не имеет реального IP-адреса в интернете, но вместо этого расположен за Network Address Translation (далее также NAT), настройте правило для пересылки подключений через NAT.

d. Создание группы администрирования для внешних устройств

Создайте группу (см. раздел "Создание групп администрирования" на стр. [1194](#)) внутри группы **Управляемые устройства**. Эта новая группа будет содержать внешние управляемые устройства.

e. Подключение шлюза соединения к Серверу администрирования

Настроенный вами шлюз соединения ожидает соединения от Сервера администрирования. Однако Сервер администрирования не перечисляет устройство со шлюзом соединения среди управляемых устройств. Это связано с тем, что шлюз соединения не пытался установить соединение с Сервером администрирования. Следовательно, вам потребуется особая процедура, чтобы Сервер администрирования инициировал соединение со шлюзом соединения.

Выполните следующие действия:

1. Добавьте шлюз соединения в качестве точки распространения (см. раздел "Назначение точек распространения вручную" на стр. [1370](#)).
2. Переместите шлюз соединения (см. раздел "Перемещение устройств или кластеров в состав группы администрирования вручную" на стр. [1196](#)) из группы **Нераспределенные устройства** в группу, которую вы создали для внешних устройств.

Шлюз соединения подключен и настроен.

f. Подключение внешних настольных компьютеров к Серверу администрирования

Обычно внешние настольные компьютеры не перемещаются внутрь периметра сети. Поэтому вам необходимо настроить их для подключения (см. раздел "Подключение внешних настольных компьютеров к Серверу администрирования" на стр. [1069](#)) к Серверу администрирования через шлюз соединения при установке Агента администрирования.

g. Настройка обновлений для внешних настольных компьютеров

Если обновления приложений безопасности настроены на загрузку с Сервера администрирования, внешние компьютеры загружают обновления через шлюз соединения. Это имеет два недостатка:

- Это лишний трафик, занимающий пропускную способность интернет-канала компании.
- Это не обязательно самый быстрый способ получать обновления. Возможно для внешних компьютеров будет удобнее получать обновления с серверов обновлений "Лаборатории Касперского".

Выполните следующие действия:

1. Переместите все внешние компьютеры в отдельную группу администрирования, (см. раздел "Перемещение устройств или кластеров в состав группы администрирования вручную" на стр. [1196](#)) которую вы создали ранее.

2. Исключить группу с внешними устройствами из задачи обновления (см. раздел "Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows" см. стр. [1361](#)).
3. Создайте отдельную задачу обновления для группы с внешними устройствами (см. раздел "Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows" см. стр. [1361](#)).

h. Подключение ноутбуков к Серверу администрирования

Иногда ноутбуки находятся внутри сети, а в другое время – вне сети. Для эффективного управления вам необходимо, чтобы они по-разному подключались к Серверу администрирования в зависимости от своего местоположения. Для эффективного использования трафика им также необходимо получать обновления из разных источников в зависимости от их местоположения.

Вам необходимо настроить правила для автономных пользователей (см. раздел "О переключении Агента администрирования на другой Сервер администрирования" на стр. [1073](#)): профили подключения (см. раздел "Создание профиля соединения для автономных пользователей" на стр. [1070](#)) и описания сетевых расположений (см. раздел "Создание правила переключения Агента администрирования по сетевому местоположению" на стр. [1074](#)). Каждое правило определяет экземпляр Сервера администрирования, к которому должны подключаться ноутбуки в зависимости от их местоположения, и экземпляр Сервера администрирования, с которого они должны получать обновления.

Сценарий: подключение автономных устройств через подчиненный Сервер администрирования в демилитаризованной зоне

Если вы хотите подключить управляемые устройства (см. раздел "О подключении автономных устройств" см. стр. [300](#)), расположенные вне основной сети, к Серверу администрирования, вы можете сделать это с помощью подчиненного Сервера администрирования, расположенного в демилитаризованной зоне (DMZ).

Предварительные требования

Прежде чем приступить, убедитесь, что вы выполнили следующее:

- В сети вашей организации организована демилитаризованная зона (DMZ).
- Сервер администрирования Kaspersky Security Center развернут во внутренней сети организации.

Этапы

Этот сценарий состоит из следующих этапов:

a. Выбор клиентского устройства в демилитаризованной зоне

В демилитаризованной зоне (DMZ) выберите клиентское устройство, которое будет использоваться в качестве подчиненного Сервера администрирования.

b. Установка Сервера администрирования Kaspersky Security Center.

Установите Сервер администрирования Kaspersky Security Center на этом клиентском устройстве.

c. Создание иерархии Серверов администрирования

Если вы размещаете подчиненный Сервер администрирования в демилитаризованной зоне, подчиненный Сервер администрирования должен принимать подключение от главного Сервера администрирования. Для этого добавьте новый Сервер администрирования в качестве подчиненного Сервера так, чтобы главный Сервер подключался к подчиненному Серверу по порту 13000. При объединении Серверов в иерархию (см. раздел "Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования" см. стр. [1020](#))

необходимо, чтобы порт 13299 обоих Серверов был доступен. Приложение Kaspersky Security Center Web Console подключается к Серверу администрирования по порту 13299.

d. Подключение автономных управляемых устройств к подчиненному Серверу администрирования

Вы можете подключить автономные устройства к Серверу администрирования в демилитаризованной зоне аналогично тому, как устанавливается соединение между Сервером администрирования и управляемыми устройствами находящимися в основной сети. Автономные устройства инициируют подключение через порт 13000.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

О подключении автономных устройств

Некоторые управляемые устройства, которые всегда находятся вне основной сети (например, компьютеры в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; компьютеры в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Некоторые устройства время от времени выходят за пределы периметра сети (например, ноутбуки пользователей, которые посещают региональные филиалы или офис клиента).

Вам по-прежнему необходимо отслеживать и управлять защитой устройств вне офиса – получать актуальную информацию об их статусе защиты и поддерживать приложения безопасности на них в актуальном состоянии. Это необходимо, например, потому, что если такое устройство будет скомпрометировано, находясь вдали от основной сети, то оно может стать платформой для распространения угроз, как только подключится к основной сети. Для подключения автономных устройств к Серверу администрирования вы можете использовать два способа:

- Шлюз соединения в демилитаризованной зоне (DMZ).
См. схему трафика данных: Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения.
- Сервер администрирования в демилитаризованной зоне (DMZ)
См. схему трафика данных: Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете.

Шлюз соединения в демилитаризованной зоне

Рекомендуемый способ подключения автономных устройств к Серверу администрирования это создание демилитаризованной зоны в сети организации и установка шлюза соединения в демилитаризованной зоне. Внешние устройства будут подключаться к шлюзу соединения, а Сервер администрирования внутри сети инициирует подключение к устройствам через шлюз соединения.

По сравнению с другим способ этот является более безопасным:

- Вам не нужно открывать доступ к Серверу администрирования извне.
- Скомпрометированный шлюз соединения не представляет большого риска для безопасности сетевых устройств. Шлюз соединения ничем не управляет и не устанавливает никаких соединений.

Кроме того, шлюз соединения не требует много аппаратных ресурсов.

Однако этот способ имеет более сложный процесс настройки:

- Чтобы устройство выполняло роль шлюза соединения в демилитаризованной зоне, вам необходимо установить Агент администрирования и подключить его к Серверу администрирования особым образом.
- Вы не сможете использовать один и тот же адрес подключения к Серверу администрирования для ситуаций. С внешней стороны периметра вам нужно будет использовать не только другой адрес (адрес шлюза соединения), но и другой режим подключения: через шлюз соединения.
- Вам также необходимо определить разные параметры подключения для ноутбуков в разных месторасположениях.

► *Чтобы добавить шлюз соединения в ранее настроенную сеть:*

1. Установите Агент администрирования в режиме шлюза соединения.
2. Переустановите Агент администрирования на устройствах, которые вы хотите подключить к вновь добавленному шлюзу соединения.

Сервер администрирования в демилитаризованной зоне (DMZ)

Другой способ это установка единого Сервера администрирования в демилитаризованной зоне.

Эта конфигурация менее безопасна, чем конфигурация первого способа. В этом случае для управления внешними ноутбуками Сервер администрирования должен принимать соединения с любого адреса из интернета. Сервер администрирования управляет всеми устройствами во внутренней сети, но из демилитаризованной зоны. Поэтому скомпрометированный Сервер может нанести огромный ущерб, несмотря на низкую вероятность такого события.

Риск значительно снижается, если Сервер администрирования в демилитаризованной зоне не управляет устройствами внутренней сети. Такая конфигурация может использоваться, например, поставщиком услуг для управления устройствами клиентов.

Вы можете использовать этот способ в следующих случаях:

- Если вы знакомы с установкой и настройкой Сервера администрирования и не хотите выполнять другую процедуру по установке и настройке шлюза соединения.
- Если вам нужно управлять большим количеством устройств. Максимальное количество устройств, которыми может управлять Сервер администрирования – 100 000 устройств, шлюз соединения может поддерживать до 10 000 устройств.

Это решение также имеет некоторые сложности:

- Серверу администрирования требуется больше аппаратных ресурсов и еще одна база данных.
- Информация об устройствах будет храниться в двух несвязанных между собой базах данных (для Сервера администрирования внутри сети и другой в демилитаризованной зоне), что усложняет контроль.
- Для управления всеми устройствами Сервер администрирования необходимо объединить в иерархию, что усложняет и контроль и управление. Экземпляр подчиненного Сервера администрирования накладывает ограничения на возможные структуры групп администрирования. Вам нужно решить, как и какие задачи и политики распространять на подчиненный Сервер администрирования.
- Настройка внешних устройств для использования Сервера администрирования в демилитаризованной зоне извне и для использования главного Сервера администрирования изнутри не проще, чем настройка подключения через шлюз.

- Высокие риски безопасности. Скомпрометированный Сервер администрирования упрощает взлом управляемых ноутбуков. Если это произойдет, хакерам просто нужно дождаться, пока один из ноутбуков вернется в корпоративную сеть, чтобы продолжить атаку на локальную сеть.

Подключение внешних настольных компьютеров к Серверу администрирования

Настольные компьютеры, которые всегда находятся вне основной сети (например, компьютеры в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; компьютеры в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Они должны быть подключены к Серверу администрирования через шлюз соединения, установленный в демилитаризованной зоне (DMZ). Такая конфигурация выполняется при установке Агента администрирования на эти устройства.

► Чтобы подключить внешние настольные компьютеры к Серверу администрирования:

1. Создание инсталляционного пакета Агента администрирования (см. раздел "Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"" см. стр. [1087](#)).
2. Откройте свойства созданного инсталляционного пакета, перейдите в раздел **Параметры** → **Дополнительно** и выберите параметр **Подключаться к Серверу администрирования через шлюз соединения**.

Параметр **Подключаться к Серверу администрирования через шлюз соединения** несовместим с параметром **Использовать в качестве шлюза соединения в демилитаризованной зоне**. Вы не можете включить оба этих параметра одновременно.

3. Укажите адрес шлюза соединения в поле **Адрес шлюза соединения**.
Если шлюз соединения расположен за Network Address Translation (NAT) и не имеет собственного общедоступного адреса, настройте правило шлюза NAT для перенаправления соединений с общедоступного адреса на внутренний адрес шлюза соединения.
4. Создайте автономный инсталляционный пакет (см. раздел "Создание автономного инсталляционного пакета" см. стр. [1090](#)) на основе созданного инсталляционного пакета.
5. Доставьте автономный инсталляционный пакет на целевые компьютеры в электронном виде или на съемном диске.
6. Установите Агент администрирования из автономного инсталляционного пакета.

К Серверу администрирования подключены внешние настольные компьютеры.

О профилях соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также "устройства"), может потребоваться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

Использование различных адресов одного и того же Сервера администрирования

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети организации, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования добавьте профиль для подключения к Серверу администрирования из интернета (в разделе **Параметры приложения** → **Подключения** → **Профили соединений** → **Профили подключения к Серверу администрирования**). В окне создания профиля выключите параметр **Использовать только для получения обновлений** и убедитесь, что выбран параметр **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center, описанной в разделе Доступ из интернета: Агент администрирования в качестве шлюза соединения в демилитаризованной зоне), в профиле подключения следует указать адрес шлюза соединения в соответствующем поле.

Переключение между Серверами администрирования в зависимости от текущей сети

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования создайте профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения укажите адреса соответствующих Серверов администрирования и включите (либо выключите) параметр **Использовать только для получения обновлений**:

- выбрать параметр, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;
- выключить параметр, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая "домашний офис". Смысл каждого такого условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

См. также:

Создание профиля соединения для автономных пользователей[1070](#)

Создание профиля соединения для автономных пользователей

Подключение профиля Агента администрирования к Серверу администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

► *Чтобы создать профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей:*

1. Если вы хотите создать профиль подключения для группы управляемых устройств, откройте политику Агента администрирования этой группы. Для этого выполните следующие:
 - a. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
 - b. Перейдите по ссылке на текущий путь.
 - c. В открывшемся окне выберите нужную группу администрирования.
После этого текущий путь меняется.
 - d. Добавьте политику Агента администрирования для группы управляемых устройств. Если вы уже создали ее, нажмите на название политики Агента администрирования, чтобы открыть свойства политики.
2. Если вы хотите создать профиль подключения для определенного управляемого устройства, выполните следующие действия:
 - a. В главном окне приложения перейдите в раздел **Активы (Устройства) → Управляемые устройства**.
 - b. Нажмите на имя требуемого управляемого устройства.
 - c. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.
 - d. Нажмите на название политики Агента администрирования, к которой применяется только выбранное управляемое устройство.
3. В открывшемся окне свойств перейдите в раздел **Параметры приложения → Подключения → Профили соединений**.
4. В разделе **Профили подключения к Серверу администрирования** нажмите на кнопку **Добавить**.

По умолчанию список профилей подключения содержит профили <Офлайн-режим> и <Домашний Сервер администрирования>. Профили недоступны для изменения и удаления.

В профиле <Офлайн-режим> не указывается Сервер для подключения. При переходе к этому профилю Агент администрирования не пытается подключиться к какому-либо Серверу, а установленные на клиентских устройствах приложения используют политики для автономных пользователей. Профиль <Офлайн-режим> применяется в условиях отключения устройств от сети.

В профиле <Домашний Сервер администрирования> указан Сервер для подключения, который был задан при установке Агента администрирования. Профиль <Домашний Сервер администрирования> применяется в условиях, когда устройство, которое работало в другой сети, вновь подключается к домашнему Серверу администрирования.

5. В открывшемся окне **Настроить профиль** настройте параметры профиля подключения:

- **Имя профиля**

В поле ввода можно просмотреть или изменить имя профиля подключения.

- **Адрес Сервера администрирования**

Адрес Сервера администрирования, к которому должно подключаться клиентское устройство при активации профиля.

- **Номер порта**

Номер порта, по которому будет выполняться подключение.

- **SSL-порт**

Номер порта, по которому будет осуществляться подключение с использованием SSL-протокола.

- **Использовать SSL-соединение**

Если флажок установлен, подключение будет выполняться через защищенный порт (с использованием SSL-протокола).

По умолчанию флажок установлен.

- Выберите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

- **Адрес**

Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

- **Номер порта**

Номер порта, по которому будет выполняться подключение Kaspersky Security Center к прокси-серверу.

- **Аутентификация на прокси-сервере**

- **Имя пользователя**

- **Пароль**

- **Адрес шлюза соединения**

Адрес шлюза, через который устанавливается соединение клиентских устройств с Сервером администрирования.

- **Включить автономный режим, когда Сервер администрирования недоступен**

- **Использовать только для получения обновлений**

Если флажок установлен, профиль будет использоваться только при загрузке обновлений приложениями, установленными на клиентском устройстве. Для остальных операций подключение к Серверу администрирования будет выполняться с исходными параметрами подключения, заданными при установке Агента администрирования.

По умолчанию флажок установлен.

- **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**

В результате будет создан профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей. При подключении Агента администрирования к Серверу через этот профиль приложения, установленные на клиентском устройстве, будут использовать политики для устройств, находящиеся в автономном режиме, или политики для автономных пользователей.

См. также:

О профилях соединения для автономных пользователей[1069](#)

О переключении Агента администрирования на другой Сервер администрирования

В Kaspersky Security Center предусмотрена возможность переключения Агента администрирования клиентского устройства на другие Серверы администрирования при изменении следующих характеристик сети:

- **Условие для адреса DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.
- **Условие для адреса шлюза соединения по умолчанию** – изменение основного шлюза сети.
- **Условие для DNS-домена** – изменение DNS-суффикса подсети.
- **Условие для адресов DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
- **Условие для адреса WINS-сервера** – изменение IP-адреса WINS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для разрешимости имен** – у клиентского устройства изменилось NetBIOS-имя или DNS-имя.
- **Условие для подсети** – изменение адреса и маски подсети.
- **Условие для доступности Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для доступности адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с Сервером (имя:порт). Для каждого Сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат Сервера администрирования в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается.

Эта функция поддерживается только для Агентов администрирования, установленных на устройствах под управлением Windows или macOS.

Исходные параметры подключения Агента администрирования к Серверу задаются при установке Агента администрирования. В дальнейшем, если сформированы правила переключения Агента администрирования на другие Серверы администрирования, Агент реагирует на изменение характеристик сети следующим образом:

- Если характеристики сети соответствуют одному из сформированных правил, Агент администрирования подключается к указанному в этом правиле Серверу администрирования. Если это задано правилом, установленные на клиентских устройствах приложения переходят на политики для автономных пользователей.
- Если ни одно из правил не выполняется, Агент администрирования возвращается к исходным параметрам подключения к Серверу администрирования, заданным при установке. Установленные на клиентских устройствах приложения возвращаются к активным политикам.
- Если Сервер администрирования недоступен, Агент администрирования использует политики для автономных пользователей.

Агент администрирования переключается на политику для автономных пользователей, только если параметр **Включить автономный режим, когда Сервер администрирования недоступен** (см. раздел **"Создание профиля соединения для автономных пользователей"** на стр. 1070) включен в параметрах политики Агента администрирования.

Параметры подключения Агента администрирования к Серверу администрирования сохраняются в профиле подключения. В профиле подключения вы можете создавать правила перехода клиентских устройств на политики для автономных пользователей, а также настраивать профиль таким образом, чтобы он использовался только для загрузки обновлений.

См. также:

Создание правила переключения Агента администрирования по сетевому местоположению.....[1074](#)

Создание правила переключения Агента администрирования по сетевому местоположению

Переключение Агента администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

- Чтобы создать правило для переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети:
1. Если вы хотите создать правило для группы управляемых устройств, откройте политику Агента администрирования этой группы. Для этого выполните следующие:
 - a. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
 - b. Перейдите по ссылке на текущий путь.
 - c. В открывшемся окне выберите нужную группу администрирования.
После этого текущий путь меняется.
 - d. Добавьте политику Агента администрирования для группы управляемых устройств. Если вы уже создали ее, нажмите на название политики Агента администрирования, чтобы открыть свойства политики.
 2. Если вы хотите создать правило для определенного управляемого устройства, сделайте следующее:
 - a. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
 - b. Нажмите на имя требуемого управляемого устройства.
 - c. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.
 - d. Нажмите на название политики Агента администрирования, к которой применяется только выбранное управляемое устройство.
 3. В открывшемся окне свойств перейдите в раздел **Параметры приложения** → **Подключения** → **Профили соединений**.
 4. В разделе **Параметры сетевого местоположения** нажмите на кнопку **Добавить**.
 5. В открывшемся окне свойств настройте описание сетевого местоположения и правило переключения. Настройте следующие параметры описания сетевого местоположения:
 - **Описание**

Имя описания сетевого местоположения не может превышать 255 символов и содержать специальные символы ("*<>?V:|").

- **Использовать профиль подключения**

В раскрывающемся списке можно выбрать профиль подключения Агента администрирования к Серверу администрирования. Профиль будет использоваться при выполнении условий описания сетевого местоположения. Профиль подключения содержит параметры подключения Агента администрирования к Серверу администрирования и определяет переход клиентских устройств на политики для автономных пользователей. Профиль используется только для загрузки обновлений.

- **Описание активно**

6. Выберите условия для правила переключения Агента администрирования:

- **Условие для адреса DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.
- **Условие для адреса шлюза соединения по умолчанию** – изменение основного шлюза сети.
- **Условие для DNS-домена** – изменение DNS-суффикса подсети.
- **Условие для адресов DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
- **Условие для адреса WINS-сервера** – изменение IP-адреса WINS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для разрешимости имен** – у клиентского устройства изменилось NetBIOS-имя или DNS-имя.
- **Условие для подсети** – изменение адреса и маски подсети.
- **Условие для доступности Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для доступности адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с Сервером (имя:порт). Для каждого Сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат Сервера администрирования в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается.

Условия правила объединяются с использованием логического оператора AND. Чтобы правило переключения по описанию сетевого местоположения сработало, все условия переключения правила должны быть выполнены.

7. В разделе с условиями укажите, когда Агент администрирования нужно переключить на другой Сервер администрирования. Для этого нажмите на кнопку **Добавить** и установите значение условия.

Параметр **Соответствует хотя бы одному значению списка** включен по умолчанию. Можно выключить этот параметр, если вы хотите, чтобы условие выполнялось со всеми указанными значениями.

8. Сохраните изменения.

В результате будет создано правило переключения по описанию сетевого местоположения, при выполнении условий которого Агент администрирования будет использовать для подключения к Серверу администрирования указанный в описании профиль подключения.

См. также:

О переключении Агента администрирования на другой Сервер администрирования[1073](#)

Мастер развертывания защиты

Для установки приложений "Лаборатории Касперского" можно воспользоваться мастером развертывания защиты. Мастер развертывания защиты позволяет проводить удаленную установку приложений как с использованием специально созданных инсталляционных пакетов, так и напрямую из дистрибутивов.

Мастер развертывания защиты выполнит следующие действия:

- Загружает инсталляционный пакет для установки приложения (если он не был создан раньше). Инсталляционный пакет расположен: **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**. Вы можете использовать этот инсталляционный пакет для установки приложения в дальнейшем.
- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Созданная задача удаленной установки хранится в разделе **Задачи**. Вы можете запустить эту задачу в дальнейшем вручную. Тип задачи – **Удаленная установка приложения**.

Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет `insserv-compat`, чтобы настроить Агент администрирования.

См. также:

Сценарий: развертывание приложений "Лаборатории Касперского"	1084
В этом разделе	
Запуск мастера развертывания защиты	1077
Шаг 1. Выбор инсталляционного пакета	1077
Шаг 2. Выбор способа распространения файла ключа или кода активации	1078
Шаг 3. Выбор версии Агента администрирования	1078
Шаг 4. Выбор устройств	1078
Шаг 5. Задание параметров задачи удаленной установки	1079
Шаг 6. Управление перезагрузкой	1080
Шаг 7. Удаление несовместимых приложений перед установкой	1081
Шаг 8. Перемещение устройств в папку Управляемые устройства	1082
Шаг 9. Выбор учетных записей для доступа к устройствам	1082
Шаг 10. Запуск установки	1083

Запуск мастера развертывания защиты

► Чтобы запустить мастер развертывания защиты вручную,

в главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер развертывания защиты**.

Запустится мастер развертывания защиты. Для продолжения работы мастера нажмите на кнопку **Далее**.

См. также:

Мастер развертывания защиты	1076
Сценарий: развертывание приложений "Лаборатории Касперского"	1084

Шаг 1. Выбор инсталляционного пакета

Выберите инсталляционный пакет приложения, которое требуется установить.

Если инсталляционный пакет требуемого приложения не содержится в списке, нажмите на кнопку **Добавить** и выберите приложение из списка.

См. также:

Мастер развертывания защиты	1076
Сценарий: развертывание приложений "Лаборатории Касперского"	1084

Шаг 2. Выбор способа распространения файла ключа или кода активации

Выберите способ распространения файла ключа или кода активации:

- **Не добавлять лицензионный ключ в инсталляционный пакет**

Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

- если в свойствах ключа настроено автоматическое распространение;
- если создана задача **Добавление ключа**.

- **Добавить лицензионный ключ в инсталляционный пакет**

Если выбран этот вариант, ключ распространяется на устройства вместе с инсталляционным пакетом.

Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу пакетов настроен общий доступ на чтение.

Если инсталляционный пакет уже содержит файл ключа или код активации, это окно отображается, но оно содержит только информацию о лицензионном ключе.

См. также:

Мастер развертывания защиты	1076
Сценарий: развертывание приложений "Лаборатории Касперского"	1084

Шаг 3. Выбор версии Агента администрирования

Если вы выбрали инсталляционный пакет приложения, отличное от Агента администрирования, необходимо также установить Агент администрирования для подключения приложения к Серверу администрирования Kaspersky Security Center.

Выберите последнюю версию Агента администрирования.

Шаг 4. Выбор устройств

Укажите список устройств, на которые требуется установить приложение:

- **Установить на управляемые устройства**

Если выбран этот вариант, задача удаленной установки приложения будет создана для группы устройств.

- **Выбор устройств для установки**

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

См. также:

Мастер развертывания защиты	1076
Сценарий: развертывание приложений "Лаборатории Касперского"	1084

Шаг 5. Задание параметров задачи удаленной установки

В окне **Параметры задачи удаленной установки** настройте параметры удаленной установки приложения.

В блоке параметров **Принудительно загрузить инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

- **С помощью Агента администрирования**

Если флажок установлен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

Если флажок снят, доставка инсталляционных пакетов выполняется средствами Microsoft Windows.

Рекомендуется установить флажок, если задача назначена для устройств с установленными Агентами администрирования.

По умолчанию флажок установлен.

- **Средствами операционной системы с помощью точек распространения**

Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

- **Средствами операционной системы с помощью Сервера администрирования**

Если флажок установлен, доставка файлов на клиентские устройства будет

осуществляться средствами Microsoft Windows с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

По умолчанию флажок установлен.

Настройте дополнительные параметры:

- **Не устанавливать приложение, если оно уже установлено**

Если флажок установлен, выбранное приложение не устанавливается заново, если она уже установлена на клиентском устройстве.

Если флажок снят, приложение будет установлено в любом случае.

По умолчанию флажок установлен.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

Если флажок установлен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

Флажок доступен если выбран инсталляционный пакет Агента администрирования.

По умолчанию флажок снят.

Шаг 6. Управление перезагрузкой

Укажите действие, которое требуется выполнить, если необходимо перезагрузить операционную систему во время установки приложения:

- **Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать

наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

См. также:

Мастер развертывания защиты[1076](#)

Сценарий: развертывание приложений "Лаборатории Касперского"[1084](#)

Шаг 7. Удаление несовместимых приложений перед установкой

Этот шаг присутствует, только если приложение, которое вы разворачиваете, несовместимо с другими приложениями.

Выберите этот параметр, если вы хотите, чтобы приложение Kaspersky Security Center автоматически удаляло несовместимые приложения с приложением, которое вы устанавливаете.

Отображается список несовместимых приложений.

Если этот параметр не выбран, приложение будет установлено только на устройствах, на которых нет несовместимых приложений.

См. также:

Мастер развертывания защиты.....	1076
Сценарий: развертывание приложений "Лаборатории Касперского"	1084

Шаг 8. Перемещение устройств в папку Управляемые устройства

Укажите, следует ли перемещать устройства в группу администрирования после установки Агента администрирования.

- **Не перемещать устройства**

Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

- **Перемещать нераспределенные устройства в группу**

Устройства перемещаются в выбранную вами группу администрирования.

По умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

См. также:

Мастер развертывания защиты.....	1076
Сценарий: развертывание приложений "Лаборатории Касперского"	1084

Шаг 9. Выбор учетных записей для доступа к устройствам

Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной установки:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

Если выбран этот вариант, можно указать учетную запись, от имени которой будет запускаться инсталлятор приложения. Учетную запись можно указать в случае если Агент администрирования не установлен на устройствах, для которых назначена задача.

Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

Если ни одна учетная запись не добавлена, задача запускается под той учетной записью, под которой работает служба Сервера администрирования.

См. также:

Мастер развертывания защиты	1076
Сценарий: развертывание приложений "Лаборатории Касперского"	1084

Шаг 10. Запуск установки

Это последний шаг мастера. На этом шаге **Задача удаленной установки приложения** была успешно создана и настроена.

По умолчанию вариант **Запустить задачу после завершения работы мастера** не выбран. Если вы выберете этот параметр, **Задача удаленной установки приложения** начнется сразу после завершения работы мастера. Если вы не выберете этот параметр, **Задача удаленной установки приложения** не начнется. Вы можете запустить эту задачу в дальнейшем вручную.

Нажмите на кнопку **ОК**, чтобы завершить последний шаг мастера развертывания защиты.

См. также:

Мастер развертывания защиты	1076
Сценарий: развертывание приложений "Лаборатории Касперского"	1084

Развертывание приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console

В этом разделе описано, как развернуть приложения "Лаборатории Касперского" на клиентских устройствах в вашей организации с помощью Kaspersky Security Center Web Console.

В этом разделе

Сценарий: развертывание приложений "Лаборатории Касперского"	1084
Загрузка плагинов для приложений "Лаборатории Касперского"	1086
Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"	1087
Изменение ограничения на размер пользовательского инсталляционного пакета	1088
Загрузка дистрибутивов для приложений "Лаборатории Касперского"	1089
Проверка успешности развертывания Kaspersky Endpoint Security	1090
Создание автономного инсталляционного пакета	1090
Просмотр списка автономных инсталляционных пакетов	1092
Создание пользовательского инсталляционного пакета	1093
Распространение инсталляционных пакетов на подчиненные Серверы администрирования	1097
Установка приложений с помощью задачи удаленной установки	359
Указание параметров удаленной установки на устройствах под управлением Unix	1106
Управление мобильными устройствами	1107
Замещение приложений безопасности сторонних производителей	358

Сценарий: развертывание приложений "Лаборатории Касперского"

В этом сценарии описана процедура развертывания приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console. Можно либо воспользоваться мастером первоначальной настройки (см. раздел "Мастер первоначальной настройки (Kaspersky Security Center Web Console)" см. стр. [1047](#)) и мастером развертывания защиты, либо выполнить все необходимые шаги вручную.

Развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

а. Загрузка веб-плагина управления приложения

Скачайте веб-плагин управления Kaspersky Endpoint Security для Linux <https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint> с сайта "Лаборатории Касперского" и добавьте плагин в Kaspersky Security Center Web Console.

б. Загрузка и создание инсталляционных пакетов для Агента администрирования

Загрузите дистрибутив Агента администрирования <https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint> с сайта "Лаборатории Касперского" и создайте

инсталляционный пакет Агента администрирования (см. раздел "Создание пользовательского инсталляционного пакета" на стр. [1093](#)).

Вы можете использовать загруженный инсталляционный пакет для локальной установки Агента администрирования. Для этого следуйте инструкциям, приведенным в документации Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/11.2.0/en-US/197912.htm>.

с. инсталляционный пакет для Kaspersky Endpoint Security для Linux;

Загрузите дистрибутив Kaspersky Endpoint Security для Linux <https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint> с сайта "Лаборатории Касперского" и создайте инсталляционный пакет Kaspersky Endpoint Security для Linux (см. раздел "Создание пользовательского инсталляционного пакета" на стр. [1093](#)).

d. Создание автономного инсталляционного пакета

Если вы не можете установить приложения "Лаборатории Касперского" с помощью Kaspersky Security Center на некоторых устройствах, например, на устройствах удаленных сотрудников, вы можете создавать автономные инсталляционные пакеты (см. раздел "Создание автономного инсталляционного пакета" см. стр. [1090](#)) для приложений. Если вы используете автономные пакеты для установки программ «Лаборатории Касперского» пропустите пункты 5 и 6 этого сценария.

e. Создание, настройка и запуск задачи удаленной установки

Этот шаг входит в мастер развертывания защиты. Если вы не запускали мастер развертывания защиты, вам необходимо создать (см. раздел "Создание задачи" на стр. [1174](#)) и настроить эту задачу вручную.

Вы можете вручную создать несколько задач удаленной установки для различных групп администрирования или выборок устройств. Вы можете развернуть различные версии одного приложения в этих задачах.

Убедитесь, что все устройства в сети обнаружены, а затем запустите задачу (или задачи) удаленной установки.

Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет `insserv-compat`, чтобы настроить Агент администрирования.

f. Создание и настройка задач

Задача *Установка обновлений* Kaspersky Endpoint Security для Linux должна быть настроена.

Этот шаг входит в мастер первоначальной настройки: задача создается и настраивается автоматически, с параметрами по умолчанию. Если вы не запускали мастер первоначальной настройки, вам необходимо создать (см. раздел "Создание задачи" на стр. [1174](#)) и настроить эту задачу вручную. Если вы запускали мастер первоначальной настройки, убедитесь, что расписание запуска задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)) соответствует вашим требованиям. (По умолчанию для времени запуска задачи установлено значение **Вручную**, но вам может понадобиться изменить это значение.)

g. Создание политик

Создайте политику Kaspersky Endpoint Security для Linux вручную (см. раздел "Создание политики" на стр. [1251](#)) или с помощью мастера первоначальной настройки. Можно использовать установленные по умолчанию параметры политики. Также вы можете в любое время изменить заданные по умолчанию параметры (см. раздел "Создание политики" на стр. [1251](#)) политики в соответствии с вашими требованиями.

h. Проверка результатов

Убедитесь (см. раздел "Проверка успешности развертывания Kaspersky Endpoint Security" на стр. [1090](#)), что развертывание завершилось успешно: созданы политики и задачи для каждого приложения и эти приложения установлены на управляемые устройства.

Результаты

Завершение сценария дает следующее:

- Все требуемые политики и задачи для выбранных приложений созданы.
- Расписание запуска задач настроено в соответствии с вашими требованиями.
- На выбранных клиентских устройствах развернуты или запланированы к развертыванию выбранные приложения.

Загрузка плагинов для приложений "Лаборатории Касперского"

Для развертывания приложений "Лаборатории Касперского", таких как Kaspersky Endpoint Security для Windows, необходимо загрузить плагины управления для этих приложений.

► Чтобы загрузить плагин управления для приложения "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Параметры** → **Веб-плагины**.
2. В появившемся окне нажмите на кнопку **Добавить**.
Отобразится список доступных плагинов управления.
3. В списке доступных плагинов выберите имя плагина, который требуется загрузить (например, Kaspersky Endpoint Security 11 для Windows).
Отобразится страница с описанием плагина.
4. На странице описания плагина нажмите на кнопку **Установить плагин**.
5. После завершения установки нажмите на кнопку **ОК**.

Плагин управления будет загружен в конфигурации по умолчанию и появится в списке плагинов управления.

Вы можете добавлять плагины и обновлять загруженные плагины из файла. Вы можете загрузить плагины управления и веб-плагины управления с сайта Службы технической поддержки "Лаборатории Касперского" <https://support.kaspersky.com/9333>.

► Чтобы загрузить или обновить плагин из файла:

1. В главном окне приложения перейдите в раздел **Параметры** → **Веб-плагины**.
2. Выполните одно из следующих действий:
 - Нажмите на **Добавить из файла**, чтобы загрузить плагин из файла.
 - Нажмите на **Обновить из файла**, чтобы загрузить обновление для плагина из файла.
3. Укажите файл и подпись файла.
4. Загрузите указанные файлы.

Плагин управления будет загружен из файла и появится в списке плагинов управления.

См. также:

Сценарий: развертывание приложений "Лаборатории Касперского"[1084](#)

Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"

Если у Сервера администрирования есть доступ в интернет, вы можете создать инсталляционные пакеты приложений "Лаборатории Касперского" с веб-серверов "Лаборатории Касперского".

► Чтобы загрузить и создать инсталляционный пакет для приложения "Лаборатории Касперского":

1. Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
- В главном окне программы перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

Вы также можете просматривать информацию о новых пакетах для приложений "Лаборатории Касперского" в списке экранных уведомлений (см. раздел "Просмотр экранных уведомлений" на стр. [1540](#)). Если есть уведомления о новом пакете, вы можете перейти по ссылке рядом с уведомлением к списку доступных инсталляционных пакетов.

Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

Отобразится список инсталляционных пакетов доступных на веб-серверах "Лаборатории Касперского". Список содержит инсталляционные пакеты только тех приложений, которые совместимы с текущей версией Kaspersky Security Center.

4. Выберите требуемый инсталляционный пакет, например, Kaspersky Endpoint Security для Windows (11.1.0).

Откроется окно с информацией об инсталляционном пакете.

Вы можете загрузить и использовать инсталляционный пакет, который включает в себя криптографические инструменты, реализующие надежное шифрование, если он соответствует применимым законам и правилам. Чтобы загрузить инсталляционный пакет Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.

5. Ознакомьтесь с информацией и нажмите на кнопку **Загрузить и создать инсталляционный пакет**.

Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Загрузить и создать инсталляционный пакет** отображается кнопка **Загрузить дистрибутив**.

Начинается загрузка инсталляционного пакета на Сервер администрирования. Вы можете закрыть окно мастера или перейти к следующему шагу инструкции. Если вы закроете мастер, процесс загрузки продолжится в фоновом режиме.

Если вы хотите отслеживать процесс загрузки инсталляционного пакета:

- a. В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты** → **В процессе** ().
- b. Следите за ходом операции в столбцах **Ход загрузки** и **Состояние загрузки** таблицы.

После завершения процесса инсталляционный пакет добавляется в список на вкладке **Загружено**. Если процесс загрузки останавливается и статус загрузки меняется на **Принять Лицензионное соглашение**, нажмите на имя инсталляционного пакета и перейдите к следующему шагу инструкции.

Если размер данных, содержащихся в выбранном дистрибутиве, превышает текущее предельное значение, отображается сообщение об ошибке. Вы можете изменить предельное значение и продолжить создание инсталляционного пакета.

6. Во время процесса загрузки некоторых приложений "Лаборатории Касперского" отображается кнопка **Показать Лицензионное соглашение**. Если эта кнопка отображается:
 - a. Нажмите на кнопку **Показать Лицензионное соглашение**, чтобы прочитать Лицензионное соглашение (EULA).
 - b. Прочитайте появившееся на экране Лицензионное соглашение и нажмите на кнопку **Принять**.
Загрузка продолжится после того, как вы примете Лицензионное соглашение. Если вы нажмете на кнопку **Отклонить**, загрузка прекратится.
7. После завершения загрузки нажмите на кнопку **Закрыть**.

Выбранный инсталляционный пакет загружен в папку общего доступа Сервера администрирования, во вложенную папку Packages. После загрузки инсталляционный пакет отображается в списке инсталляционных пакетов.

См. также:

Просмотр экранных уведомлений	1540
Сценарий: развертывание приложений "Лаборатории Касперского"	1084

Изменение ограничения на размер пользовательского инсталляционного пакета

Общий размер данных, распакованных при создании пользовательского инсталляционного пакета, ограничен. Ограничение по умолчанию – 1 ГБ.

Если вы попытаетесь загрузить архивный файл, содержащий данные, превышающие текущее ограничение, появится сообщение об ошибке. Возможно, вам придется увеличить это максимальное значение при создании инсталляционных пакетов из больших дистрибутивов.

► *Чтобы изменить максимальное значение для размера пользовательского инсталляционного пакета:*

1. На устройстве Сервера администрирования запустите командную строку под учетной записью, которая использовалась для установки Сервера администрирования.
2. Измените текущую директорию на папку установки Kaspersky Security Center (обычно это <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).
3. В зависимости от типа установки Сервера администрирования введите одну из следующих команд с правами администратора:

- Обычная локальная установка:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <число_байтов>
```

- Установка на отказоустойчивый кластер Kaspersky Security Center:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <число_байтов>  
--stp klloc
```

- Установка отказоустойчивого кластера Windows Server:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <число_байтов>  
--stp cluster
```

Где <число_байтов> – количество байтов в шестнадцатеричном или десятичном формате.

Например, если требуемое максимальное значение составляет 2 ГБ, вы можете указать десятичное значение 2147483648 или шестнадцатеричное значение 0x80000000. В этом случае для локальной установки Сервера администрирования вы можете использовать следующую команду:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
```

Ограничение на размер пользовательских данных инсталляционного пакета изменено.

Загрузка дистрибутивов для приложений "Лаборатории Касперского"

В Kaspersky Security Center Web Console вы можете загрузить и сохранить дистрибутив для приложений "Лаборатории Касперского". Вы можете использовать дистрибутивы для установки приложений вручную, без использования Kaspersky Security Center.

► *Чтобы загрузить и сохранить дистрибутив приложений "Лаборатории Касперского":*

1. В главном меню перейдите в раздел **Операции** → **Приложения "Лаборатории Касперского"** → **Актуальные версии приложений**.

Откроется список доступных дистрибутивов, плагинов и патчей. Kaspersky Security Center отображает только те элементы, которые совместимы с текущей версией приложения.

2. В списке нажмите на имя дистрибутива, который вы хотите загрузить.

Откроется описание дистрибутива.

3. Ознакомьтесь с информацией и нажмите на кнопку **Загрузить и создать инсталляционный пакет**.

Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Загрузить дистрибутив** отображается кнопка **Загрузить и создать инсталляционный пакет**.

Начинается загрузка инсталляционного пакета на Сервер администрирования.

Выбранный инсталляционный пакет или дистрибутив загружен в папку общего доступа Сервера администрирования, во вложенную папку **Packages**. После загрузки инсталляционный пакет отображается в списке инсталляционных пакетов.

Проверка успешности развертывания Kaspersky Endpoint Security

► Чтобы убедиться, что вы правильно развернули приложения "Лаборатории Касперского", например, Kaspersky Endpoint Security:

1. С помощью Kaspersky Security Center Web Console проверьте наличие:
 - политики Kaspersky Endpoint Security и/или других приложений безопасности, которые вы используете;
 - задач Kaspersky Endpoint Security для Windows: *Быстрый поиск вирусов и Установка обновлений* (если вы используете Kaspersky Endpoint Security для Windows);
 - задач для других приложений безопасности, которые вы используете.
2. Убедитесь, что на управляемых устройствах, для которых была назначена установка:
 - Kaspersky Endpoint Security или другое приложение безопасности "Лаборатории Касперского" установлено;
 - параметры Защита от файловых угроз, Защита от веб-угроз и Защита от почтовых угроз соответствуют политике, созданной для этих устройств;
 - можно вручную запустить и остановить службу Kaspersky Endpoint Security;
 - можно вручную запустить и остановить групповые задачи.

См. также:

Сценарий: развертывание приложений "Лаборатории Касперского"[1084](#)

Создание автономного инсталляционного пакета

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для ручной установки приложений на устройства.

Автономный инсталляционный пакет представляет собой исполняемый файл (installer.exe), который можно разместить на Веб-сервере или в общей папке, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки приложения без участия Kaspersky Security Center. Вы можете создавать автономные инсталляционные пакеты как для приложений "Лаборатории Касперского", так и для приложений сторонних производителей для Windows, macOS и Linux. Чтобы создать автономный инсталляционный пакет для приложений стороннего производителя, необходимо создать пользовательский инсталляционный пакет (см. раздел "Создание пользовательского инсталляционного пакета" на стр. [1093](#)).

Убедитесь, что автономный инсталляционный пакет не доступен для неавторизованных лиц.

► *Чтобы создать автономный инсталляционный пакет:*

1. Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
- В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. В списке инсталляционных пакетов выберите пакет и над списком нажмите на кнопку **Развернуть**.

3. Выберите параметр **С использованием автономного инсталляционного пакета**.

В результате запускается мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. Убедитесь, что включен параметр **Установить Агент администрирования совместно с данным приложением**, если требуется установить Агент администрирования совместно с выбранным приложением.

По умолчанию параметр включен. Рекомендуется включить этот параметр, если вы не уверены, установлен ли на устройстве Агент администрирования. Если Агент администрирования уже установлен на устройстве, после установки автономного инсталляционного пакета с Агентом администрирования, Агент администрирования будет обновлен до более новой версии.

Если вы выключите этот параметр, Агент администрирования не будет установлен на устройство, и устройство не будет управляемым.

Если автономный инсталляционный пакет для выбранного приложения уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вам нужно выбрать одно из следующих действий:

- **Создать автономный инсталляционный пакет.** Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии приложения, и чтобы также остался автономный инсталляционный пакет для предыдущей версии приложения, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.
- **Использовать существующий автономный инсталляционный пакет.** Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.
- **Сформировать заново существующий автономный инсталляционный пакет.** Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этого же приложения еще раз. Автономный инсталляционный пакет размещается в той же папке.

5. На шаге **Перемещение в список управляемых устройств** параметр **Не перемещать устройства** включен по умолчанию. Если вы не хотите перемещать клиентское устройство в какую-либо группу администрирования после установки Агента администрирования, оставьте этот параметр включенным.

Если вы хотите переместить клиентское устройство после установки Агента администрирования, выберите параметр **Перемещать нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентское устройство. По умолчанию устройства перемещаются в группу **Управляемые устройства**.

6. После завершения процесса создания автономного инсталляционного пакета, нажмите на кнопку **Готово**.

Мастер создания автономного инсталляционного пакета закрывается.

Автономный инсталляционный пакет создан и помещен во вложенную папку PkgInst общей папки Сервера администрирования. Вы можете просмотреть список автономных инсталляционных пакетов, нажав на кнопку **Просмотреть список автономных пакетов**, расположенную над списком инсталляционных пакетов.

См. также:

Сценарий: развертывание приложений "Лаборатории Касперского"[1084](#)

Просмотр списка автономных инсталляционных пакетов

Вы можете просмотреть список автономных инсталляционных пакетов и свойства каждого отдельного инсталляционного пакета.

- *Чтобы просмотреть список автономных инсталляционных пакетов для всех инсталляционных пакетов:*

Нажмите на кнопку **Просмотреть список автономных пакетов**.

Свойства автономных инсталляционных пакетов в списке отображаются следующим образом:

- **Имя пакета.** Имя автономного инсталляционного пакета, которое автоматически формируется из имени и версии приложения, включенного в пакет.
- **Название приложения.** Имя приложения, которое включено в автономный инсталляционный пакет.
- **Версия приложения.**
- **Имя инсталляционного пакета Агента администрирования.** Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.
- **Версия Агента администрирования.** Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.
- **Размер.** Размер файла (МБ).
- **Группа.** Имя группы, в которую перемещается клиентское устройство после установки Агента администрирования.
- **Создан.** Дата и время создания автономного инсталляционного пакета.
- **Изменен.** Дата и время изменения автономного инсталляционного пакета.
- **Путь.** Полный путь к папке, в которой находится автономный инсталляционный пакет.
- **Веб-адрес.** Веб-адрес расположения автономного инсталляционного пакета.
- **Хеш файла.** Параметр используется для подтверждения того, что автономный инсталляционный пакет не был изменен третьими лицами, и у пользователя есть тот же файл, который вы создали и передали пользователю.

- Чтобы просмотреть список автономных инсталляционных пакетов для определенного инсталляционного пакета,

выберите инсталляционный пакет в списке и над списком нажмите на кнопку **Просмотреть список автономных пакетов**.

В списке автономных инсталляционных пакетов вы можете сделать следующее:

- Опубликовать автономный инсталляционный пакет на Веб-сервере, с помощью кнопки **Опубликовать**. Опубликованный автономный инсталляционный пакет доступен для загрузки пользователям, которым вы отправили ссылку на автономный инсталляционный пакет.
- Отменить публикацию автономного инсталляционного пакета на Веб-сервере, нажав на кнопку **Отменить публикацию**. Неопубликованный автономный инсталляционный пакет доступен для загрузки только вам и другим администраторам.
- Загрузить автономный инсталляционный пакет на свое устройство, нажав на кнопку **Загрузить**.
- Отправить электронное письмо со ссылкой на автономный инсталляционный пакет, нажав на кнопку **Отправить по электронной почте**.
- Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.

Создание пользовательского инсталляционного пакета

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любое приложение (такое как текстовый редактор) на клиентские устройства, например, с помощью задачи (см. стр. [1172](#));
- создать автономный инсталляционный пакет (см. раздел "Создание автономного инсталляционного пакета" см. стр. [1090](#)).

Пользовательский инсталляционный пакет – это папка с набором файлов. Источником для создания пользовательского инсталляционного пакета является *архивный файл*. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет. Во время создания пользовательского инсталляционного пакета, вы можете указать параметры командной строки, например, для установки приложения в тихом режиме.

Если у вас есть активный лицензионный ключ для функции Системного администрирования, вы можете преобразовать параметры установки по умолчанию для соответствующего пользовательского инсталляционного пакета и использовать значения, рекомендованные специалистами "Лаборатории Касперского". Параметры автоматически преобразуются при создании пользовательского инсталляционного пакета, только если соответствующий исполняемый файл включен в базу данных приложений сторонних производителей "Лаборатории Касперского".

- Чтобы создать пользовательский инсталляционный пакет:

1. Выполните одно из следующих действий:
 - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

- В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет из файла**.

4. Укажите имя инсталляционного пакета и нажмите на кнопку **Обзор**.

Откроется стандартное окно Windows **Открыть**, в котором можно выбрать файл для создания инсталляционного пакета.

5. Выберите архивный файл, расположенный на доступных дисках.

Вы можете загрузить архивный файл формата ZIP, CAB, TAR или TAR.GZ. Создать инсталляционный пакет из файла формата SFX (самораспаковывающийся архив) невозможно.

Если вы хотите, чтобы параметры были преобразованы во время установки пакета, убедитесь, что установлен флажок **Конвертировать параметры на рекомендуемые значения для приложений, распознаваемых Kaspersky Security Center после завершения работы мастера** и нажмите на кнопку **Далее**.

Начнется загрузка файла на Сервер администрирования Kaspersky Security Center.

Если вы включили использование рекомендуемых параметров установки, Kaspersky Security Center 15.1 проверяет, включен ли исполняемый файл в базу данных приложений сторонних производителей "Лаборатории Касперского". Если проверка прошла успешно, вы получите уведомление о том, что файл распознан. Параметры сконвертированы и пользовательский инсталляционный пакет создан. Никаких дальнейших действий не требуется. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

6. Выберите файл (из списка файлов, которые извлечены из выбранного архивного файла) и укажите параметры командной строки исполняемого файла.

Вы можете указать параметры командной строки для установки приложения из инсталляционного пакета в тихом режиме. Указывать параметры командной строки необязательно.

Начнется процесс создания инсталляционного пакета.

В окне мастера отобразится информация о завершении процесса.

Если инсталляционный пакет не создан, отобразится соответствующее сообщение.

7. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования. После загрузки инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов доступных на Сервере администрирования, нажав на имя инсталляционного пакета, вы можете:

- Просмотреть следующие свойства инсталляционного пакета:
 - **Имя**. Название инсталляционного пакета.

- **Источник.** Имя поставщика приложения.
- **Приложение.** Название приложения, упакованного в пользовательский инсталляционный пакет.
- **Версия.** Версия приложения.
- **Язык.** Язык приложения, упакованного в пользовательский инсталляционный пакет.
- **Размер (МБ).** Размер инсталляционного пакета.
- **Операционная система.** Тип операционной системы, для которой предназначен инсталляционный пакет.
- **Создано.** Дата создания инсталляционного пакета.
- **Изменено.** Дата изменения инсталляционного пакета.
- **Тип.** Тип инсталляционного пакета.
- Изменить имя пакета и параметры командной строки. Эта функция доступна только для пакетов, которые не созданы на основе приложений "Лаборатории Касперского".

Если во время конвертации вы установили рекомендуемые значения параметров для создания пользовательского пакета, могут появиться два дополнительных раздела на вкладке **Параметры** в свойствах пользовательского инсталляционного пакета: **Параметры** и **Последовательность установки**.

Разделе **Параметры** содержит следующие свойства, представленные в таблице:

- **Название.** В этом столбце отображается имя, назначенное параметру установки.
- **Тип.** В этом столбце указан тип параметра установки.
- **Значение.** В этом столбце отображается тип данных, определенный параметром установки (логическое значение, путь к файлу, числовое значение, путь или строковое значение).

Раздел **Последовательность установки** содержит таблицу, в которой описаны следующие свойства обновления, включенного в пользовательский инсталляционный пакет:

- **Название.** Название обновления.
- **Описание.** Описание обновления.
- **Источник.** Источник обновления, то есть выпущено ли обновление Microsoft или другим сторонним производителем.
- **Тип.** Тип обновления, то есть предназначено ли обновление для драйвера или приложения.
- **Категория.** Категория служб Windows Server Update Services (WSUS), отображаемая для обновлений Microsoft (Критические обновления, Обновления определений, Драйверы, Пакеты дополнительных компонентов, Обновления системы безопасности, Пакеты обновления, Средства, Накопительные пакеты обновления, Обновления или Обновления с предыдущих версий).
- **Уровень важности по MSRC.** Уровень важности обновления, определенный Microsoft Security Response Center (MSRC).
- **Уровень важности.** Уровень важности обновления определен "Лабораторией Касперского".
- **Уровень важности патча (для патчей приложений "Лаборатории Касперского").** Уровень важности патча, если он предназначен для приложений "Лаборатории Касперского".

- **Статья.** Идентификатор статьи в Базе знаний с описанием обновления.
- **Бюллетень.** Идентификатор бюллетеня безопасности с описанием обновления.
- **Не назначено к установке.** Отображается, имеет ли обновление статус Не назначено к установке.
- **Назначено к установке.** Отображается, имеет ли обновление статус Назначено к установке.
- **Устанавливается.** Отображается, имеет ли обновление статус Устанавливается.
- **Установлено.** Отображается, имеет ли обновление состояние Установлено.
- **Сбой.** Отображается, имеет ли обновление статус Сбой.
- **Restart is required.** Отображается, имеет ли обновление статус Требуется перезагрузка.
- **Зарегистрировано.** Отображается дата и время, когда обновление было зарегистрировано.
- **Устанавливается интерактивно.** Отображается, требуется ли взаимодействие с пользователем во время установки обновления.
- **Отозвано.** Отображается дата и время, когда обновление было отозвано.
- **Статус одобрения обновления.** Отображается, одобрена ли установка обновления.
- **Ревизия.** Отображается номер текущей ревизии обновления.
- **Идентификатор обновления.** Отображается идентификатор обновления.
- **Версия приложения.** Отображается номер версии, до которой будет обновлено приложение.
- **Заменяемое.** Отображаются другие обновления, которые могут заменить это обновление.
- **Заменяющее.** Отображаются другие обновления, которые можно заменить этим обновлением.
- **Требуется принять условия Лицензионного соглашения.** Отображается, требует ли обновление согласие с условиями Лицензионного соглашения.
- **Поставщик.** Отображается имя поставщика обновлений.
- **Семейство приложений.** Отображается имя семейства приложений, к которым относится обновление.
- **Приложение.** Отображается название приложения, которому принадлежит обновление.
- **Язык.** Отображается язык локализации обновления.
- **Не назначено к установке (новая версия).** Отображается, имеет ли обновление статус Не назначено к установке (новая версия).
- **Требуется установки пререквизитов.** Отображается, имеет ли обновление состояние Требуется установки пререквизитов.
- **Режим загрузки.** Отображается режим загрузки обновлений.
- **Является патчем.** Отображается, является ли обновление патчем.
- **Не установлено.** Отображается, имеет ли обновление статус Не установлено.

См. также:

Просмотр экранных уведомлений	1540
Сценарий: развертывание приложений "Лаборатории Касперского"	1084

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

Kaspersky Security Center позволяет вам создавать инсталляционные пакеты для приложений "Лаборатории Касперского" и для приложений сторонних производителей, а также распространять инсталляционные пакеты на клиентские устройства и устанавливать приложения из пакетов. Для оптимизации нагрузки на главном Сервере администрирования вы можете распространять инсталляционные пакеты на подчиненные Серверы администрирования. После этого подчиненные Серверы передают пакеты на клиентские устройства, после чего вы можете выполнять удаленную установку приложений на свои клиентские устройства.

► *Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования:*

1. Убедитесь что подчиненные Серверы администрирования подключены к главному Серверу администрирования.
2. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
Отобразится список задач.
3. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Следуйте далее указаниям мастера.
4. На странице **Параметры новой задачи** в раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**. Затем в раскрывающемся списке **Тип задачи** выберите **Распространить инсталляционный пакет** и укажите имя задачи.
5. На странице **Область действия задачи** выберите устройства, которым назначена задача, одним из следующих способов:
 - Если вы хотите сформировать задачу для всех подчиненных Серверов определенной группы администрирования, выберите эту группу и запустите создание групповой задачи для этой группы.
 - Если вы хотите создать задачу для определенных подчиненных Серверов администрирования, выберите эти Серверы и создайте для них задачу.
6. На странице **Распространяемые инсталляционные пакеты** выберите инсталляционные пакеты, которые необходимо скопировать на подчиненные Серверы администрирования.
7. Укажите учетную запись для запуска задачи *Распространение инсталляционного пакета* под этой учетной записью. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.
8. На странице **Завершение создания задачи**, можно включить параметр **Открыть окно свойств задачи после ее создания**, чтобы открыть окно свойств задачи и изменить параметры задачи (см. раздел "Общие параметры задач" на стр. [1176](#)) по умолчанию. Также можно настроить параметры задачи позже в любое время.
9. Нажмите на кнопку **Готово**.
Задача, созданная для распространения инсталляционных пакетов на подчиненные Серверы администрирования, отображается в списке задач.
10. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи выбранные инсталляционные пакеты скопированы на указанные подчиненные Серверы администрирования.

Установка приложений с помощью задачи удаленной установки

Kaspersky Security Center позволяет удаленно устанавливать приложения на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам (до 1000 устройств), вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования.** В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка.** Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
- **Назначить задачу выборке устройств.** В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать predetermined выборку или вашу собственную выборку.
- **Назначить задачу группе администрирования.** В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

Для правильной работы задачи удаленной установки на устройстве, на котором не установлен Агент администрирования, необходимо открыть порты TCP 139 и 445, UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке.

В этом разделе

Удаленная установка приложений	1098
Установка приложения с помощью групповых политик Active Directory	1104
Установка приложений на подчиненные Серверы администрирования	1105

Удаленная установка приложений

Этот раздел содержит информацию о том, как удаленно установить приложение на устройства в группе администрирования, устройства с определенными IP-адресами или набор управляемых устройств.

► Чтобы установить приложение на выбранные устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи.

3. В поле **Тип задачи** выберите **Удаленная установка приложения**.

4. Выберите один из следующих вариантов:

- **Назначить задачу группе администрирования**

Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- **Задать адреса устройств вручную или импортировать из списка**

Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Задача *Удаленная установка приложения* создана для указанных устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На шаге **Инсталляционные пакеты** укажите следующие параметры:

- В поле **Выбор инсталляционного пакета** выберите инсталляционный пакет приложения, которое требуется установить.
- В блоке параметров **Принудительно загрузить инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

- **С помощью Агента администрирования**

Если флажок установлен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

Если флажок снят, доставка инсталляционных пакетов выполняется средствами Microsoft Windows.

Рекомендуется установить флажок, если задача назначена для устройств с установленными Агентами администрирования.

По умолчанию флажок установлен.

- **Средствами операционной системы с помощью точек распространения**

Если флажок установлен, инсталляционные пакеты передаются на клиентские

устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

- **Средствами операционной системы с помощью Сервера администрирования**

Если флажок установлен, доставка файлов на клиентские устройства будет осуществляться средствами Microsoft Windows с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

По умолчанию флажок установлен.

- В поле **Максимальное количество одновременных загрузок** укажите максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы.
- В поле **Максимальное количество попыток установок** укажите максимально допустимое количество запусков приложения установки.

Если количество попыток, указанное в параметрах задачи, превышено, Kaspersky Security Center больше не запускает приложение установки на устройстве. Чтобы перезапустить задачу *Удаленная установка приложения*, увеличьте значение параметра **Максимальное количество попыток установок** и запустите задачу. Также вы можете создать другую задачу *Удаленная установка приложения*.

- Если вы переносите данные из одного приложения "Лаборатории Касперского" в другое, и ваше текущее приложение защищено паролем, введите пароль в поле **Пароль для удаления приложения "Лаборатории Касперского"**. Обратите внимание, что во время переноса данных ваше текущее приложение "Лаборатории Касперского" будет удалено.

Поле **Пароль для удаления приложения "Лаборатории Касперского"** доступно, только если вы выбрали параметр **С помощью Агента администрирования** в группе параметров **Принудительно загрузить инсталляционный пакет**.

Вы можете использовать пароль удаления только для сценария переноса данных Kaspersky Security для Windows Server в Kaspersky Endpoint Security для Windows при установке Kaspersky Endpoint Security для Windows с помощью задачи *Удаленная установка приложения*. Использование пароля деинсталляции при установке других компонентов может вызвать ошибки установки.

Для успешного завершения сценария переноса данных убедитесь, что выполнены следующие предварительные условия:

- Вы используете Агент администрирования Kaspersky Security Center версии 14.2 для Windows или выше.
- Вы устанавливаете приложение на устройства под управлением Windows.

- Настройте дополнительный параметр:
 - **Не устанавливать приложение, если оно уже установлено**

Если флажок установлен, выбранное приложение не устанавливается заново, если оно уже установлена на клиентском устройстве.

Если флажок снят, приложение будет установлено в любом случае.

По умолчанию флажок установлен.
 - **Предварительно проверять тип операционной системы перед загрузкой**
 - **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

Если флажок установлен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

Флажок доступен если выбран инсталляционный пакет Агента администрирования.

По умолчанию флажок снят.
 - **Предлагать пользователю закрыть работающие приложения**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

- Выберите, на какие устройства вы хотите установить приложение:
 - **Устанавливать на все устройства**

Приложение устанавливается даже на устройства, управляемые другими Серверами администрирования.

По умолчанию этот вариант выбран. Не нужно изменять этот параметр, если в вашей сети есть только один Сервер администрирования.
 - **Устанавливать на устройства, управляемые только этим Сервером администрирования**

Приложение устанавливается только на устройства, которые управляются данным Сервером администрирования. Выберите этот параметр, если в вашей сети установлено больше одного Сервера администрирования и вы хотите избежать конфликтов между ними.
- Укажите, следует ли перемещать устройства в группу администрирования после установки:
 - **Не перемещать устройства**

Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

- **Переместить нераспределенные устройства в выбранную группу (можно выбрать только одну группу)**

Устройства перемещаются в выбранную вами группу администрирования.

Обратите внимание, что по умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

7. На этом шаге мастера укажите, требуется ли перезагрузка устройства при установке приложений:

- **Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

Запущенные приложения могут не позволить перезагрузить клиентское устройство.

Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

8. При необходимости на шаге **Выбор учетных записей для доступа к устройствам** добавьте учетные записи, которые будут использоваться для запуска задачи *Удаленная установка приложения*:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

Если выбран этот вариант, можно указать учетную запись, от имени которой будет запускаться инсталлятор приложения. Учетную запись можно указать в случае если Агент администрирования не установлен на устройствах, для которых назначена задача.

Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

Если ни одна учетная запись не добавлена, задача запускается под той учетной записью, под которой работает служба Сервера администрирования.

9. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

10. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

После выполнения задачи удаленной установки, выбранное приложение устанавливается на указанный набор устройств.

См. также:

Мастер развертывания защиты [1076](#)

Установка приложения с помощью групповых политик Active Directory

Kaspersky Security Center позволяет устанавливать приложения "Лаборатории Касперского" на управляемые устройства с помощью групповых политик Active Directory.

Установка приложений с помощью групповых политик Active Directory возможна только из инсталляционных пакетов, в состав которых входит Агент администрирования.

► Чтобы установить приложение с помощью групповых политик Active Directory:

1. Запустите мастер развертывания защиты. Следуйте далее указаниям мастера.
2. На странице **Параметры задачи удаленной установки** (см. раздел "**Шаг 5. Задание параметров задачи удаленной установки**" на стр. [1079](#)) мастера развертывания защиты выберите параметр **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.
3. На странице **Выбор учетных записей для доступа к устройствам** (см. раздел "**Шаг 9. Выбор учетных записей для доступа к устройствам**" на стр. [1082](#)) выберите параметр **Учетная запись требуется (Агент администрирования не используется)**.
4. Добавьте учетную запись с правами администратора на устройство, на котором установлен Kaspersky Security Center, или учетную запись, входящую в доменную группу Владельцы-создатели групповой политики.
5. Предоставьте разрешения выбранной учетной записи:
 - a. Перейдите в **Панель управления** → **Администрирование** и откройте **Управление групповой политикой**.
 - b. Нажмите на узел с нужным доменом.
 - c. Нажмите на раздел **Делегирование**.
 - d. В раскрывающемся списке **Права доступа** выберите **Связанные объекты GPO**.
 - e. Нажмите на кнопку **Добавить**.
 - f. В открывшемся окне **Выбор пользователя, компьютера или группы** выберите необходимую учетную запись.
 - g. Нажмите на кнопку **ОК** чтобы закрыть окно **Выбор пользователя, компьютера или группы**.
 - h. В списке **Группы и пользователи** выберите только что добавленную учетную запись и нажмите на **Дополнительно** → **Дополнительно**.
 - i. В списке **записей разрешений** дважды нажмите на только что добавленную учетную запись.
 - j. Предоставьте следующие разрешения:
 - **создание объектов группы;**
 - **удаление объектов группы;**
 - **создание объектов контейнера групповой политики;**
 - **удаление объектов контейнера групповой политики.**
 - k. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
6. Задайте другие параметры, следуя инструкциям мастера.

7. Запустите созданную задачу удаленной установки вручную или дождитесь ее запуска по расписанию.

В результате будет запущен следующий механизм удаленной установки:

1. После запуска задачи в каждом домене, которому принадлежат клиентские устройства из набора, будут созданы следующие объекты:
 - Объект групповой политики (Group policy object, GPO) с именем **Kaspersky_AK{GUID}**.
 - Группа безопасности содержит клиентские устройства, на которые распространяется задача. Эта группа безопасности содержит клиентские устройства, на которые распространяется задача. Состав группы безопасности определяет область объекта групповой политики (GPO).
2. Kaspersky Security Center устанавливает выбранные приложения "Лаборатории Касперского" на клиентские устройства осуществляется непосредственно из сетевой папки общего доступа приложения Share. При этом в папке установки Kaspersky Security Center будет создана вложенная вспомогательная папка, содержащая файл с расширением msi для устанавливаемого приложения.
3. При добавлении новых устройств в область действия задачи они будут добавлены в группу безопасности после следующего запуска задачи. Если в расписании задачи выбран флажок **Запускать пропущенные задачи**, устройства будут добавлены в группу безопасности сразу.
4. При удалении устройств из области действия задачи их удаление из группы безопасности произойдет при следующем запуске задачи.
5. При удалении задачи из Active Directory будут удалены объект групповой политики (GPO), ссылка на объект групповой политики (GPO) и группа безопасности, связанная с задачей.

Если вы хотите использовать другую схему установки через Active Directory, вы можете настроить параметры установки вручную. Это может потребоваться, например, в следующих случаях:

- при отсутствии у администратора антивирусной защиты прав на внесение изменений в Active Directory некоторых доменов;
- при необходимости размещения исходного дистрибутива на отдельном сетевом ресурсе;
- для привязки групповой политики к конкретным подразделениям Active Directory.

Доступны следующие варианты использования другой схемы установки через Active Directory:

- Если установку требуется осуществлять непосредственно из папки общего доступа Kaspersky Security Center, в свойствах групповой политики Active Directory следует указать файл с расширением msi, расположенный во вложенной папке ехес в папке инсталляционного пакета нужного приложения.
- Если инсталляционный пакет нужно разместить на другом сетевом ресурсе, следует скопировать в него все содержимое папки ехес, так как помимо файла с расширением msi в ней содержатся конфигурационные файлы, сформированные при создании инсталляционного пакета. Чтобы лицензионный ключ был установлен вместе с приложением, в эту папку следует также скопировать файл ключа.

Установка приложений на подчиненные Серверы администрирования

► *Чтобы установить приложение на подчиненные Серверы администрирования:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.

2. Убедитесь в том, что соответствующий устанавливаемому приложению инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если вы не можете найти инсталляционный пакет ни на одном из подчиненных Серверов, распространите его. Для этого создайте задачу (см. раздел "Создание задачи" на стр. [1174](#)) с типом задачи **Распространение инсталляционного пакета**.

3. Создайте задачу удаленной установки приложения (см. раздел "Удаленная установка приложений" на стр. [1098](#)) на подчиненных Серверах администрирования. Выберите тип задачи **Удаленная установка приложения на подчиненный Сервер администрирования**.

В результате работы мастера создания задачи будет создана задача удаленной установки выбранного приложения на выбранные подчиненные Серверы администрирования.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи удаленной установки выбранное приложение устанавливается на подчиненные Серверы администрирования.

Указание параметров удаленной установки на устройствах под управлением Unix

Когда вы устанавливаете приложение на устройство под управлением Unix с помощью задачи удаленной установки, вы можете указать параметры, специфичные для Unix, для этой задачи. Эти параметры доступны в свойствах задачи после ее создания.

► Чтобы указать параметры, специфичные для Unix, для задачи удаленной установки:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на имя задачи удаленной установки, для которой вы хотите указать параметры, специфичные для Unix.
Откроется окно свойств задачи.
3. Перейдите в раздел **Параметры приложения → Параметры, специфичные для Unix**.
4. Задайте следующие параметры:
 - **Установить пароль для учетной записи root (только для развертывания через SSH)**
 - **Укажите путь к временной папке с правами Выполнение на целевом устройстве (только для развертывания через SSH)**
5. Нажмите на кнопку **Сохранить**.

Указанные параметры задачи сохранены.

См. также:

Общие параметры задач.....	1176
Сценарий: развертывание приложений "Лаборатории Касперского"	1084
Сценарий: мониторинг и отчеты	1466

Управление мобильными устройствами.

Управление защитой мобильными устройствами через Kaspersky Security Center выполняется с помощью компонента Управление мобильными устройствами. Если вы планируете управлять мобильными устройствами, принадлежащими сотрудникам вашей организации, включите и настройте Управление мобильными устройствами.

Управление мобильными устройствами позволяет управлять Android-устройствами сотрудников. Защиту обеспечивает мобильное приложение Kaspersky Endpoint Security для Android, установленное на устройствах. Это мобильное приложение обеспечивает защиту мобильных устройств от веб-угроз, вирусов и других приложений, которые представляют собой угрозы. Для централизованного управления через Kaspersky Security Center Web Console необходимо установить следующие веб-плагины управления на устройство, на котором установлено приложение Kaspersky Security Center Web Console:

- Плагин Kaspersky Security для мобильных устройств
- Плагин Kaspersky Endpoint Security для Android

Информацию о разворачивании защиты и управлении мобильными устройствами см. в справке Kaspersky Security для мобильных устройств <https://support.kaspersky.com/KESMob/10SP4MR3/en-US/216448.htm>.

Изменение параметров Управления мобильными устройствами в Kaspersky Security Center Web Console

► Чтобы изменить параметры Управления мобильными устройствами:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Дополнительные порты**.
3. Измените требуемые параметры:

- **Открыть порт для мобильных устройств**

Если флажок установлен, на Сервере администрирования будет открыт порт для мобильных устройств.

Использование порта для мобильных устройств возможно только в случае, если установлен компонент Поддержка мобильных устройств.

Если флажок снят, порт для мобильных устройств на Сервере администрирования не используется.

По умолчанию флажок снят.

- **Порт для синхронизации мобильных устройств**

Номер порта, по которому осуществляется подключение мобильных устройств к Серверу администрирования. По умолчанию используется порт 13292.

Используется десятичная форма записи.

- **Порт для активации мобильных устройств**

Порт подключения Kaspersky Endpoint Security для Android к серверам активации "Лаборатории Касперского".

По умолчанию используется порт 17100.

4. Нажмите на кнопку **Сохранить**.

Мобильные устройства могут подключаться к Серверу администрирования.

См. также:

Назначение пользователя владельцем устройства [1313](#)

Замещение приложений безопасности сторонних производителей

Для установки приложений безопасности "Лаборатории Касперского" средствами Kaspersky Security Center может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемым приложением. Kaspersky Security Center предоставляет несколько способов удаления приложений сторонних производителей.

Удаление несовместимых приложений с помощью приложения установки

Этот параметр доступен только в Консоли администрирования на основе консоли управления Microsoft Management Console.

Метод удаления несовместимых приложений поддерживается различными типами установки. Перед установкой приложения безопасности несовместимые с ним приложения удаляются автоматически, если в окне свойств инсталляционного пакета приложений безопасности (раздел **Несовместимые приложения**) выбран параметр **Удалять несовместимые приложения автоматически**.

Удаление несовместимых приложений при настройке удаленной установки приложения

Вы можете включить параметр **Удалять несовместимые приложения автоматически** во время настройки удаленной установки приложения безопасности. В Консоли администрирования на основе консоли Microsoft Management Console (MMC) этот параметр доступен в мастере удаленной установки. В приложении Kaspersky Security Center Web Console этот параметр можно найти в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center удаляет несовместимые приложения перед установкой приложения безопасности на управляемое устройство.

Инструкции:

- Консоль администрирования: Удаление несовместимых приложений с помощью мастера удаленной установки.
- Kaspersky Security Center Web Console: Удаление несовместимых приложений перед установкой (см. раздел "Шаг 7. Удаление несовместимых приложений перед установкой" см. стр. [1081](#)).

Удаление несовместимых приложений с помощью отдельной задачи

Для удаления несовместимых приложений используется задача **Удаленная деинсталляция приложений**. Задачу следует запускать на устройствах перед задачей установки приложения безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача **Удаленная деинсталляция приложения**.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор приложения безопасности не может успешно удалить какое-либо из несовместимых приложений.

Инструкции для Консоли администрирования: Создание задачи.

Обнаружение устройств в сети

В этом разделе описаны поиск устройств и опрос сети.

Kaspersky Security Center позволяет искать устройства на основании заданных критериев. Вы можете сохранить результаты поиска в текстовый файл.

Функция поиска позволяет находить следующие устройства:

- управляемые устройства в группах администрирования Сервера администрирования Kaspersky Security Center и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования Kaspersky Security Center и его подчиненных Серверов.

Сценарий: обнаружение сетевых устройств

Вам нужно выполнить поиск устройств перед установкой приложений безопасности. Сервер администрирования получает информацию об обнаруженных устройствах и позволяет управлять устройствами с помощью политик. Регулярные опросы сети необходимы для обновления списка устройств, доступных в сети.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Обнаружение сетевых устройств содержит следующие этапы:

a. Обнаружение устройств

Мастер первоначальной настройки выполняет начальное обнаружение устройств и помогает найти сетевые устройства, такие как компьютеры, планшеты и мобильные телефоны. Вы можете также запустить обнаружение устройств вручную.

b. Настройка расписания опросов

Определите, какой тип опроса вы хотите регулярно использовать. Включите нужные типы опроса и настройте необходимое расписание опроса. Также см. рекомендации по частоте опроса сети.

c. Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)

Новые устройства появляются в сети в результате их обнаружения при опросах сети. Они автоматически попадают в группу **Нераспределенные устройства**. Можно настроить правила перемещения устройств (см. раздел "Создание правил перемещения устройств" на стр. [1197](#)), в соответствии с которыми устройства будут распределены в группу **Управляемые устройства**. Можно также настроить правила хранения.

Если вы пропустили шаг 3, список новых обнаруженных устройств располагается в группе **Нераспределенные устройства**. Вы можете переместить эти устройства в группу **Управляемые устройства** вручную. Если вы вручную переместили устройства в группу **Управляемые устройства**, вы можете проанализировать информацию о каждом из устройств и решить, требуется ли переместить его в группу администрирования и в какую.

Результаты

Завершение сценария дает следующее:

- Сервер администрирования Kaspersky Security Center обнаруживает устройства в сети и предоставляет информацию о них.
- Настроены будущие опросы сети и расписание их запуска.
- Новые обнаруженные устройства распределены в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

Обнаружение устройств

В этом разделе описаны типы обнаружения устройств, доступные в Kaspersky Security Center, а также приведена информация об использовании каждого из них.

Во время регулярных опросов сети Сервер администрирования получает информацию о структуре сети и устройствах в сети. Данные записываются в базу данных Сервера администрирования. Сервер администрирования может проводить следующие типы опросов сети:

- **Опрос сети Windows.** Сервер администрирования может проводить два типа опросов сети Windows: быстрый и полный. При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. При полном опросе с каждого клиентского устройства запрашивается более подробная информация, например, имя операционной системы, IP-адрес, DNS-имя и NetBIOS-имя. По умолчанию включены быстрый и полный опрос. При опросе сети Windows может не удастся обнаружить устройства, например, если роутером или сетевым экраном закрыты порты UDP 137, UDP 138, TCP 139.
- **Опрос контроллеров домена.** Сервер администрирования или точка распространения получает информацию о структуре домена и DNS-именах устройств, входящих в домен. По умолчанию этот тип опроса включен. Рекомендуется использовать опрос контроллеров домена, если все сетевые устройства являются членами домена. Если некоторые из сетевых устройств не включены в домен, эти устройства не могут быть обнаружены с помощью опроса контроллеров домена.
- **Опрос IP-диапазонов.** Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов или NBNS-протоколов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows и/или опрос Active Directory.
- **Опрос Zeroconf.** Точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией <http://www.zeroconf.org/> (далее также *Zeroconf*). По умолчанию этот тип опроса выключен. Вы можете использовать опрос Zeroconf, если точка распространения работает под управлением Linux.

Если вы настроили и включили правила перемещения устройств (см. раздел "Создание правил перемещения устройств" на стр. [1197](#)), новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства**. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Можно изменить параметры обнаружения устройств для каждого типа. Например, может потребоваться изменить расписание опроса или указать, нужно опрашивать весь лес доменов или только определенный домен.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

В этом разделе

Опрос сети Windows	1111
Опрос IP-диапазонов	1113
Добавление и изменение IP-диапазона.....	1115
Опрос Zeroconf	1116
Опрос контроллеров домена	1117
Аутентификация и подключение к контроллеру домена.....	1120
Настройка контроллеров домена Samba.....	1121
Настройка правил хранения для нераспределенных устройств	1121

Опрос сети Windows

Об опросе сети Windows

При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация:

- Имя операционной системы
- IP-адрес
- DNS-имя
- NetBIOS-имя

Как во время быстрого опроса, так и во время полного опроса необходимо:

- наличие открытых портов UDP 137/138, TCP 139, UDP 445, TCP 445;
- SMB-протокол включен;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на Сервере администрирования;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на клиентском устройстве:
 - наличие хотя бы одного устройства, если количество сетевых устройств не превышает 32;

- наличие как минимум одного устройства на каждые 32 сетевых устройства.

Полный опрос сети может быть запущен, только если быстрый опрос был запущен как минимум один раз.

Просмотр и изменение параметров опроса сети Windows

► Чтобы изменить параметры опроса сети Windows:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Windows-домены**.
2. Нажмите на кнопку **Свойства**.
Откроется окно свойств Windows-домена.
3. Включите или выключите опрос Windows сети, используя переключатель **Включить опрос сети Windows**.
4. Настройте расписание опроса. По умолчанию быстрый опрос запускается каждые 15 минут, а полный опрос запускается каждые 60 минут.

Варианты расписания опроса:

- **Каждые N дней**

Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **Каждые N минут**

Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

- **По дням недели**

Опрос выполняется регулярно, в указанные дни недели, в указанное время.

- **Ежемесячно, в указанные дни выбранных недель**

Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр выключен.

5. Сохраните параметры опроса сети Windows.

Параметры сохранены и применены ко всем Windows-доменам и рабочим группам.

Запуск опроса вручную

- Чтобы запустить проверку немедленно,

нажмите на **Начать быстрый опрос** или **Начать полный опрос**.

Когда опрос завершен, вы можете просмотреть список обнаруженных устройств на странице **Windows-домены**, установив флажок рядом с именем домена, а затем нажать на кнопку **Устройства**.

См. также:

Сценарий: обнаружение сетевых устройств [1109](#)

Опрос IP-диапазонов

Исходно Kaspersky Security Center получает IP-диапазоны для опроса из сетевых параметров устройства, на которое он установлен. Если адрес устройства 192.168.0.1, а маска подсети – 255.255.255.0, Kaspersky Security Center автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Kaspersky Security Center выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254.

Не рекомендуется использовать опрос IP-диапазонов, если вы используете опрос сети Windows и/или опрос Active Directory.

Kaspersky Security Center может опрашивать диапазоны IP-адресов путем обратного поиска DNS или по NBNS-протоколу:

- **Обратный поиск DNS.**

Kaspersky Security Center пытается выполнить обратное преобразование имен: для каждого IP-адреса из указанного диапазона выполнить преобразование в DNS-имя с помощью стандартных DNS-запросов. Если данная операция завершается успешно, сервер отправляет запрос `ICMP ECHO REQUEST` (аналог команды ping) на полученное имя. Если устройство отвечает, информация об этом устройстве добавляется в базу данных Kaspersky Security Center. Обратное преобразование имен необходимо для исключения сетевых устройств, которые могут иметь IP-адреса, но не являются компьютерами, таких как сетевые принтеры или роутеры.

Этот способ опроса основывается на правильно настроенной локальной службе DNS. Для его использования должна быть настроена зона обратного просмотра DNS. В сетях, в которых используется Active Directory, такая зона поддерживается автоматически. Но в таких сетях опрос IP-подсети не предоставляет дополнительной информации, помимо информации из опроса Active Directory. Кроме того, администраторы малых сетей часто не выполняют настройку зон обратного просмотра DNS, поскольку это не является необходимым для работы многих сетевых служб. Из-за этих причин опрос IP-подсети по умолчанию отключен.

- **NBNS-протокол.**

Если обратное разрешение имен в вашей сети по каким-либо причинам невозможно, Kaspersky Security Center использует NBNS-протокол для опроса IP-диапазонов. Если запрос к IP-адресу возвращает NetBIOS-имя, информация об этом устройстве добавляется в базу данных Kaspersky Security Center.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Просмотр и изменение параметров опроса IP-диапазонов

► Чтобы просмотреть и изменить параметры опроса IP-диапазонов:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.
2. Нажмите на кнопку **Свойства**.
Откроется окно свойств опроса IP-диапазонов.
3. Включите или выключите опрос IP-диапазонов, используя переключатель **Разрешить опрос**.
4. Настройте расписание опроса. По умолчанию опрос IP-диапазонов запускается каждые 420 минут (семь часов).

При указании интервала опроса убедитесь, что его значение не превышает значения параметра время действия IP-адреса (см. раздел "Добавление и изменение IP-диапазона" см. стр. [1115](#)). Если IP-адрес не подтвержден при опросе в течение времени действия IP-адреса, он автоматически удаляется из результатов опроса. По умолчанию срок существования запросов составляет 24 часа, поскольку динамические IP-адреса, назначенные по протоколу DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации сетевого узла), меняются каждые 24 часа.

Варианты расписания опроса:

- **Каждые N дней**

Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **Каждые N минут**

Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

- **По дням недели**

Опрос выполняется регулярно, в указанные дни недели, в указанное время.

- **Ежемесячно, в указанные дни выбранных недель**

Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего

планового опроса.

По умолчанию параметр выключен.

5. Нажмите на кнопку **Сохранить**.

Параметры будут сохранены и применены ко всем IP-диапазонам.

Запуск опроса вручную

- Чтобы запустить проверку немедленно,

нажмите на кнопку **Начать опрос**.

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Добавление и изменение IP-диапазона

Исходно Kaspersky Security Center получает IP-диапазоны для опроса из сетевых параметров устройства, на которое он установлен. Если адрес устройства 192.168.0.1, а маска подсети – 255.255.255.0, Kaspersky Security Center автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Kaspersky Security Center выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254. Вы можете изменять автоматически определенные IP-диапазоны или добавлять собственные IP-диапазоны.

Вы можете создать диапазон только для IPv4-адресов. Если вы включите опрос Zeroconf (на стр. [1116](#)), Kaspersky Security Center будет опрашивать всю сеть.

- Чтобы добавить новый IP-диапазон:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.
2. Чтобы добавить IP-диапазон, нажмите на кнопку **Добавить**.
3. В открывшемся окне настройте следующие параметры:

- **Имя IP-диапазона**

Имя IP-диапазона. Вы можете указать IP-диапазон по имени, например, 192.168.0.0/24.

- **IP-интервал или адрес и маска подсети**

Задайте IP-диапазон, указав либо начальный и конечный IP-адреса, либо адрес подсети и маску подсети. Можно также выбрать один из существующих диапазонов IP-адресов, нажав на кнопку **Обзор**.

- **Время действия IP-адреса (ч)**

При задании этого параметра убедитесь, что он превышает значение интервала опроса, заданного в расписании опроса (см. раздел "Опрос IP-диапазонов" см. стр. [1113](#)). Если IP-адрес не подтвержден при опросе в течение времени действия IP-адреса, он автоматически удаляется из результатов опроса. По

умолчанию срок существования запросов составляет 24 часа, поскольку динамические IP-адреса, назначенные по протоколу DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации сетевого узла), меняются каждые 24 часа.

4. Выберите **Разрешить опрос IP-диапазона**, если вы хотите опрашивать подсеть или интервал, который вы указали. В противном случае подсеть или интервал, которые вы добавили, не будут опрошены.
5. Нажмите на кнопку **Сохранить**.

IP-диапазон добавлен в список IP-диапазонов.

Вы можете запустить опрос для каждого IP-диапазона в отдельности, используя кнопку **Начать опрос**. После завершения опроса вы можете просмотреть список обнаруженных устройств, нажав на кнопку **Устройства**. По умолчанию срок действия результатов опроса составляет 24 часа, он равен времени действия IP-адреса.

► *Чтобы добавить подсеть в существующий IP-диапазон:*

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.
2. Нажмите на имя IP-диапазона, в который вы хотите добавить подсеть.
3. В появившемся окне нажмите на кнопку **Добавить**.
4. Укажите подсеть либо с помощью ее адреса и маски, либо задав первый и последний IP-адреса в IP-диапазоне. Или добавьте существующую подсеть, нажав на кнопку **Обзор**.
5. Нажмите на кнопку **Сохранить**.

Подсеть добавлена в IP-диапазон.

6. Нажмите на кнопку **Сохранить**.

Параметры IP-диапазона сохранены.

Вы можете добавить столько подсетей, сколько необходимо. Именованные IP-диапазоны не должны пересекаться, но на неименованные подсети внутри IP-диапазонов это ограничение не распространяется. Вы можете включить или отключить опрос независимо для каждого IP-диапазона.

См. также:

Сценарий: обнаружение сетевых устройств [1109](#)

Опрос Zeroconf

Этот тип опроса поддерживается только для точек распространения с операционными системами Linux.

Точка распространения может опрашивать сети, в которых есть устройства с IPv6-адресами. В этом случае IP-диапазоны не указываются, и точка распространения опрашивает всю сеть, используя сеть с нулевой конфигурацией <http://www.zeroconf.org/> (далее также *Zeroconf*). Чтобы начать использовать Zeroconf, вам нужно установить утилиту avahi-browse на точке распространения.

► Чтобы включить опрос IPv6-сети:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.
2. Нажмите на кнопку **Свойства**.
3. В открывшемся окне нажмите на кнопку **Использовать Zeroconf для опроса IPv6-сетей**.

После этого точка распространения начинает опрашивать вашу сеть. В этом случае указанные IP-диапазоны игнорируются.

Опрос контроллеров домена

Kaspersky Security Center поддерживает опрос контроллеров домена Microsoft Active Directory и контроллеров домена Samba.

Kaspersky Security Center позволяет опрашивать контроллер домена Samba только с помощью точки распространения с операционной системой Linux. Для контроллеров домена Samba, в качестве контроллеров домена Active Directory используется Samba 4 (см. раздел "Настройка контроллеров домена Samba" см. стр. [1121](#)).

При опросе контроллера домена Сервер администрирования или точка распространения получают информацию о структуре домена, учетных записях пользователей, группах безопасности и о DNS-именах устройств, входящих в домен.

Рекомендуется использовать опрос контроллеров домена, если все сетевые устройства являются членами домена. Если некоторые из сетевых устройств не включены в домен, эти устройства не могут быть обнаружены с помощью опроса контроллеров домена.

Предварительные требования

Перед опросом контроллера домена убедитесь, что вы разрешаете подключения к контроллеру домена через сетевой экран или прокси-сервер. Также убедитесь, что на контроллере домена включены следующие протоколы:

- Lightweight Directory Access Protocol (LDAP).
- Simple Authentication and Security Layer (SASL).
Этот протокол используется, если соединение с контроллером домена установлено с использованием SASL-аутентификации. Сервер администрирования и точки распространения поддерживают только механизм DIGEST-MD5.
- Lightweight Directory Access Protocol через Secure Sockets Layer (LDAPS)
Этот протокол используется, если вам нужно подключиться к контроллеру домена по зашифрованному подключению.

Убедитесь, что на устройстве контроллеров домена доступны следующие порты:

- 389 для LDAP-протокола и Simple Authentication (включая SASL).
- 636 для LDAPS-протокола.

Опрос контроллеров домена с помощью Сервера администрирования

Вы можете использовать Сервер администрирования для опроса только контроллера домена Microsoft Active Directory.

► Чтобы опросить контроллеры домена с помощью Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Контроллеры доменов**.
2. Нажмите на кнопку **Параметры опроса**.
Откроется окно **Параметры опроса контроллеров домена**.
3. Выберите параметр **Включить опрос контроллеров домена**.
4. В разделе **Дополнительные параметры** укажите область опроса:
 - **Опросить текущий домен**
Выберите этот параметр, чтобы опросить домен, которому принадлежит Kaspersky Security Center.
 - **Опросить весь лес доменов**
Выберите этот параметр, чтобы опросить лес доменов, к которому принадлежит Kaspersky Security Center.
 - **Опросить указанные домены**
Выберите этот параметр, чтобы опросить домен с указанным адресом и учетными данными пользователя.
5. При необходимости настройте расписание опроса. По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

Доступны следующие варианты расписания опроса сети:

- **Каждые N дней**
Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.
По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.
- **Каждые N минут**
Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.
- **По дням недели**
Опрос выполняется регулярно, в указанные дни недели, в указанное время.
- **Ежемесячно, в указанные дни выбранных недель**
Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.
- **Запускать пропущенные задачи**
Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос

сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр выключен.

Если вы измените учетные записи пользователей в группе безопасности домена, эти изменения отобразятся в Kaspersky Security Center через час после опроса контроллеров домена.

6. Нажмите на кнопку **Сохранить**, чтобы применить изменения.
7. Если требуется запустить опрос сети немедленно, нажмите на кнопку **Начать опрос**.

Опрос контроллеров домена с помощью точки распространения

Вы также можете опросить контроллер домена Microsoft Active Directory и контроллер домена Samba с помощью точки распространения. Управляемое устройство с операционной системой Windows или Linux может выступать в роли точки распространения.

Для точки распространения с операционной системой Linux поддерживается опрос контроллеров домена Microsoft Active Directory и контроллеров домена Samba.
Для точки распространения с операционной системой Windows поддерживается только опрос контроллеров домена Microsoft Active Directory.
Опрос с помощью точки распространения с операционной системой Mac не поддерживается.

► Чтобы настроить опрос контроллеров домена с помощью точки распространения:

1. Откройте свойства точки распространения (см. раздел "Назначение точек распространения вручную" см. стр. [1370](#)).
2. Выберите раздел **Опрос контроллеров домена**.
3. Выберите параметр **Включить опрос контроллеров домена**.
4. Выберите контроллеры домена, которые вы хотите опросить.

Если вы используете точку распространения с операционной системой Linux, в разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, а затем укажите адрес и учетные данные пользователя контроллеров домена.

Если вы используете точку распространения с операционной системой Windows, можно выбрать один из следующих вариантов:

- **Опросить текущий домен**
- **Опросить весь лес доменов**
- **Опросить указанные домены**

5. Нажмите на кнопку **Настроить расписание опроса**, чтобы указать параметры расписания опроса при необходимости.

Опрос запускается в соответствии с расписанием. Запуск опроса вручную недоступен.

После завершения опроса в разделе **Контроллеры доменов** отобразится структура домена.

Если вы настроили и включили правила перемещения устройств (см. раздел "Создание правил перемещения устройств" на стр. [1197](#)), новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства**. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Обнаруженные учетные записи пользователей могут быть использованы для доменной аутентификации в Kaspersky Security Center Web Console (см. раздел "Вход в приложение Kaspersky Security Center Web Console и выход из него" на стр. [1006](#)).

См. также:

Аутентификация и подключение к контроллеру домена [1120](#)

Аутентификация и подключение к контроллеру домена

Аутентификация и подключение к контроллеру домена при опросе домена

При опросе контроллера домена (см. раздел "Опрос контроллеров домена" см. стр. [1117](#)) точкой распространения с операционной системой Linux, точка распространения идентифицирует протокол соединения для установления начального соединения с контроллером домена. Этот протокол используется для всех будущих подключений к контроллеру домена. При первоначальном подключении к контроллеру домена вы можете изменить параметры подключения с помощью флагов Агента администрирования `KLNAG_LDAP_TLS_REQCERT` и `KLNAG_LDAP_SSL_CACERT`. Вы можете настроить флаги Агента администрирования с помощью команды `klsclflag`, как описано в этой статье.

Первоначальное подключение к контроллеру домена происходит следующим образом:

1. Точка распространения с операционной системой Linux пытается подключиться к контроллеру домена через LDAPS.

По умолчанию проверка сертификата не требуется. Для флага `KLNAG_LDAP_TLS_REQCERT` установите значение 1, чтобы принудительно выполнить проверку сертификата.

Возможные значения флага `KLNAG_LDAP_TLS_REQCERT`:

- 0 – сертификат запрошен, но если он не предоставлен или проверка сертификата завершилась неудачно, соединение TLS по-прежнему считается успешно созданным (значение по умолчанию).
- 1 – требуется строгая проверка сертификата LDAP-сервера.

По умолчанию, если флаг `KLNAG_LDAP_SSL_CACERT` не задан, для доступа к цепочке сертификатов используется зависящий от операционной системы путь к центру сертификации (CA). Используйте флаг `KLNAG_LDAP_SSL_CACERT`, чтобы указать другой путь.

2. В случае сбоя LDAPS-соединения точка распространения с операционной системой Linux пытается подключиться к контроллеру домена по незашифрованному TCP-соединению с помощью SASL (DIGEST-MD5).

Настройка флагов

Вы можете использовать утилиту `klsclflag` для настройки флагов.

На точке распространения с операционной системой Linux запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. По умолчанию на точке распространения с операционной системой Linux утилита klscflag находится в папке /opt/kaspersky/ksc64/sbin.

Например, следующая команда принудительно проверяет сертификат:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Настройка контроллеров домена Samba

Kaspersky Security Center поддерживает контроллеры домена Linux, работающие только на Samba 4.

Контроллер домена Samba поддерживает те же расширения схемы, что и контроллер домена Microsoft Active Directory. Вы можете включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory, используя расширение схемы Samba 4. Это необязательное действие.

Рекомендуется включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory. Это обеспечит корректное взаимодействие Kaspersky Security Center и контроллером домена Samba.

► Чтобы включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory:

1. Выполните следующую команду, чтобы использовать расширение схемы RFC2307:

```
samba-tool domain provision --use-rfc2307 --interactive
```

2. Включите обновление схемы на контроллере домена Samba. Для этого добавьте следующую строку в файл /etc/samba/smb.conf:

```
dsdb:schema update allowed = true
```

Если обновление схемы завершается с ошибкой, необходимо выполнить полное восстановление контроллера домена, который выполняет роль схемы master.

Если вы хотите правильно опросить контроллер домена Samba, вам нужно указать netbios name и параметры workgroup в файле /etc/samba/smb.conf.

См. также:

Опрос контроллеров домена[1117](#)

Настройка правил хранения для нераспределенных устройств

После того как опрос сети Windows завершен, обнаруженные устройства помещаются в подгруппы группы администрирования Нераспределенные устройства. Эта группа администрирования находится по следующему пути: **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Windows-**

домены. Папка **Windows-домены** является родительской группой. Папка содержит дочерние группы, имена которых соответствуют доменам и рабочим группам, обнаруженным во время опроса. Родительская группа может также содержать группы администрирования мобильных устройств. Вы можете настроить правила хранения нераспределенных устройств для родительской группы администрирования и для каждой дочерней группы. Правила хранения не зависят от параметров обнаружения устройств и работают, даже если обнаружение устройств выключено.

Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования (см. раздел "Шифрование и защита данных." на стр. [1268](#)). Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство (см. раздел "Удаление объектов" см. стр. [858](#)) с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

► *Чтобы настроить правила хранения нераспределенных устройств:*

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Windows-домены**.

2. Выполните одно из следующих действий:

- Чтобы настроить параметры родительской группы, нажмите на кнопку **Свойства**.

Откроется окно свойств Windows-домена.

- Чтобы настроить параметры дочерней группы, нажмите на ее имя.

Откроется окно свойств дочерней группы.

3. Настройте следующие параметры:

- **Удалять устройство из группы, если оно неактивно больше (сут)**

Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. По умолчанию этот параметр распространяется на дочерние группы. Временной интервал, установленный по умолчанию, составляет 7 дней.

По умолчанию параметр включен.

- **Наследовать из родительской группы**

Если этот параметр включен, период хранения для устройств в текущей группе наследуется от родительской группы и не может быть изменен.

Этот параметр доступен только для дочерних групп.

По умолчанию параметр включен.

- **Обеспечить принудительное наследование для дочерних групп**

Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

По умолчанию параметр выключен.

4. Нажмите на кнопку **Принять**.

Ваши изменения сохранены и применены.

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Приложения "Лаборатории Касперского": лицензирование и активация

В этом разделе описаны возможности Kaspersky Security Center по работе с лицензионными ключами управляемых приложений "Лаборатории Касперского".

Kaspersky Security Center позволяет централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

При добавлении лицензионного ключа с помощью Kaspersky Security Center свойства лицензионного ключа сохраняются на Сервере администрирования. На основании этой информации приложение формирует отчет об использовании лицензионных ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах лицензионных ключей. Вы можете настраивать параметры оповещений об использовании лицензионных ключей в составе параметров Сервера администрирования.

См. также:

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console[985](#)

В этом разделе

Лицензирование управляемых приложений[1124](#)

Добавление лицензионного ключа в хранилище Сервера администрирования.[1126](#)

Распространение лицензионного ключа на клиентские устройства.[1127](#)

Автоматическое распространение лицензионного ключа.[1129](#)

Просмотр информации об используемых лицензионных ключах[1131](#)

Удаление лицензионного ключа из хранилища[1132](#)

Отзыв согласия с Лицензионным соглашением[1133](#)

Продление срока действия лицензии приложений "Лаборатории Касперского"[1135](#)

Использование Kaspersky Marketplace для выбора бизнес-решений.....[1136](#)

Лицензирование управляемых приложений

Приложения "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения файла ключа или кода активации к каждому из приложений. Файл ключа или код активации может быть распространен следующими способами:

- с помощью автоматического распространения;
- с помощью инсталляционного пакета управляемого приложения;
- с помощью задачи *Добавление лицензионного ключа* управляемого приложения;
- активация управляемого приложения вручную.

Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. Приложение "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Приложение, для которого вы добавляете лицензионный ключ, определяет, является ли ключ активным или резервным. Определение ключа не зависит от способа, который вы используете для добавления лицензионного ключа.

Автоматическое распространение

Если вы используете разные управляемые приложения и вам важно распространить определенный файл ключ или код активации на устройства, используйте другие способы распространения кода активации или ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Для всех лицензионных ключей установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства**. На устройствах организации установлено приложение безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Приложение определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае невозможно предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

При распространении лицензионного ключа на устройства происходит подсчет устройств для данного лицензионного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение, таким устройствам будет присвоен статус *Критический*.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
 - Добавление лицензионного ключа в хранилище Сервера администрирования.
 - Автоматическое распространение лицензионного ключа.

Или

- Kaspersky Security Center Web Console:
 - Добавление лицензионного ключа в хранилище Сервера администрирования (см. стр. [1126](#)).
 - Автоматическое распространение лицензионного ключа (см. стр. [1129](#)).

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для приложения.
- Виртуальный Сервер администрирования не имеет управляемых устройств.
- Лицензионный ключ уже используется для устройств, управляемых другим виртуальным Сервером администрирования, и достигнуто лицензионное ограничение на количество устройств.

Добавление файла ключа или кода активации в инсталляционный пакет управляемого приложения

Из соображений безопасности не рекомендуется использовать этот параметр. Файл ключа или код активации, добавленный в инсталляционный пакет, может быть скомпрометирован.

В случае установки управляемого приложения с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этого приложения. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

Инструкции:

- Консоль администрирования:
 - Создание инсталляционного пакета.
 - Установка приложений на клиентские устройства.

Или

- Kaspersky Security Center Web Console: Добавление лицензионного ключа в инсталляционный пакет (см. раздел "Шаг 2. Выбор способа распространения файла ключа или кода активации" см. стр. [1078](#)).

Распространение с помощью задачи добавления лицензионного ключа управляемого приложения

В случае использования задачи *Добавление лицензионного ключа* управляемого приложения вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
 - Добавление лицензионного ключа в хранилище Сервера администрирования.
 - Распространение лицензионного ключа на клиентские устройства.

Или

- Kaspersky Security Center Web Console:
 - Добавление лицензионного ключа в хранилище Сервера администрирования (см. стр. [1126](#)).
 - Распространение лицензионного ключа на клиентские устройства (см. стр. [1127](#)).

Добавление кода активации или файла ключа вручную на устройства

Вы можете активировать установленное приложение "Лаборатории Касперского" локально, используя инструменты приложения. Дополнительную информацию см. в документации к установленным приложениям.

См. также

Добавление лицензионного ключа в хранилище Сервера администрирования.	1126
Распространение лицензионного ключа на клиентские устройства.	1127
Автоматическое распространение лицензионного ключа.	1129
Просмотр информации об используемых лицензионных ключах	1131
Удаление лицензионного ключа из хранилища	1132
Отзыв согласия с Лицензионным соглашением	1133
Продление срока действия лицензии приложений "Лаборатории Касперского"	1135
Использование Kaspersky Marketplace для выбора бизнес-решений.....	1136

Добавление лицензионного ключа в хранилище Сервера администрирования.

► Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Добавить**.
3. Выберите то, что вы хотите добавить:
 - **Добавить файл ключа**
Нажмите на кнопку **Выберите файл ключа** и выберите файл .key, который вы хотите добавить.
 - **Ввести код активации**
Укажите код активации в текстовом поле и нажмите на кнопку **Отправить**.
4. Нажмите на кнопку **Закрыть**.

Лицензионный ключ или несколько лицензионных ключей добавлены в хранилище Сервера администрирования.

См. также:

Лицензирование управляемых приложений	1124
Распространение лицензионного ключа на клиентские устройства.	1127
Автоматическое распространение лицензионного ключа.	1129
Просмотр информации об используемых лицензионных ключах	1131
Удаление лицензионного ключа из хранилища	1132
Отзыв согласия с Лицензионным соглашением	1133
Продление срока действия лицензии приложений "Лаборатории Касперского"	1135
Использование Kaspersky Marketplace для выбора бизнес-решений.....	1136
Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985

Распространение лицензионного ключа на клиентские устройства.

Kaspersky Security Center Web Console позволяет распространить лицензионный ключ на клиентские устройства автоматически или с помощью задачи **Активация приложения**. Вы можете использовать задачу для распространения ключей в определенной группе устройств. При распространении лицензионного ключа с помощью задачи учитывается лицензионное ограничение на количество устройств. Используйте автоматическое распространение ключей, чтобы автоматически прекратить распространение лицензионного ключа при достижении лицензионного ограничения.

Если вы включили автоматическое распространение лицензионного ключа (см. раздел "Автоматическое распространение лицензионного ключа." см. стр. [1129](#)), не создавайте задачу **Активация приложения** для распространения этого ключа на клиентские устройства. Иначе нагрузка на Сервер администрирования увеличится из-за частой синхронизации.

Перед распространением добавьте лицензионный ключ в хранилище Сервера администрирования (см. раздел "Добавление лицензионного ключа в хранилище Сервера администрирования." см. стр. [1126](#)).

► *Чтобы распространить лицензионный ключ на клиентские устройства с помощью задачи **Активация приложения**:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится **Мастер создания задачи**. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите добавить лицензионный ключ.
4. В списке **Тип задачи** выберите задачу **Активация приложения**.
5. В поле **Название задачи** укажите название новой задачи.
6. Выберите устройства, которым будет назначена задача (см. раздел "Общие параметры задач" см. стр. [1176](#)).

7. На шаге мастера **Выбор лицензионного ключа** перейдите по ссылке **Добавить ключ**, чтобы добавить лицензионный ключ.
8. В панели добавления ключа добавьте лицензионный ключ, используя один из следующих параметров:

Вам необходимо добавить лицензионный ключ только в том случае, если вы не добавляли его в хранилище Сервера администрирования до создания задачи **Активация приложения**.

- Выберите параметр **Ввести код активации**, чтобы ввести код активации, а затем выполните следующие действия:
 - a. Укажите код активации и нажмите на кнопку **Отправить**.
Информация о лицензионном ключе отображается в панели добавления ключа.
 - b. Нажмите на кнопку **Сохранить**.

Если вы хотите автоматически распространять лицензионный ключ на управляемые устройства, включите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

Панель добавления ключа закрыта.

- Выберите параметр **Добавить файл ключа**, чтобы добавить файл ключа, и выполните следующие действия:
 - a. Нажмите на кнопку **Выберите файл ключа**.
 - b. В открывшемся окне выберите файл ключа и нажмите на кнопку **Открыть**.
Информация о лицензионном ключе отображается в панели добавления лицензионного ключа.
 - c. Нажмите на кнопку **Сохранить**.

Если вы хотите автоматически распространять лицензионный ключ на управляемые устройства, включите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

Панель добавления ключа закрыта.

9. Выберите лицензионный ключ в таблице ключей.
10. На шаге мастера **Информация о лицензии** снимите флажок **Использовать по умолчанию в качестве резервного лицензионного ключа**, если вы хотите заменить действующий активный лицензионный ключ.

Например, это необходимо, когда организация меняется и на устройстве требуется ключ другой организации или если ключ был перевыпущен и срок действия новой лицензии истекает раньше, чем срок действия текущей лицензии. Чтобы избежать ошибок, снимите флажок **Использовать как резервный лицензионный ключ**.

Если вы хотите узнать больше о проблемах, которые могут возникнуть при добавлении лицензионного ключа в Kaspersky Security Center, и способах их решения, обратитесь к Базе знаний Kaspersky Security Center <https://support.kaspersky.com/us/ksc/14.2/troubleshooting/other/16001>.

11. Если на шаге **Завершение создания задачи** включить параметр **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи.

Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже.

12. Нажмите на кнопку **Готово**.

В результате работы мастера задача создана. Если включен параметр **Открыть окно свойств задачи после ее создания**, автоматически откроется окно параметров задачи. В этом окне вы можете указать общие параметры задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)) и изменить параметры, указанные при создании задачи, если это необходимо.

Вы также можете открыть окно свойств задачи, нажав на название созданной задачи в списке задач.

Задача будет создана, настроена и отобразится в списке задач.

13. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

Вы также можете создать расписание запуска задачи на вкладке **Расписание** в окне свойств задачи.

Подробное описание параметров запуска по расписанию см. в общих параметрах задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)).

После завершения задачи, лицензионный ключ распространится на выбранные устройства.

См. также:

Лицензирование управляемых приложений	1124
Добавление лицензионного ключа в хранилище Сервера администрирования.	1126
Автоматическое распространение лицензионного ключа.	1129
Просмотр информации об используемых лицензионных ключах	1131
Удаление лицензионного ключа из хранилища	1132
Отзыв согласия с Лицензионным соглашением	1133
Продление срока действия лицензии приложений "Лаборатории Касперского"	1135
Использование Kaspersky Marketplace для выбора бизнес-решений.....	1136
Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console.....	985

Автоматическое распространение лицензионного ключа.

Kaspersky Security Center позволяет автоматически распространять на управляемые устройства лицензионные ключи, размещенные в хранилище ключей на Сервере администрирования.

► *Чтобы автоматически распространять лицензионный ключ на управляемые устройства:*

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии** **"Лаборатории Касперского"**.
2. Нажмите на имя лицензионного ключа, который вы хотите автоматически распространять на устройства.
3. В открывшемся окне свойств лицензионного ключа установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.
4. Нажмите на кнопку **Сохранить**.

Лицензионный ключ будет автоматически распространяться на те устройства, для которых он подходит.

Распространение лицензионного ключа выполняется средствами Агента администрирования. Задачи распространения резервного лицензионного ключа для приложения при этом не создаются.

При автоматическом распространении лицензионного ключа учитывается лицензионное ограничение на количество устройств. Лицензионное ограничение задано в свойствах лицензионного ключа. Если лицензионное ограничение достигнуто, распространение лицензионного ключа на устройства автоматически прекращается.

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для приложения.
- Виртуальный Сервер администрирования не имеет управляемых устройств.
- Лицензионный ключ уже используется для устройств, управляемых другим виртуальным Сервером администрирования, и достигнуто лицензионное ограничение на количество устройств.

Виртуальный Сервер администрирования автоматически распространяет лицензионные ключи из своего хранилища и из хранилища Сервера администрирования. Рекомендуется:

- Используйте задачу *Добавить лицензионный ключ*, чтобы выбрать лицензионный ключ, который необходимо развернуть на устройствах.
- Не выключайте параметр **Разрешить автоматическое распространение лицензионных ключей этого виртуального Сервера на его устройства** в параметрах виртуального Сервера администрирования. Иначе виртуальный Сервер администрирования не будет распространять лицензионные ключи на устройства, в том числе лицензионные ключи из хранилища Сервера администрирования.

Если установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства** в окне свойств лицензионного ключа, лицензионный ключ будет немедленно распространен в вашей сети. Если вы не выберете этот параметр, вы можете использовать задачу распространения лицензионного ключа позже.

Автоматическое распространение лицензионных ключей, настроенных на главном Сервере администрирования, не включает устройства, управляемые неvirtуальными подчиненными Серверами администрирования.

См. также:

Лицензирование управляемых приложений	1124
Добавление лицензионного ключа в хранилище Сервера администрирования.	1126
Распространение лицензионного ключа на клиентские устройства.	1127
Просмотр информации об используемых лицензионных ключах	1131
Удаление лицензионного ключа из хранилища	1132
Отзыв согласия с Лицензионным соглашением	1133
Продление срока действия лицензии приложений "Лаборатории Касперского"	1135
Использование Kaspersky Marketplace для выбора бизнес-решений.....	1136
Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985

Просмотр информации об используемых лицензионных ключах

- *Чтобы просмотреть список лицензионных ключей, добавленных в хранилище Сервера администрирования:*

В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии** **"Лаборатории Касперского"**.

Отобразится список файлов ключей и кодов активации, добавленных в хранилище Сервера администрирования.

- *Чтобы просмотреть подробную информацию о лицензионном ключе:*

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии** **"Лаборатории Касперского"**.
2. Нажмите на имя требуемого лицензионного ключа.

В открывшемся окне свойств лицензионного ключа вы можете просмотреть:

- На вкладке **Общие** – основную информацию о лицензионном ключе.
- На вкладке **Устройства** – список клиентских устройств, на которых использовался лицензионный ключ для активации установленного приложения "Лаборатории Касперского".

- *Чтобы просмотреть, какие лицензионные ключи распространены на выбранное клиентское устройство:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства выберите вкладку **Приложения**.
4. Нажмите на название приложения, для которого вы хотите просмотреть информацию о распространенном лицензионном ключе.

- В открывшемся окне свойств приложения перейдите на вкладку **Общие** и откройте раздел **Лицензия**.

Отобразится основная информация об активных и резервных лицензионных ключах.

Для определения актуальных параметров лицензионных ключей виртуального Сервера администрирования Сервер администрирования отправляет запрос на серверы активации "Лаборатории Касперского" не реже одного раза в сутки. Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы.

См. также:

Лицензирование управляемых приложений	1124
Добавление лицензионного ключа в хранилище Сервера администрирования.	1126
Распространение лицензионного ключа на клиентские устройства.	1127
Автоматическое распространение лицензионного ключа.	1129
Удаление лицензионного ключа из хранилища	1132
Отзыв согласия с Лицензионным соглашением	1133
Продление срока действия лицензии приложений "Лаборатории Касперского"	1135
Использование Kaspersky Marketplace для выбора бизнес-решений.....	1136

Удаление лицензионного ключа из хранилища

При удалении активного лицензионного ключа для дополнительной возможности Сервера администрирования, например, для возможности Системного администрирования или Управления мобильными устройствами, соответствующая функциональность становится недоступной. Если был добавлен резервный лицензионный ключ, он автоматически становится активным после удаления предыдущего активного лицензионного ключа.

При удалении активного лицензионного ключа, который распространен на управляемые устройства, приложения продолжают работать на управляемых устройствах.

► Чтобы удалить файл ключа или код активации из хранилища Сервера администрирования:

- Убедитесь, что Сервер администрирования не использует файл ключ или код активации, который вы хотите удалить. Если Сервер администрирования использует такой ключ, вы не сможете удалить ключ. Чтобы выполнить проверку:

- В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

- На вкладке **Общие** выберите раздел **Лицензионные ключи**.

- с. Если в открывшемся разделе отображается требуемый файл ключа или код активации, нажмите на кнопку **Удалить активный лицензионный ключ** и подтвердите операцию. После этого Сервер администрирования не использует удаленный лицензионный ключ, ключ остается в хранилище Сервера администрирования. Если требуемый файл ключа или код активации не отображается, Сервер администрирования его не использует.
2. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
3. Выберите нужный файл ключа или код активации и нажмите на кнопку **Удалить**.

Выбранный файл ключа или код активации удален из хранилища.

Можно добавить (см. раздел "Добавление лицензионного ключа в хранилище Сервера администрирования." см. стр. [1126](#)) удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

См. также:

Лицензирование управляемых приложений	1124
Добавление лицензионного ключа в хранилище Сервера администрирования.	1126
Распространение лицензионного ключа на клиентские устройства.	1127
Автоматическое распространение лицензионного ключа.	1129
Просмотр информации об используемых лицензионных ключах	1131
Отзыв согласия с Лицензионным соглашением	1133
Продление срока действия лицензии приложений "Лаборатории Касперского"	1135
Использование Kaspersky Marketplace для выбора бизнес-решений.....	1136

Отзыв согласия с Лицензионным соглашением

Если вы решите прекратить защиту некоторых своих клиентских устройств, вы можете отозвать Лицензионное соглашение для любой управляемого приложения "Лаборатории Касперского". Вам нужно удалить выбранное приложение, прежде чем отзываться его Лицензионное соглашение.

Лицензионные соглашения, принятые на виртуальном Сервере администрирования, можно отозвать на виртуальном Сервере администрирования или на главном Сервере администрирования. Лицензионные соглашения, принятые на главном Сервере администрирования, можно отозвать только на главном Сервере администрирования.

► *Чтобы отозвать Лицензионное соглашение для управляемых приложений "Лаборатории Касперского":*

1. Откройте окно свойств Сервера администрирования и на вкладке **Общие** выберите раздел **Лицензионные соглашения**.
Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов, установке обновлений или развертывании Kaspersky Security для мобильных устройств.
2. В списке выберите Лицензионные соглашения, которые вы хотите отозвать.
Можно просмотреть следующие свойства Лицензионных соглашений:

- Дата принятия Лицензионного соглашения.
 - Имя пользователя, принявшего Лицензионное соглашение.
3. Нажмите на дату принятия любого Лицензионного соглашения, чтобы открыть окно его свойств, в котором отображаются следующие данные:
- Имя пользователя, принявшего Лицензионное соглашение.
 - Дата принятия Лицензионного соглашения.
 - Уникальный идентификатор (UID) Лицензионного соглашения.
 - Полный текст Лицензионного соглашения.
 - Список объектов (инсталляционных пакетов, обновлений, мобильных приложений), связанных с Лицензионным соглашением, и их соответствующие имена и типы.
4. В нижней части окна свойств Лицензионного соглашения нажмите на кнопку **Отозвать Лицензионное соглашение**.

Если существуют какие-либо объекты (инсталляционные пакеты и их соответствующие задачи), которые не позволяют отозвать Лицензионное соглашение, отображается соответствующее уведомление. Вы не можете продолжить отзыв, пока не удалите эти объекты.

В открывшемся окне отобразится сообщение о том, что сначала необходимо удалить приложение "Лаборатории Касперского", которому соответствует это Лицензионное соглашение.

5. Нажмите на кнопку, подтверждающую отзыв лицензии.

Лицензионное соглашение отозвано. Лицензионное соглашение больше не отображается в списке Лицензионных соглашений в разделе **Лицензионные соглашения**. Окно свойств Лицензионного соглашения закрывается; приложение больше не установлено.

См. также:

Лицензирование управляемых приложений	1124
Добавление лицензионного ключа в хранилище Сервера администрирования.	1126
Распространение лицензионного ключа на клиентские устройства.	1127
Автоматическое распространение лицензионного ключа.	1129
Просмотр информации об используемых лицензионных ключах	1131
Удаление лицензионного ключа из хранилища	1132
Продление срока действия лицензии приложений "Лаборатории Касперского"	1135
Использование Kaspersky Marketplace для выбора бизнес-решений.....	1136

Продление срока действия лицензии приложений "Лаборатории Касперского"

Вы можете продлить срок действия лицензии приложений "Лаборатории Касперского", срок действия которой истек или скоро истечет (менее чем через 30 дней).

► Чтобы продлить лицензии срок действия истекает или уже истек:

1. Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
- В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и перейдите по ссылке **Просмотреть лицензии, срок действия которых истек** рядом с уведомлением.

Откроется окно **Лицензии "Лаборатории Касперского"**, в котором вы можете просмотреть и продлить срок действия лицензии.

2. Перейдите по ссылке **Продлить срок действия лицензии** рядом с требуемой лицензией.

Нажимая на ссылку продления срока действия лицензии, вы соглашаетесь передавать в "Лабораторию Касперского" следующие данные Kaspersky Security Center: версию, локализацию, которую вы используете, идентификатор лицензии на программное обеспечение (то есть идентификатор лицензии, которую вы продлеваете), а также то, приобрели ли вы лицензию через компанию-партнера или нет.

3. В открывшемся окне продления срока действия лицензии следуйте инструкциям.

Срок действия лицензии продлен.

В Kaspersky Security Center Web Console уведомления отображаются при приближении истечения срока действия лицензии по следующему расписанию:

- за 30 дней до истечения срока действия;
- за 7 дней до истечения срока действия;
- за 3 дней до истечения срока действия;
- за 24 часа до истечения срока действия;
- когда срок действия лицензии истек.

См. также:

Лицензирование управляемых приложений	1124
Добавление лицензионного ключа в хранилище Сервера администрирования.	1126
Распространение лицензионного ключа на клиентские устройства.	1127
Автоматическое распространение лицензионного ключа.	1129
Просмотр информации об используемых лицензионных ключах	1131
Удаление лицензионного ключа из хранилища	1132
Отзыв согласия с Лицензионным соглашением	1133
Использование Kaspersky Marketplace для выбора бизнес-решений.....	1136

Использование Kaspersky Marketplace для выбора бизнес-решений

Marketplace – раздел главного меню, позволяющий просмотреть весь спектр бизнес-решений "Лаборатории Касперского", выбрать те, которые вам нужны, и перейти к покупке на сайте "Лаборатории Касперского". Вы можете использовать фильтры для просмотра только тех решений, которые соответствуют вашей организации и требованиям вашей системы информационной безопасности. Когда вы выбираете решение, Kaspersky Security Center перенаправляет вас на соответствующую страницу на сайте "Лаборатории Касперского", чтобы вы могли узнать о решении подробнее. Каждая веб-страница позволяет вам перейти к покупке или содержит инструкции по процессу покупки.

В разделе **Marketplace** вы можете фильтровать решения "Лаборатории Касперского" по следующим критериям:

- Количество устройств (конечных точек, серверов и других типов активов), которые вы хотите защитить:
 - 50–250
 - 250–1000
 - Более 1000
- Уровень опытности команды информационной безопасности вашей организации:
 - **Foundations**

Этот уровень типичен для предприятий, в которых есть только ИТ-команда. Максимально возможное количество угроз блокируется автоматически.
 - **Optimum**

Этот уровень типичен для предприятий, у которых есть конкретная функция ИТ-безопасности в ИТ-команде. На этом уровне компаниям требуются решения, которые позволят им противостоять товарным угрозам и угрозам в обход существующих превентивных механизмов.
 - **Expert**

Этот уровень типичен для предприятий со сложной и распределенной ИТ-средой. Группа ИТ-безопасности состоит из опытных специалистов, или в компании есть группа SOC (Security Operations Center). Необходимые решения позволяют компаниям противостоять комплексным угрозам и целевым атакам.

- Типы активов, которые вы хотите защитить:
 - **Конечные точки:** рабочие станции сотрудников, физические и виртуальные машины, встраиваемые системы.
 - **Серверы:** физические и виртуальные серверы.
 - **Cloud:** публичные, частные или гибридные облачные среды; облачные сервисы.
 - **Сеть:** локальная сеть, ИТ-инфраструктура.
 - **Услуга:** услуги, связанные с безопасностью, предоставляемые "Лабораторией Касперского".

► *Чтобы найти и приобрести бизнес-решение "Лабораторией Касперского":*

1. В главном окне приложения перейдите в раздел **Marketplace**.

По умолчанию в разделе отображаются все доступные бизнес-решения "Лаборатории Касперского".

2. Чтобы просмотреть только те решения, которые подходят вашей организации, выберите нужные значения в фильтрах.
3. Нажмите на решение, которое вы хотите приобрести или о котором хотите узнать больше.

Вы будете перенаправлены на веб-страницу решения. Следуйте инструкциям на экране, чтобы перейти к покупке.

См. также:

Лицензирование управляемых приложений	1124
Добавление лицензионного ключа в хранилище Сервера администрирования.	1126
Распространение лицензионного ключа на клиентские устройства.	1127
Автоматическое распространение лицензионного ключа.	1129
Просмотр информации об используемых лицензионных ключах	1131
Удаление лицензионного ключа из хранилища	1132
Отзыв согласия с Лицензионным соглашением	1133
Продление срока действия лицензии приложений "Лаборатории Касперского"	1135

Настройка защиты сети

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства	405
Настройка и распространение политик: подход, ориентированный на пользователя	1143

Сценарий: настройка защиты сети

Мастер первоначальной настройки создает политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться не оптимальными или даже запрещенными в организации. Поэтому рекомендуется настроить эти политики и задачи и создать дополнительные политики и задачи, если это необходимо для вашей сети.

Предварительные требования

Прежде чем приступить, убедитесь, что вы выполнили следующее:

- Установили Сервер администрирования Kaspersky Security Center.
- Установили Kaspersky Security Center Web Console (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)) (если требуется).
- Выполнили основной сценарий установки Kaspersky Security Center.
- Мастер первоначальной настройки (см. раздел "Мастер первоначальной настройки (Kaspersky Security Center Web Console)" см. стр. [1047](#)) завершен или следующие политики и задачи созданы вручную в группе администрирования **Управляемые устройства**:
 - политика Kaspersky Endpoint Security;
 - групповая задача обновления Kaspersky Endpoint Security;
 - политика Агента администрирования;
 - задача *Поиск уязвимостей и требуемых обновлений*.

Настройка защиты сети состоит из следующих этапов:

a. Настройка и распространение политик и профилей политик для приложений "Лаборатории Касперского"

Для настройки и распространения параметров приложений "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью: ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода. Для реализации ориентированного на устройства (см. раздел "Настройка и распространение политик: подход, ориентированный на устройства" см. стр. [405](#)) метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center Web Console. Для реализации ориентированного на пользователей (см. раздел "Настройка и распространение политик: подход, ориентированный на пользователя" см. стр. [1143](#)) метода управления безопасностью подходит только Kaspersky Security Center Web Console.

b. Настройка задач для удаленного управления приложениями "Лаборатории Касперского"

Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

Инструкции:

- Консоль администрирования:
 - Настройка групповой задачи обновления Kaspersky Endpoint Security.
 - Настройка расписания задачи Поиск уязвимостей и требуемых обновлений.

- Kaspersky Security Center Web Console:
 - Настройка групповой задачи обновления Kaspersky Endpoint Security (см. раздел "Ручная настройка групповой задачи обновления Kaspersky Endpoint Security" см. стр. [1167](#)).
 - Параметры задачи поиска уязвимостей и требуемых обновлений (см. стр. [1396](#)).

При необходимости создайте дополнительные задачи управления приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

с. Оценка и ограничение загрузки событий в базу данных

Информация о событиях в работе управляемых приложений передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

Инструкции:

- Консоль администрирования: Настройка максимального количества событий.
- Kaspersky Security Center Web Console: Настройка максимального количества событий (см. раздел "Настройка количества событий в хранилище событий" на стр. [1018](#)).

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке приложений "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- Приложения "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление приложениями осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и приложений "Лаборатории Касперского" (см. раздел "Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"" см. стр. [455](#)).

Подробнее о настройке автоматического ответа на угрозы, обнаруженных Kaspersky Sandbox, см. в онлайн-справке Kaspersky Sandbox 2.0 <https://support.kaspersky.com/KSB/2.0/en-US/189425.htm>.

См. также:

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455

Подходы к управлению безопасностью, ориентированные на устройства и на пользователей

Вы можете управлять параметрами безопасности с позиции функций устройства и с позиции пользовательских ролей. Первый подход называется *управление безопасностью, ориентированное на устройства*, второй подход называется *управление безопасностью, ориентированное на пользователей*. Чтобы применить разные параметры приложений к разным устройствам, вы можете использовать один или

оба типа управления в комбинации. Для реализации ориентированного на устройства метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center Web Console. Для реализации ориентированного на пользователей метода управления безопасностью подходит только Kaspersky Security Center Web Console.

Управление безопасностью, ориентированное на устройства (см. раздел "Настройка и распространение политик: подход, ориентированный на устройства" см. стр. [405](#)), позволяет вам применять различные параметры приложения безопасности к управляемым устройствам в зависимости от особенностей устройства. Например, вы можете применить различные параметры к устройствам, которые размещены в разных группах администрирования. Вы также можете разграничить устройства по использованию этих устройств в Active Directory или по характеристикам аппаратного обеспечения.

Управление безопасностью, ориентированное на пользователя (см. раздел "Настройка и распространение политик: подход, ориентированный на пользователя" см. стр. [1143](#)), позволяет вам применять различные параметры приложений безопасности к различным ролям пользователей. Вы можете создать несколько пользовательских ролей, назначить соответствующую пользовательскую роль каждому пользователю и определить различные параметры приложения для устройств, принадлежащих пользователям с различными ролями. Например, можно применить различные параметры приложений к устройствам бухгалтеров и к устройствам специалистов отдела кадров. В результате внедрения управления безопасностью, ориентированного на пользователей, каждый отдел – отдел бухгалтерии и отдел кадров – получит свою собственную конфигурацию параметров для работы с приложениями "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры приложения могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры приложений для отдельных пользователей. Это может потребоваться, если сотруднику назначена уникальная роль в организации или если требуется проконтролировать проблемы безопасности, связанные с определенным сотрудником. В зависимости от роли этого сотрудника в компании, можно расширить или сократить его права, чтобы изменить параметры приложения. Например, может потребоваться расширить права системного администратора, управляющего клиентскими устройствами в локальном офисе.

Вы также можете комбинировать подходы к управлению безопасностью, ориентированные на пользователей и ориентированные на устройства. Например, можно настроить разные политики для каждой группы администрирования, а затем дополнительно создать профили политик (см. раздел "Профили политик в иерархии политик" см. стр. [1245](#)) для одной или нескольких пользовательских ролей вашей организации. В этом случае политики и профили политик применяются в следующем порядке:

1. Применяются политики, созданные для управления безопасностью, ориентированного на устройства.
2. Они модифицируются профилями политик в соответствии с параметрами профилей политик.
3. Политики модифицируются профилями политик, связанными с ролями пользователей (см. раздел "Связь профилей политики с ролями" см. стр. [1318](#)).

См. также:

Сценарий: настройка защиты сети.....[403](#)

Настройка и распространение политик: подход, ориентированный на устройства

После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center и Kaspersky Security Center Web Console (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)) (если требуется). Если вы установили Kaspersky Security Center Web Console, вам может быть интересно также управление безопасностью (см. раздел "Настройка и распространение политик: подход, ориентированный на пользователя" см. стр. [1143](#)), ориентированное на пользователей, в качестве альтернативы или дополнения к управлению безопасностью, ориентированному на устройства.

Этапы

Сценарий управления приложениями «Лаборатории Касперского», ориентированный на устройства, содержит следующие шаги:

а. Настройка политик приложений

Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики (см. раздел "Создание политики" на стр. [1251](#)) для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для следующих приложений:

- Kaspersky Endpoint Security для Windows – для клиентских устройств с операционной системой Windows.
- Kaspersky Endpoint Security для Linux – для клиентских устройств с операционной системой Linux.

Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать новую политику для этого приложения. Перейдите к настройке политики Kaspersky Endpoint Security вручную.

Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

Инструкции:

- Консоль администрирования: Создание политики.
- Kaspersky Security Center Web Console: Создание политики (на стр. [1251](#)).

б. Создание профилей политики (если требуется)

Если вы хотите, чтобы к устройствам из одной группы администрирования применялись разные параметры политики, создайте профили политики (см. раздел "Профили политик в иерархии политик" см. стр. [1245](#)) для этих устройств. Профиль политики представляет собой именованное

подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве.

Используя условия активации профиля, вы можете применять различные профили политики, например, к устройствам, расположенным в определенном подразделении или группе безопасности Active Directory, имеющим определенную конфигурацию программного обеспечения или имеющим заданные теги (см. раздел "Теги устройств" см. стр. [1231](#)). Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *Windows*, назначить его всем устройствам под управлением операционной системы Windows, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы Windows установленные приложения "Лаборатории Касперского" будут управляться своим профилем политики.

Инструкции:

- Консоль администрирования:
 - Создание профиля политики.
 - Создание правила активации профиля политики.
- Kaspersky Security Center Web Console:
 - Создание профиля политики (см. раздел "Создание профиля политики" см. стр. [1262](#)).
 - Создание правила активации профиля политики (см. раздел "Создание правила активации профиля политики" см. стр. [1264](#)).

с. Распространение политик и профилей политик на управляемые устройства

По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. Также принудительная синхронизация выполняется после создания или изменения политики или профиля политики. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам.

Если вы используете Kaspersky Security Center Web Console, можно проверить, доставлены ли политики и профили политик на устройства. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

Инструкции:

- Консоль администрирования: Принудительная синхронизация.
- Kaspersky Security Center Web Console: Принудительная синхронизация (см. стр. [1376](#)).

Результаты

После завершения сценария, ориентированного на устройства, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики приложений и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

См. также:

О ролях пользователей	1274
Сценарий: настройка защиты сети.....	403

Настройка и распространение политик: подход, ориентированный на пользователя

В этом разделе описывается сценарий, ориентированный на пользователя для централизованной настройке приложений "Лаборатории Касперского", установленных на управляемых устройствах. После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Этот сценарий можно реализовать с помощью Kaspersky Security Center Web Console версии 13 и выше.

Предварительные требования

Убедитесь, что вы успешно установили Сервер администрирования Kaspersky Security Center и Kaspersky Security Center Web Console (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)) и завершили основной сценарий установки. Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на устройства (см. раздел "Настройка и распространение политик: подход, ориентированный на устройства" см. стр. [405](#)) как альтернативу или дополнительную возможность для подхода, ориентированного на пользователя. Узнайте больше о двух подходах к управлению.

Процесс

Сценарий управления приложениями "Лаборатории Касперского", ориентированный на пользователя, содержит следующие шаги:

а. Настройка политик приложений

Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для Kaspersky Endpoint Security. Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать новую политику для этого приложения. Перейдите к настройке политики Kaspersky Endpoint Security вручную (см. раздел "Ручная настройка политики Kaspersky Endpoint Security" см. стр. [1161](#)).

Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики (см. раздел "Блокировка (замок) и заблокированные параметры" на стр. [1242](#)). Остальные незаблокированные параметры будут доступны для

изменения в политике ниже по иерархии. Созданная иерархия политик (см. стр. [1244](#)) позволяет эффективно управлять устройствами в группах администрирования.

Инструкция: Создание политики (на стр. [1251](#)).

b. Укажите пользователей в качестве владельцев устройств

Назначьте управляемым устройствам соответствующие роли.

Инструкция: Назначение пользователя владельцем устройства (см. стр. [1313](#)).

c. Определение пользовательских ролей, типичных для вашей организации

Подумайте о различных видах работ, которые обычно выполняют сотрудники вашей организации. Вам нужно разделить всех сотрудников в соответствии с их ролями. Например, вы можете разделить их по отделам, профессиям или должностям. После этого вам потребуется создать роль пользователя для каждой группы. В этом случае каждая пользовательская роль будет иметь свой собственный профиль политики, содержащий параметры приложения, специфичные для этой роли.

d. Создание пользовательских ролей

Создайте и настройте пользовательскую роль для каждой группы сотрудников, которую вы определили на предыдущем шаге, или используйте предопределенные роли. Роли пользователей содержат набор прав доступа к функциям приложения.

Инструкция: Создание роли пользователя (см. стр. [1316](#)).

e. Определение области для каждой роли пользователя

Для каждой созданной роли пользователя определите пользователей и/или группы безопасности и группы администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Инструкция: Изменение области для роли пользователя (см. стр. [1317](#)).

f. Создание профилей политики

Создайте профиль политики (см. раздел "Профили политик в иерархии политик" см. стр. [1245](#)) для каждой роли пользователя вашей организации. Профили политики определяют, какие параметры должны применяться к приложениям, установленным на устройствах пользователей, в зависимости от роли каждого пользователя.

Инструкция: Создание профиля политики (см. стр. [1262](#)).

g. Связь профиля политики с ролями пользователей

Свяжите профиль политики с ролями пользователей. После чего, профиль политики становится активным для пользователей, которым определена эта роль. Параметры профиля политики, применяются к приложениям "Лаборатории Касперского", установленным на устройствах пользователя.

Инструкция: связь профилей политики с ролями (см. стр. [1318](#)).

h. Распространение политик и профилей политик на управляемые устройства

По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. После завершения синхронизации политики и профили политик доставляются и применяются к установленным приложениям "Лаборатории Касперского".

Вы можете проверить, доставлены ли политики и профили политик на устройство. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

Инструкции: Принудительная синхронизация (см. стр. [1376](#)).

Результаты

После завершения сценария, ориентированного на пользователя, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик и профили политик.

Для нового пользователя вам необходимо создать учетную запись, назначить пользователю одну из созданных пользовательских ролей и назначить устройства пользователю. Политики приложений и профили политик будут автоматически применяться к устройствам этого пользователя.

См. также:

О ролях пользователей	1274
Настройка и распространение политик: подход, ориентированный на устройства	405
Сценарий: настройка защиты сети.....	403

Параметры политики Агента администрирования

► Чтобы настроить параметры политики Агента администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на имя политики Агента администрирования.

Откроется окно свойств политики Агента администрирования.

Обратите внимание, что для устройств под управлением Windows, macOS и Linux, доступны различные параметры (см. раздел "Сравнение параметров политики Агента администрирования по операционным системам" на стр. [1158](#)).

Общие

На этой вкладке можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
 - **Активна**
Если выбран этот вариант, политика становится активной.
По умолчанию выбран этот вариант.
 - **Неактивна**
Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
 - **Наследовать параметры родительской политики**

Если флажок установлен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

По умолчанию флажок установлен.

- **Обеспечить принудительное наследование параметров для дочерних политик**

Если флажок установлен, после применения изменений в политике будут выполнены следующие действия:

- значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
- в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически установлен флажок **Наследовать параметры политики верхнего уровня**.

Когда флажок установлен, значения параметров дочерних политик недоступны для изменения.

По умолчанию флажок снят.

Настройка событий

На этой вкладке можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности в следующих разделах на вкладке **Настройка событий**:

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке типов событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). После того как вы нажмете на тип события, можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений, указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Например, в разделе **Предупреждение**, вы можете настроить тип события **Произошла проблема безопасности**. Такие события могут произойти, например, когда свободное место на диске точки распространения меньше 2 ГБ (для установки приложений и удаленной загрузки обновлений требуется не менее 4 ГБ). Чтобы настроить событие **Произошла проблема безопасности**, нажмите на него и укажите, где хранить произошедшие события и как о них уведомлять.

Если Агент администрирования обнаружил проблему безопасности, вы можете управлять этой проблемой безопасности с помощью параметров управляемого устройства.

Параметры приложения

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Распространять файлы только через точки распространения**

Если флажок установлен, клиентские устройства получают обновления только через агенты обновлений, а не напрямую с серверов обновлений.

Если флажок снят, клиентские устройства могут получать обновления из разных источников: напрямую с серверов обновлений, от главного Сервера администрирования, из локальной или сетевой папки.

По умолчанию флажок снят.

- **Максимальный размер очереди событий (МБ)**

В поле можно указать максимальное место на диске, которое может занимать очередь событий.

По умолчанию указано значение 2 МБ.

- **Приложение может получать расширенные данные политики на устройстве**

Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в приложение безопасности (например, Kaspersky Endpoint Security для Windows). Передаваемая информация отображается в интерфейсе приложения безопасности.

Агент администрирования передает следующую информацию:

- время доставки политики на управляемое устройство;
- имя активной политики и политики для автономных пользователей в момент доставки политики на управляемое устройство;
- имя и полный путь группы администрирования, которой принадлежит управляемое устройство на момент доставки политики на управляемое устройство;
- список активных профилей политики.

Вы можете использовать эту информацию, чтобы обеспечить применение правильной политики к устройству и в целях устранения неполадок. По умолчанию параметр выключен.

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

Если этот параметр включен, после того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

По умолчанию параметр выключен.

- **Использовать пароль деинсталляции**

Если флажок установлен, при нажатии на кнопку **Изменить** можно указать пароль для задачи удаленной деинсталляции Агента администрирования.

По умолчанию флажок снят.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения.

- **Информация об установленных приложениях**

Если флажок установлен, на Сервер администрирования отправляется информация о приложениях, установленных на клиентских устройствах.

По умолчанию флажок установлен.

- **Включить информацию о патчах**

Информация о патчах приложений, установленных на клиентских устройствах, отправляется на Сервер администрирования. Включение этого параметра может увеличить нагрузку на Сервер администрирования и СУБД, а также вызвать увеличение объема базы данных.

По умолчанию параметр включен. Доступен только для Windows.

- **Информация об обновлениях Центра обновления Windows**

Если флажок установлен, на Сервер администрирования отправляется информация об обновлениях Microsoft Windows, которые необходимо установить на клиентских устройствах.

По умолчанию флажок установлен.

- **Информация об уязвимостях в приложениях и соответствующих обновлениях**

Если флажок установлен, на Сервер администрирования отправляется информация об уязвимостях программного обеспечения, обнаруженных на клиентских устройствах.

По умолчанию флажок установлен.

- **Информация о реестре оборудования**

Если флажок установлен, на Сервер администрирования отправляется информация об оборудовании, обнаруженном в результате опроса сети.

По умолчанию флажок установлен.

Обновления и уязвимости в приложениях

В разделе **Обновления и уязвимости в приложениях** можно настроить поиск и распространение обновлений Windows, а также включить проверку исполняемых файлов на наличие уязвимостей.

Параметры раздела **Обновления и уязвимости в приложениях** доступны только для устройств под управлением Windows:

- **Использовать Сервер администрирования в роли WSUS-сервера**

Если флажок установлен, обновления Windows загружаются на Сервер администрирования. Загруженные обновления Сервер администрирования централизованно предоставляет службам Windows Update на клиентских устройствах с помощью Агентов администрирования.

Если флажок снят, Сервер администрирования не используется для загрузки обновлений Windows. В этом случае клиентские устройства получают обновления Windows самостоятельно.

По умолчанию флажок снят.

- **Вы можете ограничить обновления Центра обновления Windows, которые могут устанавливать пользователи на своих устройствах вручную, используя Центр обновления Windows.**

Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, то новый параметр, который вы выбрали под **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

Выберите параметр из раскрывающегося списка:

- **Устанавливать все применимые обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

Выберите этот вариант, если вы не хотите влиять на установку обновлений.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Устанавливать только одобренные обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Запретить устанавливать обновления Центра обновления Windows**

Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

- В блоке параметров **Режим поиска Центра обновления Windows** можно выбрать режим поиска обновлений:

- **Активный**

Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на

клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от агента обновлений Windows.

По умолчанию выбран этот вариант.

- **Пассивный**

Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при последней синхронизации агента обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.

- **Выключен**

Если выбран этот вариант, Сервер администрирования не запрашивает информацию об обновлениях.

- **Проверять исполняемые файлы на наличие уязвимостей при запуске**

Если флажок установлен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

По умолчанию флажок установлен.

Управление перезагрузкой

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если в ходе работы, установки или удаления приложения требуется перезагрузка операционной системы управляемого устройства. Параметры раздела **Управление перезагрузкой** доступны только для устройств под управлением Windows:

- **Не перезагружать операционную систему**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **При необходимости перезагрузить операционную систему автоматически**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос периодически через (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагружать через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

Совместный доступ к рабочему столу Windows

В разделе **Совместный доступ к рабочему столу Windows** можно включить и настроить аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу. Параметры раздела **Совместный доступ к рабочему столу Windows** доступны только для устройств под управлением Windows:

- **Включить аудит**

Если флажок установлен, аудит действий администратора на удаленном устройстве включен. Записи о действиях администратора на удаленном устройстве сохраняются:

- в журнале событий на удаленном устройстве;
- в файле с расширением syslog, который находится в папке установки Агента администрирования на удаленном устройстве;
- в базе событий Kaspersky Security Center.

Аудит действий администратора доступен при выполнении следующих условий:

- есть в наличии действующая лицензия на Системное администрирование;
- у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

Если флажок снят, аудит действий администратора на удаленном устройстве

выключен.

По умолчанию флажок снят.

- **Маски файлов, чтение которых нужно отслеживать**

В списке содержатся маски файлов. Когда аудит включен, приложение отслеживает чтение администратором файлов, соответствующих маскам, и сохраняет информацию о чтении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Маски файлов, изменение которых нужно отслеживать**

В списке содержатся маски файлов на удаленном устройстве. Когда аудит включен, приложение отслеживает изменение администратором файлов, соответствующих маскам, и сохраняет информацию об изменении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Управление патчами и обновлениями

В разделе **Управление патчами и обновлениями** можно настроить получение и распространение обновлений и установку патчей на управляемые устройства:

- **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**

Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Автоматическая установка патчей со статусом *Не определено* доступна для версий Kaspersky Security Center Service Pack 2 и выше.

Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того как администратор изменит их статус на *Одобен*.

По умолчанию флажок установлен.

- **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**

Если флажок установлен, включена офлайн-модель получения обновлений. В этом случае, когда Сервер администрирования получает обновления, он оповещает Агенты администрирования о том, какие обновления потребуются для приложения на клиентских устройствах. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загружает все обновления, обновления становятся доступными для приложений на клиентском устройстве.

Когда управляемое приложение на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него

необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемого приложения, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемому приложению обновления из локального кеша. Соединение с Сервером администрирования при этом может отсутствовать, но оно и не требуется для обновления.

Если флажок снят, офлайн-модель получения обновлений выключена. Обновления распределяются по расписанию задачи обновления.

По умолчанию флажок установлен.

Подключения

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**
- **Профили соединений**
- **Расписание соединений**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер.

- В блоке **Подключиться к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования:

- **Период синхронизации (мин)**

Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (периодический сигнал) равным 15 минут на 10 000 управляемых устройств.

Если установлен период синхронизации меньше 15 минут, то синхронизация выполняется каждые 15 минут. Если период синхронизации установлен на 15 минут или более, синхронизация выполняется с указанным периодом.

- **Сжимать сетевой трафик**

Если флажок установлен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

Нагрузка на центральный процессор клиентского компьютера может возрасти.

По умолчанию флажок установлен.

- Открывать порты Агента администрирования в брандмауэре Microsoft Windows
- **Использовать SSL-соединение**

Если флажок установлен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

По умолчанию флажок установлен.

- **Использовать шлюз соединения точки распространения (при наличии) в параметрах подключения по умолчанию**

Если флажок установлен, то используется шлюз соединений агента обновлений, параметры которого заданы в свойствах группы администрирования.

По умолчанию флажок установлен.

- **Использовать UDP-порт**

Чтобы управляемое устройство подключалось к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **Номер UDP-порта**

В поле можно ввести номер UDP-порта. По умолчанию используется порт 15000.

Используется десятичная форма записи.

Если клиентское устройство работает под управлением операционной системы Windows XP Service Pack 2, встроенный межсетевой экран блокирует UDP-порт с номером 15000. Этот порт требуется открыть вручную.

- **Использовать точку распространения для принудительного подключения к Серверу**

В подразделе **Профили соединений** можно задать параметры сетевого местоположения и включить автономный режим, когда Сервер администрирования недоступен. Параметры раздела **Профили соединений** доступны только для устройств под управлением Windows и macOS:

- **Параметры сетевого местоположения**

Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети.

- **Профили подключения к Серверу администрирования**

В этом разделе можно просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

- подключении клиентского устройства к другой локальной сети;
- отключении устройства от локальной сети организации;
- изменении адреса шлюза соединения или изменении адреса DNS-сервера.
- **Включить автономный режим, когда Сервер администрирования недоступен**

Если флажок установлен, при подключении через этот профиль приложения, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

Если флажок снят, приложения будут использовать активные политики.

По умолчанию флажок снят.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту

администрирования нужно передать данные на Сервер администрирования.

Этот вариант выбран по умолчанию.

- **Подключаться в указанные периоды**

Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Опрос сети точками распространения

В разделе **Опрос сети точками распространения** вы можете настроить автоматический опрос сети. Параметры опроса сети доступны только для устройств под управлением Windows. Вы можете использовать следующие параметры, чтобы включить опрос и настроить его расписание:

- **Сеть Windows**

Если флажок установлен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить период быстрого опроса** и **Настроить период полного опроса**.

Если флажок снят, Сервер администрирования не выполняет опрос сети.

Периодичность опроса сети для версий Агента администрирования версий ниже 10.2 можно настроить в полях **Период запроса информации с доменов, мин** и **Период опроса компьютерной сети, мин**. Поля доступны, если флажок установлен.

По умолчанию флажок установлен.

- **Zeroconf**

- **IP-диапазоны**

Если флажок установлен, Сервер администрирования автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

Если флажок снят, Сервер администрирования не выполняет опрос IP-диапазонов.

Периодичность опроса IP-диапазонов для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если флажок установлен.

По умолчанию флажок снят.

- **Контроллеры доменов**

Параметры сети для точек распространения

В разделе **Параметры сети для точек распространения** вы можете указать параметры доступа к интернету:

- **Использовать прокси-сервер**
- **Адрес**
- **Номер порта**
- **Не использовать прокси-сервер для локальных адресов**

Если флажок установлен, то при подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

По умолчанию флажок снят.

- **Аутентификация на прокси-сервере**

Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

По умолчанию флажок снят.

- **Имя пользователя**
- **Пароль**

Прокси-сервер KSN (точки распространения)

В разделе **Прокси-сервер KSN (точки распространения)** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки Kaspersky Security Network (KSN) запросов от управляемых устройств:

- **Включить прокси-сервер KSN на стороне точки распространения**

Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Пересылать KSN запрос Серверу администрирования**

Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

По умолчанию параметр включен.

- **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к KPSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения.

Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к KPSN.

- **Порт**

Номер TCP-порта, который управляемые устройства используют для подключения к

прокси-серверу KSN. По умолчанию установлен порт 13111.

- **UDP-порт**

Чтобы управляемое устройство подключалось к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

Обновления (точки распространения)

В разделе **Обновления (точки распространения)** вы можете включить функцию загрузки файлов различий, так как точки распространения получают обновления в виде файлов различий с серверов обновлений "Лаборатории Касперского".

Управление учетными записями (только для Linux)

Раздел **Управление учетными записями (только для Linux)** состоит из трех подразделов:

- **Управление пользовательскими сертификатами**
- **Добавление или изменение групп локальных администраторов**
- **Загрузка референсного файла, для защиты файла sudoers на устройстве пользователя от изменений**

В подразделе **Управление пользовательскими сертификатами** вы можете указать, какие корневые сертификаты устанавливать. Эти сертификаты могут использоваться, например, для проверки подлинности веб-сайтов или веб-серверов.

- **Установить корневые сертификаты**
- **Добавить**

В подразделе **Добавление или изменение групп локальных администраторов** вы можете управлять группами локальных администраторов. Эти группы используются, например, при отзыве прав локального администратора (см. раздел "Отзыв прав локального администратора" на стр. [1321](#)). Вы также можете проверить список учетных записей привилегированных пользователей, используя **Отчет о привилегированных пользователях устройств (только для Linux)**.

- **Добавить**
- **Изменить**
- **Удалить**

В подразделе **Загрузка референсного файла, для защиты файла sudoers на устройстве пользователя от изменений** вы можете настроить управление файлом sudoers. Привилегированные группы и пользователи устройства определяются файлом sudoers на устройстве. Файл sudoers находится в папке `/etc/sudoers`. Вы можете загрузить референсный файл sudoers, чтобы защитить файл sudoers от изменений. Это предотвратит нежелательные изменения файла sudoers.

Недопустимый референсный файл sudoers может привести к неисправности устройства пользователя.

- **Контролировать файл sudoers**
- **Референсный файл sudoers**
- **Загрузить**

- Текущий референсный файл sudoers

История ревизий

На этой вкладке вы можете просмотреть список ревизий политики и изменения, для которых был выполнен откат (см. раздел "Откат изменений объекта к предыдущей ревизии" см. стр. [1323](#)).

См. также:

Сценарий: развертывание приложений "Лаборатории Касперского"[1084](#)

Сравнение параметров политики Агента администрирования по операционным системам.....[1158](#)

В этом разделе

Сравнение параметров политики Агента администрирования по операционным системам.....[1158](#)

Сравнение параметров политики Агента администрирования по операционным системам

В таблице ниже показано, какие параметры политики Агента администрирования (см. стр. [1145](#)) можно использовать для настройки Агента администрирования для конкретной операционной системы.

Таблица 87. Параметры политики Агента администрирования: сравнение по операционным системам

Раздел Политики	Windows	macOS	Linux
Общие	✓	✓	✓
Настройка событий	✓	✓	✓
Параметры	✓	✓	Доступны следующие параметры: • Распространять файлы только через точки распространения • Максимальный размер очереди событий (МБ) • Приложение может получать расширенные данные политики на устройстве

Раздел Политики	Windows	macOS	Linux
Хранилища	✓	✓ Параметр Информация о реестре оборудования доступен.	✓ Доступны следующие параметры: • Информация об установленных приложениях • Информация о реестре оборудования
Обновления и уязвимости в приложениях	✓	—	—
Управление перезагрузкой	✓	—	—
Совместный доступ к рабочему столу Windows	✓	—	—
Управление патчами и обновлениями	✓	—	—
Подключения → Сеть	✓	✓	✓ Кроме параметра Открывать порты Агента администрирования в брандмауэре Microsoft Windows .
Подключения → Профили соединений	✓	✓	—
Подключения → Расписание соединений	✓	✓	✓
Опрос сети точками распространения	✓ Доступны только параметры Сеть Windows , IP-диапазоны и Контроллеры доменов .	—	✓ Доступны следующие параметры: • Zeroconf • IP-диапазоны • Контроллеры доменов
Параметры сети для точек распространения	✓	✓	✓

Раздел Политики	Windows	macOS	Linux
Прокси-сервер KSN (точки распространения)	✓	—	✓
Обновления (точки распространения)	✓	—	✓
История ревизий	✓	✓	✓

Включение и выключение режима низкого потребления ресурсов для Агента администрирования

Режим низкого потребления ресурсов позволяет ограничить использование оперативной памяти Агента администрирования, установленного на клиентском устройстве. По умолчанию режим низкого потребления ресурсов выключен.

В режиме низкого потребления ресурсов не выполняются следующие функции:

- Агент администрирования не может быть назначен точкой распространения (вручную или автоматически).
- Агент администрирования не записывает информацию о состоянии Агента администрирования в отдельный текстовый файл.
- Агент администрирования не поддерживает офлайн-модель получения обновлений.
- Следующие компоненты и процессы выключены:
 - Получение информации о сторонних обновлениях и уязвимостях.
 - Запуск прокси-сервера KSN на стороне точки распространения.
 - Загрузка обновлений в хранилище точки распространения.
 - Не использование блокировки DNS-сервера.
 - Получение информации о свободном месте на диске.

Компоненты и процессы возобновляют работу после выключения режима низкого потребления ресурсов.

► Чтобы включить режим низкого потребления ресурсов:

1. Выполните следующую команду в командной строке на клиентском устройстве:

```
C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv
klnagent -n KLNAG_FLAG_TEST_VM_PERF -t d -v 1
```

2. Перезапустите Агент администрирования.

3. Чтобы проверить, включен ли режим низкого потребления ресурсов, в Windows откройте **Просмотр событий** и выберите **Журналы приложений и служб** → **Журнал событий Kaspersky Event Log**.

Убедитесь, что в журнале событий есть такие события, как **Агент администрирования Kaspersky Security Center работает в режиме низкого потребления ресурсов**.

Режим низкого потребления ресурсов включен.

► Чтобы выключить режим низкого потребления ресурсов:

1. Выполните следующую команду в командной строке на клиентском устройстве:

```
C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv  
klnagent -n KLNAG_FLAG_TEST_VM_PERF -t d -v 0
```

2. Перезапустите Агент администрирования.
3. Чтобы проверить, выключен ли режим низкого потребления ресурсов, в Windows откройте **Просмотр событий** и выберите **Журналы приложений и служб** → **Журнал событий Kaspersky Event Log**.

Убедитесь, что последнее событие klnagent не содержит сообщение **Агент администрирования Kaspersky Security Center работает в режиме низкого потребления ресурсов**.

Режим низкого потребления ресурсов выключен.

Также можно включить режим низкого потребления ресурсов удаленно с помощью задачи *Удаленное выполнение скриптов* (см. раздел "Создание задачи Удаленное выполнение скриптов" см. стр. [1188](#)).

Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security. Вы можете выполнить настройку в окне свойств политики. При изменении параметра, нажмите на значок замка справа от соответствующей группы параметров, чтобы применить указанные значения к рабочей станции.

См. также:

Сценарий: настройка защиты сети.....[403](#)

В этом разделе

Настройка Kaspersky Security Network[1162](#)

Проверка списка сетей, которые защищает сетевой экран[1162](#)

Выключение проверки сетевых устройств[1163](#)

Исключение сведений о программном обеспечении из памяти Сервера администрирования[1164](#)

Настройка доступа к интерфейсу Kaspersky Endpoint Security для Windows на рабочих станциях.....[1164](#)

Сохранение важных событий политики в базе данных Сервера администрирования[1165](#)

Настройка Kaspersky Security Network

Kaspersky Security Network (KSN) – инфраструктура облачных служб, обладающая информацией о репутации файлов, веб-ресурсов и программного обеспечения. Kaspersky Security Network позволяет Kaspersky Endpoint Security для Windows быстрее реагировать на различные виды угроз, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Подробнее о Kaspersky Security Network см. документацию Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/KESWin/12.6/en-US/176440.htm>.

► Чтобы задать рекомендуемые параметры KSN:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.
Откроется окно свойств выбранной политики.
3. В окне свойств политики перейдите в раздел **Параметры приложения → Продвинутая защита → Kaspersky Security Network**.
4. Убедитесь, что параметр **Использовать прокси-сервер KSN** включен. Использование этого параметра поможет перераспределить и оптимизировать трафик сети.

Если вы используете Managed Detection and Response <https://support.kaspersky.com/MDR/en-US/>, необходимо включить параметр **Прокси-сервер KSN** (см. раздел "Параметры политики Агента администрирования" см. стр. 1145) для точки распространения и расширенный режим KSN <https://support.kaspersky.com/KESWin/12.6/en-us/126799.htm>.

5. Если служба прокси-сервера KSN недоступна, можно включить использование серверов KSN. Серверы KSN могут располагаться как на стороне "Лаборатории Касперского" (при использовании KPSN), так и у третьих сторон (при использовании KPSN).
6. Нажмите на кнопку **ОК**.
Рекомендованные параметры KSN настроены.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Проверка списка сетей, которые защищает сетевой экран

Убедитесь, что сетевой экран Kaspersky Endpoint Security для Windows защищает все ваши сети. По умолчанию сетевой экран защищает сети со следующими типами подключения:

- **Общедоступная сеть.** Приложения безопасности, сетевые экраны или фильтры не защищают устройства в такой сети.
- **Локальная сеть.** Доступ к файлам и принтерам ограничен для устройств в этой сети.
- **Доверенная сеть.** Устройства в такой сети защищены от атак и несанкционированного доступа к файлам и данным.

Если вы настроили пользовательскую сеть, убедитесь, что сетевой экран защищает ее. Для этого проверьте список сетей в свойствах политики Kaspersky Endpoint Security для Windows. В списке могут отображаться не все сети.

Подробнее о сетевом экране см. документацию Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/KESWin/12.6/en-US/176738.htm>.

► *Чтобы проверить список сетей:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.
Откроется окно свойств выбранной политики.
3. В свойствах политики перейдите в раздел **Параметры приложения → Базовая защита → Сетевой экран**.
4. В блоке **Доступные сети** перейдите по ссылке **Настройки сети**.
Отобразится окно **Сетевые соединения**. В этом окне отобразится список сетей.
5. Если в списке отсутствует сеть, добавьте ее.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Выключение проверки сетевых устройств

Проверка сетевых дисков приложением Kaspersky Endpoint Security для Windows, может оказывать на них значительную нагрузку. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

Вы можете выключить проверку сетевых дисков в свойствах политики Kaspersky Endpoint Security для Windows. Полное описание этих параметров политики приведено в документации Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/KESWin/12.6/en-US/176733.htm>.

► *Чтобы выключить проверку сетевых дисков:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.
Откроется окно свойств выбранной политики.
3. В свойствах политики перейдите в раздел **Параметры приложения → Базовая защита → Защита от файловых угроз**.
4. В блоке **Область защиты**, выключите параметр **Все сетевые диски**.
5. Нажмите на кнопку **ОК**.

Проверка сетевых дисков выключена.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Исключение сведений о программном обеспечении из памяти Сервера администрирования

Рекомендуется, настроить Сервер администрирования так, чтобы он не сохранял информацию о модулях приложений, запущенных на сетевых устройствах. В результате память Сервера администрирования не переполняется.

Вы можете выключить сохранение этой информации в свойствах политики Kaspersky Endpoint Security для Windows.

► *Чтобы выключить сохранение информации об установленных модулях приложений:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.
Откроется окно свойств выбранной политики.
3. В свойствах политики перейдите **Параметры приложения → Общие параметры → Отчеты и хранилища**.
4. В блоке **Информировать Сервер администрирования**, снимите флажок **О запускаемых приложениях**, если он установлен в политике верхнего уровня.

Когда этот флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех модулей приложений на устройствах в сети организации. Указанная информация может занимать значительный объем в базе данных Kaspersky Security Center (десятики гигабайтов).

Информация об установленных модулях приложений больше не сохраняется в базе данных Сервера администрирования.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Настройка доступа к интерфейсу Kaspersky Endpoint Security для Windows на рабочих станциях

Если защитой от угроз в сети организации требуется управлять централизованно через Kaspersky Security Center, укажите параметры интерфейса в свойствах политики Kaspersky Endpoint Security для Windows, как описано ниже. В результате вы предотвратите несанкционированный доступ к Kaspersky Endpoint Security для Windows на рабочих станциях и изменение параметров Kaspersky Endpoint Security для Windows.

Полное описание этих параметров политики приведено в документации Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/KESWin/12.6/en-US/178492.htm>.

► *Чтобы задать рекомендуемые параметры интерфейса:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.
Откроется окно свойств выбранной политики.
3. В свойствах политики перейдите в раздел **Параметры приложения → Общие параметры → Интерфейс**.
4. В блоке **Взаимодействие с пользователем** выберите параметр **Без интерфейса**. Отображение пользовательского интерфейса Kaspersky Endpoint Security для Windows на рабочих станциях будет выключено, и их пользователи не могут изменять параметры Kaspersky Endpoint Security для Windows.
5. В блоке **Включить защиту паролем** включите переключатель. Это снижает риск несанкционированного или непреднамеренного изменения параметров Kaspersky Endpoint Security для Windows на рабочих станциях.

Рекомендуемые параметры интерфейса Kaspersky Endpoint Security для Windows заданы.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Сохранение важных событий политики в базе данных Сервера администрирования

Чтобы избежать переполнения базы данных Сервера администрирования, рекомендуется сохранять в базе данных только важные события.

► *Чтобы настроить регистрацию важных событий в базе данных Сервера администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.
Откроется окно свойств выбранной политики.
3. В окне свойств политики перейдите на вкладку **Настройка событий**.
4. В разделе **Критическое** нажмите на кнопку **Добавить событие** и установите флажок только рядом со следующим событием:
 - *Нарушено Лицензионное соглашение.*
 - *Автозапуск приложения выключен.*
 - *Ошибка активации.*
 - *Обнаружена активная угроза. Требуется запуск процедуры лечения.*
 - *Лечение невозможно.*
 - *Обнаружена ранее открытая опасная ссылка.*

- Процесс прерван.
 - Сетевая активность запрещена.
 - Обнаружена сетевая атака.
 - Запуск приложения запрещен.
 - Доступ запрещен (на основе локальных параметров).
 - Доступ запрещен (KSN).
 - Локальная ошибка обновления.
 - Невозможен запуск двух задач одновременно.
 - Ошибка взаимодействия с Kaspersky Security Center.
 - Обновлено не все компоненты.
 - Ошибка применения правил шифрования/расшифровки файлов.
 - Ошибка активации портативного режима.
 - Ошибка деактивации портативного режима.
 - Не удалось загрузить модуль шифрования.
 - Политика не может быть применена.
 - Ошибка при изменении компонентов приложения.
5. Нажмите на кнопку **ОК**.
6. В разделе **Отказ функционирования** нажмите на кнопку **Добавить событие** и установите флажок только рядом с событием *Неверные параметры задачи. Параметры задачи не применены*.
7. Нажмите на кнопку **ОК**.
8. В разделе **Предупреждение** нажмите на кнопку **Добавить событие** и установите флажки только рядом со следующими событиями:
- Самозащита приложения выключена.
 - Компоненты защиты выключены.
 - Недопустимый резервный ключ.
 - Обнаружено легальное ПО, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или персональным данным (на основе локальных параметров).
 - Обнаружено легальное ПО, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или персональным данным (KSN).
 - Объект удален.
 - Объект вылечен.
 - Пользователь отказался от политики шифрования.
 - Файл восстановлен администратором из карантина на сервере Kaspersky Anti Targeted Attack Platform.
 - Файл помещен администратором на карантин на сервере Kaspersky Anti Targeted Attack Platform.
 - Сообщение администратору о запрете запуска приложения.

- Сообщение администратору о запрете доступа к устройству.
- Сообщение администратору о запрете доступа к веб-странице.

9. Нажмите на кнопку **ОК**.

10. В разделе **Информационное сообщение** нажмите на кнопку **Добавить событие** и установите флажки только рядом со следующими событиями:

- Создана резервная копия объекта.
- Запуск приложения запрещен в тестовом режиме.

11. Нажмите на кнопку **ОК**.

Регистрация важных событий в базе данных Сервера администрирования настроена.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Оптимальный и рекомендуемый вариант расписания для Kaspersky Endpoint Security **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Предоставление автономного доступа к внешнему устройству, заблокированному компонентом Контроль устройств

В компоненте Контроль устройств политики Kaspersky Endpoint Security для Windows вы можете управлять доступом пользователей к внешним устройствам, которые установлены или подключены к клиентскому устройству (например, жестким диском, камерам или модулям Wi-Fi). Это позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных.

Если вам необходимо предоставить временный доступ к внешнему устройству, заблокированному компонентом Контроль устройств, но невозможно добавить устройство в список доверенных устройств, вы можете предоставить временный автономный доступ к внешнему устройству. Автономный доступ означает, что клиентское устройство не имеет доступа к сети.

Вы можете предоставить автономный доступ к внешнему устройству, заблокированному Контролем устройств, только если в параметрах политики Kaspersky Endpoint Security для Windows включен параметр **Разрешать запрашивать временный доступ** в разделе **Параметры приложения** → **Контроль безопасности** → **Контроль устройств**.

Предоставление автономного доступа к внешнему устройству, заблокированному компонентом Контроль устройств, включает в себя следующие этапы:

1. В диалоговом окне Kaspersky Endpoint Security для Windows пользователь устройства, который хочет получить доступ к заблокированному внешнему устройству, формирует файл запроса доступа и отправляет его администратору Kaspersky Security Center.
2. Получив этот запрос, администратор Kaspersky Security Center создает файл ключа доступа и отправляет его пользователю устройства.
3. В диалоговом окне Kaspersky Endpoint Security для Windows пользователь устройства активирует файл ключа доступа и получает временный доступ к внешнему устройству.

► *Чтобы предоставить временный доступ к внешнему устройству, заблокированному компонентом Контроль устройств:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Управляемые устройства**.
Отобразится список управляемых устройств.
2. В этом списке выберите пользовательское устройство, которое запрашивает доступ к внешнему устройству, заблокированному компонентом Контроль устройств.
Можно выбрать только одно устройство.
3. Над списком управляемых устройств нажмите на кнопку с многоточием (**...**) и нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
4. В открывшемся окне **Параметры приложения** в разделе **Контроль устройств** нажмите на кнопку **Обзор**.
5. Выберите файл запроса доступа, который вы получили от пользователя, а затем нажмите на кнопку **Открыть**. Файл должен иметь формат AKEY.
Отображается информация о заблокированном устройстве, к которому пользователь запросил доступ.
6. Укажите значение параметра **Длительность доступа к устройству**.
Этот параметр определяет продолжительность времени, в течение которого вы предоставляете пользователю доступ к заблокированному устройству. Значением по умолчанию является значение, указанное пользователем при создании файла запроса доступа.
7. Укажите значение параметра **Период активации**.
Этот параметр определяет период, в течение которого пользователь может активировать доступ к заблокированному устройству с помощью предоставленного ключа доступа.
8. Нажмите на кнопку **Сохранить**.
Откроется стандартное окно Microsoft Windows **Сохранение ключа доступа**.
9. Выберите папку назначения, в которой вы хотите сохранить файл, содержащий ключ доступа для заблокированного устройства.
10. Нажмите на кнопку **Сохранить**.

В результате, когда вы отправляете пользователю файл ключа доступа и он активирует его в диалоговом окне Kaspersky Endpoint Security для Windows, пользователь получает временный доступ к заблокированному устройству на определенный период.

См. также:

Сценарий: настройка защиты сети.....403

Удаленная деинсталляция приложений или обновлений программного обеспечения

► Чтобы удаленно деинсталлировать приложения или обновления программного обеспечения:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center выберите тип задачи **Удаленная деинсталляция приложения**.
4. Укажите имя задачи, которую вы создаете.
Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\\:|).
5. Выберите устройства, которым будет назначена задача.
6. Выберите, какое приложение вы хотите деинсталлировать, а затем выберите требуемые приложения, обновления или патчи, которые вы хотите удалить:
 - Удалить управляемое приложение
 - Удалить несовместимое приложение
 - Удалить приложение из реестра приложений
 - Удалить указанное обновление приложения, патч или стороннее приложение
7. Укажите, как клиентские устройства будут загружать утилиту удаления:
 - С помощью Агента администрирования
 - Средствами операционной системы с помощью Сервера администрирования
 - Средствами операционной системы с помощью точек распространения
 - Максимальное количество одновременных загрузок
 - Максимальное количество попыток деинсталляции
 - Предварительно проверять тип операционной системы перед загрузкой
 - Использовать пароль деинсталляции
8. Укажите параметры перезагрузки операционной системы:
 - Не перезагружать устройство

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами).

Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

9. Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной деинсталляции:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

10. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
11. Нажмите на кнопку **Готово**.
Задача будет создана и отобразится в списке задач.
12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
13. В окне свойств задачи укажите общие параметры задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)).
14. Нажмите на кнопку **Сохранить**.
15. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной деинсталляции выбранное приложение будет удалено с выбранных устройств.

См. также:

Замещение приложений безопасности сторонних производителей.....	358
Сценарий: настройка защиты сети.....	403

Задачи

В этом разделе описаны задачи, которые используются в Kaspersky Security Center.

В этом разделе

О задачах.....	1172
Область задачи	1173
Создание задачи	1174
Запуск задачи вручную	1175
Просмотр списка задач	1176
Общие параметры задач.....	1176
Экспорт задачи.....	1184
Импорт задачи.....	1184
Запуск мастера изменения паролей задач	1185
Создание задачи Удаленное выполнение скриптов	1188

См. также:

Сценарий: настройка защиты сети	403

О задачах

Kaspersky Security Center управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска **задач**. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения в Kaspersky Security Center Web Console, только если для этого приложения установлен плагин управления на сервере Kaspersky Security Center Web Console.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования, включают:

- автоматическая рассылка отчетов;
- загрузку обновлений в хранилище;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.

На устройствах выполняются следующие типы задач:

- **Локальные задачи** – это задачи, которые выполняются на конкретном устройстве.

Локальные задачи могут быть изменены не только администратором средствами Консоли администрирования, но и пользователем удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- **Групповые задачи** – это задачи, которые выполняются на всех устройствах указанной группы.

Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- **Глобальные задачи** – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в журнале событий операционной системы на каждом устройстве, в журнале событий на Сервере администрирования и в базе данных Сервера администрирования.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

См. также:

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console [985](#)

Область задачи

Область задачи (см. раздел "О задачах" см. стр. [1172](#)) – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Область *локальной задачи* – само устройство.
- Область *задачи Сервера администрирования* – Сервер администрирования.
- Область *групповой задачи* – перечень устройств, входящих в группу.

При создании *глобальной задачи* можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя.

- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования. Данные должны быть занесены в базу при подключении этих устройств или в результате обнаружения устройств.

- Указать выборку устройств.

С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка устройств является наиболее гибким способом задания области действия задачи.

Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запускаются на устройствах, не имеющих связи с Сервером администрирования. Задачи, область действия которых задается другим способом, запускаются непосредственно на устройствах и не зависят от наличия связи устройства с Сервером администрирования.

Задачи для выборок устройств будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования. Задачи, область действия которых задается другим способом, запускаются по локальному времени устройства.

См. также:

Задачи.....[1172](#)

Создание задачи

► Чтобы создать задачу:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Следуйте шагам мастера.
3. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
4. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

► *Чтобы создать задачу, назначенную выбранным устройствам:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

Отобразится список управляемых устройств.

2. В списке управляемых устройств установите флажки рядом с устройствами, для которых нужно запустить задачу. Вы можете использовать функции поиска и фильтрации, чтобы найти необходимые устройства.

3. Нажмите на кнопку **Запустить задачу** и выберите **Создание задачи**.

Запустится мастер создания задачи.

На первом шаге мастера вы можете удалить устройства, выбранные для включения в область действия задачи. Следуйте инструкциям мастера.

4. Нажмите на кнопку **Готово**.

Задача создана для выбранных устройств.

См. также:

Задачи.....	1172
Общие параметры задач.....	1176
Сценарий: развертывание приложений "Лаборатории Касперского"	1084
Сценарий: мониторинг и отчеты.....	1466
Сценарий: настройка защиты сети.....	403

Запуск задачи вручную

Приложение запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время из списка задач. Также можно выбрать устройства в списке **Управляемые устройства** и запустить для них существующую задачу.

► *Чтобы запустить задачу вручную:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.
3. Нажмите на кнопку **Запустить**.

Задача будет запущена. Вы можете проверить статус задачи в столбце **Статус** или нажав на кнопку **Результат выполнения**.

См. также:

О задачах.....	1172
Создание задачи.....	1174
Общие параметры задач.....	1176
Сценарий: настройка защиты сети.....	403

Просмотр списка задач

Вы можете просмотреть список задач, созданных в Kaspersky Security Center.

► Чтобы просмотреть список задач,

в главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям приложений, к которыми они относятся. Например, задача Удаленная деинсталляция приложения относится к Серверу администрирования, а задача Поиск уязвимостей и требуемых обновлений относится к Агенту администрирования.

► Чтобы просмотреть свойства задачи,

нажмите на имя задачи.

Окно свойств задачи отображается с несколькими именными вкладками (см. раздел "Общие параметры задач" см. стр. [1176](#)). Например, **Тип задачи** отображается на вкладке **Общие**, а расписание задачи на вкладке **Расписание**.

См. также:

Задачи.....	1172
Сценарий: настройка защиты сети.....	403
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....	529

Общие параметры задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:
 - Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения

операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

- Параметры расписания задачи:

- **Параметры Запуск задачи:**

- **Каждый N час**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрываемым списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрываемым списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрываемым списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим

Ежемесячно, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При загрузке обновлений в хранилище**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При загрузке обновлений в хранилище**, задача будет запускаться после загрузки обновлений в хранилище.

- **При обнаружении вирусной атаки**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрывающимся списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрывающимся списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.

- **Результат выполнения.** В раскрывающемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- Окно Выбор устройств, которым будет назначена задача:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**

В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **Задать адреса устройств вручную или импортировать из списка**

Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- Параметры учетной записи:

- **Учетная запись по умолчанию.**

Задача будет запускаться под той же учетной записью, под которой была установлено и запущено приложение, выполняющее эту задачу.

По умолчанию выбран этот вариант.

- **Задать учетную запись**

Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

- **Учетная запись**

Учетная запись, от имени которой будет запускаться задача.

- **Пароль.**

Пароль учетной записи, от имени которой будет запускаться задача.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:
 - **Распространить на подгруппы**
 - **Распространить на подчиненные и виртуальные Серверы администрирования**
- Дополнительные параметры расписания:
 - **Включать устройства перед запуском задачи функцией Wake-on-LAN за**

Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройства после выполнения задачи**. Параметр находится в этом же окне.

По умолчанию параметр выключен.

- **Выключать устройства после выполнения задачи**

Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

По умолчанию параметр выключен.

- **Остановить, если задача выполняется дольше**

По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:
 - Блок **Сохранять информацию о результатах**:
 - **Хранить в базе данных Сервера администрирования в течение (сут)**

События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

По умолчанию параметр включен.

- **Хранить в журнале событий ОС на устройстве**

События приложения, связанные с выполнением задачи, хранятся локально в журнале событий Windows каждого клиентского устройства.

По умолчанию параметр выключен.

- **Хранить в журнале событий ОС на Сервере администрирования**

События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в журнале событий Windows операционной системы Сервера администрирования.

По умолчанию параметр выключен.

- **Сохранять все события**

Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

- **Сохранять события, связанные с ходом выполнения задачи**

Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением задачи.

- **Сохранять только результат выполнения задачи**

Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

- **Уведомлять администратора о результатах**

Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

По умолчанию отключены все способы уведомлений.

- **Уведомлять только об ошибках**

Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

По умолчанию параметр включен.

- Параметры безопасности.
- Параметры области действия задачи.

В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

- **Устройства**

Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

- **Выборка устройств**

Вы можете изменить выборку устройств, к которым применяется задача.

- **Исключения из области действия задачи**

Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**

См. также:

Сценарий: развертывание приложений "Лаборатории Касперского"	1084
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455

Экспорт задачи

Kaspersky Security Center позволяет сохранить задачу и ее параметры в файл KLT. Вы можете использовать файл KLT для импорта сохраненной задачи (см. раздел "Импорт задачи" см. стр. [1184](#)) как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

► Чтобы экспортировать задачу:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Установите флажок рядом с задачей, которую вы хотите экспортировать.
Невозможно экспортировать несколько задач одновременно. Если вы выберете несколько задач, кнопка **Экспортировать** будет неактивна. Задачи Сервера администрирования также недоступны для экспорта.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя файла задачи и путь. Нажмите на кнопку **Сохранить**.
Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл задачи автоматически сохраняется в папку **Загрузки**.

Импорт задачи

Kaspersky Security Center позволяет импортировать задачу из файла KLT. Файл KLT содержит экспортированную задачу (см. раздел "Экспорт задачи" см. стр. [1184](#)) и ее параметры.

► Чтобы импортировать задачу:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Импортировать**.
3. Нажмите на кнопку **Обзор**, чтобы выбрать файл задачи, которую вы хотите импортировать.
4. В открывшемся окне укажите путь к файлу KLT задачи и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл задачи.
Начнется обработка задачи.
5. После того как задача будет успешно обработана, выберите устройства, которым вы хотите назначить задачу. Для этого выберите один из следующих параметров:
 - **Назначить задачу группе администрирования**
Задача назначается устройствам, входящим в ранее созданную группу

администрирования. Можно указать одну из существующих групп или создать новую группу.

Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- **Задать адреса устройств вручную или импортировать из списка**

Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

6. Укажите область действия задачи.

7. Нажмите на кнопку **Завершить**, чтобы завершить задачу импорта.

Появится уведомление с результатами импорта. Если задача успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств задачи.

После успешного импорта задача отображается в списке задач. Параметры задачи и расписание также импортируются. Задача будет запущена в соответствии с расписанием.

Если имя новой импортированной задачи идентично имени существующей задачи, имя импортированной задачи расширяется с помощью окончания вида (**<порядковый номер>**), например: **(1)**, **(2)**.

Запуск мастера изменения паролей задач

Для не-локальной задачи можно указать учетную запись, с правами которой будет запускаться задача. Учетную запись можно указать во время создания задачи или в свойствах существующей задачи. Если указанная учетная запись используется в соответствии с правилами безопасности, установленными в организации, эти правила могут требовать периодического изменения пароля учетной записи. После истечения срока действия пароля учетной записи и задания нового пароля, задача не будет запускаться до тех пор, пока вы не укажете новый действующий пароль в свойствах задачи.

Мастер изменения паролей задач позволяет автоматически заменить старый пароль на новый во всех задачах, в которых указана учетная запись. Вы также можете изменить пароль вручную в свойствах каждой задачи.

► Чтобы запустить мастер изменения паролей задач

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
 2. Нажмите на кнопку **Управление учетными данными учетной записи для запуска задач**.
- Следуйте далее указаниям мастера.

См. также:

О задачах.....	1172
Область задачи.....	1173
Просмотр списка задач	1176
В этом разделе	
Шаг 1. Выбор учетных данных.....	1186
Шаг 2. Выбор выполняемого действия	1187
Шаг 3. Просмотр результатов	1187

Шаг 1. Выбор учетных данных

Укажите новые учетные данные, действующие в вашей системе (например, в Active Directory). При переходе на следующий шаг мастера, Kaspersky Security Center проверяет, совпадает ли имя указанной учетной записи с именем учетной записи в свойствах каждой не-локальной задачи. Если имена учетных записей совпадают, пароль в свойствах задачи автоматически меняется на новый.

Чтобы указать новую учетную запись, выберите один из вариантов:

- **Использовать текущую учетную запись**

Мастер использует имя учетной записи, под которой вы в настоящее время вошли в Kaspersky Security Center Web Console. Вручную укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

- **Указать другую учетную запись**

Укажите имя учетной записи, под которой должны запускаться задачи. Укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

При заполнении поля **Предыдущий пароль (необязательно; если вы хотите заменить его на текущий)** Kaspersky Security Center заменит пароль только для тех задач, для которых совпадают значения имени и старого пароля. Замена выполняется автоматически. Во всех остальных случаях необходимо выбрать действие, выполняемое на следующем шаге мастера.

См. также:

Запуск мастера изменения паролей задач.....	1185
Шаг 2. Выбор выполняемого действия	1187
Шаг 3. Просмотр результатов	1187

Шаг 2. Выбор выполняемого действия

Если на первом шаге мастера вы не указали предыдущий пароль или если указанный старый пароль не соответствует паролям, которые указаны в свойствах задач, необходимо выбрать действие, выполняемое с этими задачами.

► Чтобы выбрать действие с задачей:

1. Установите флажок около задачи, с которой вы хотите выполнить действие.
2. Выполните одно из следующих действий:
 - Чтобы удалить пароль в свойствах задачи, нажмите **Удалить учетные данные**.
Задача переключена на запуск под учетной записью по умолчанию.
 - Чтобы заменить пароль на новый, нажмите **Принудительно изменить пароль, даже если старый пароль неверен или не указан**.
 - Чтобы отменить изменение пароля, нажмите **Действие не выбрано**.

Выбранные действия применяются после перехода к следующему шагу мастера.

См. также:

Запуск мастера изменения паролей задач.....	1185
Шаг 1. Выбор учетных данных	1186
Шаг 3. Просмотр результатов	1187

Шаг 3. Просмотр результатов

На последнем шаге мастера просмотрите результаты для каждой из обнаруженных задач. Для завершения работы мастера нажмите на кнопку **Готово**.

См. также:

Запуск мастера изменения паролей задач.....	1185
Шаг 1. Выбор учетных данных	1186
Шаг 2. Выбор выполняемого действия	1187

Создание задачи Удаленное выполнение скриптов

Вы можете создать задачу *Удаленное выполнение скриптов* для выполнения инсталляционного пакета на клиентском устройстве и удаленной установки приложения.

Инсталляционный пакет содержит ZIP-архив с набором скриптов для выполнения на клиентских устройствах, а также файл manifest.json. Подробнее о создании этого типа инсталляционного пакета см. статью (см. раздел "Создание инсталляционного пакета на основе манифест-файла" см. стр. [1190](#)).

Эту задачу нужно запускать только на устройствах с Агентом администрирования для Linux.

► Чтобы запустить задачу *Удаленное выполнение скриптов*:

1. Перейдите в **Мастер создания задачи** и выберите тип задачи **Удаленное выполнение скриптов**.
2. Введите имя задачи и выберите устройства, которым будет назначена задача. Нажмите на кнопку **Далее**.
3. Выберите инсталляционный пакет на основе ZIP-архива с файлом manifest.json для удаленного выполнения.

Если вы не хотите повторно запускать задачу на устройствах, на которых она уже была выполнена, включите параметр **Не запускать эту задачу на устройствах, на которых она уже была выполнена**.

4. Выберите учетную запись для запуска задачи.

Если вы выберете учетную запись по умолчанию, то задачу будет выполнять Агент администрирования (учетная запись root).

При запуске задачи *Удаленное выполнение скриптов* вы не можете изменить учетную запись, которая назначена задаче. Чтобы изменить учетную запись, которой назначена задача, остановите задачу в параметрах задачи и создайте задачу снова с требуемой учетной записью.

5. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
6. Нажмите на кнопку **Готово**.

Задача *Удаленное выполнение скриптов* создана и отображается в списке задач.

После получения данных из задачи *Удаленное выполнение скриптов*, Агент администрирования ограничивает доступ к полученным данным для всех пользователей, кроме администратора и пользователя, указанного в параметрах задачи.

В этом разделе

Удаленная установка приложений на устройства с помощью задачи Удаленное выполнение скриптов	1189
Configuring notifications and monitoring for the Execute scripts remotely task	1189
Подготовка архива для задачи Удаленное выполнение скриптов	1190
Создание инсталляционного пакета на основе манифест-файла	1190

Удаленная установка приложений на устройства с помощью задачи Удаленное выполнение скриптов

Задачу *Удаленное выполнение скриптов* можно использовать для удаленной установки приложения на клиентское устройство с помощью создания пользовательского инсталляционного пакета.

О том, как подготовить архив для этой задачи, см. статью (см. раздел "Подготовка архива для задачи Удаленное выполнение скриптов" см. стр. [1190](#)).

Чтобы создать инсталляционный пакет для удаленной установки приложения на клиентское устройство, в архив, который вы хотите загрузить для этой задачи, должны быть включены следующие файлы:

- `<название_пакета>.deb`
- `install.sh`
- `manifest.json`

При запуске задачи *Удаленное выполнение скриптов* Агент администрирования загрузит инсталляционный пакет с приложением на клиентское устройство. Когда клиентское устройство получает инсталляционный пакет, Агент администрирования на этом устройстве анализирует файл `manifest.json` и определяет порядок выполнения скриптов и действий в зависимости от результата, а затем начинает выполнение.

После завершения задачи *Удаленное выполнение скриптов* приложение будет установлено на клиентском устройстве.

Настройка уведомлений и мониторинга для задачи Удаленное выполнение скриптов

Вы можете настроить мониторинг, поведение при сохранении событий и уведомления для задачи *Удаленное выполнение скриптов*.

► Чтобы просмотреть статус задачи Удаленное выполнение скриптов:

1. В главном окне приложения перейдите в раздел **Устройства** → **Задачи**.
Отобразится список задач.
2. Выберите задачу и нажмите на **История устройства**.
Отображается ход выполнения задачи.

► Чтобы настроить поведение при сохранении событий:

1. В списке задач нажмите на имя задачи и перейдите на вкладку **Параметры**.
2. В разделе **Уведомления** нажмите на кнопку **Параметры**.

3. Выберите один из следующих вариантов поведения приложения после выполнения задачи:

- **Сохранять все события.**
- **Сохранять события, связанные с ходом выполнения задачи.**
- **Сохранять только результат выполнения задачи.**

События сохраняются в разделе **История устройства** и **Хранилище событий**.

По умолчанию сохраняются только результаты выполнения задачи.

Если вы выберете **Сохранять все события**, сохраняются только результаты выполнения задачи.

4. Если вы хотите сохранить события в базе данных Сервера администрирования, в журнале событий на Сервере администрирования или на устройстве, включите соответствующий параметр.

Подготовка архива для задачи **Удаленное выполнение скриптов**

Архив для задачи **Удаленное выполнение скриптов** на основе файла manifest.json должен соответствовать следующим требованиям:

- Формат архива: ZIP.
- Общий размер: не более 1 ГБ.
- Количество файлов и папок в архиве не ограничено.
- Манифест-файл архива должен соответствовать приведенной ниже схеме и называться manifest.json. Схема проверяется только во время выполнения задачи на устройстве.

Схема JSON манифест-файла и описание массивов

Пример манифест-файла

- Архив должен иметь следующую структуру:

```
manifest.json
```

```
<файл1>
```

```
<файл2>
```

```
<папка1>/<файл3>
```

```
<папка2>/<папка3>/<файл4>
```

```
...
```

```
<файлX>
```

manifest.json – это манифест-файл задачи.

<файл1>, ..., <файлX> – это набор файлов со скриптами, которые нужно выполнить.

Создание инсталляционного пакета на основе манифест-файла

► Чтобы создать инсталляционный пакет на основе манифест-файла:

1. Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
- В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите параметр **Создать инсталляционный пакет для задачи "Удаленное выполнение скриптов" на основе архива ZIP с файлом manifest.json**.

4. Укажите имя инсталляционного пакета и нажмите на кнопку **Обзор**.

Откроется стандартное окно Windows **Открыть**, в котором можно выбрать файл для создания инсталляционного пакета.

5. Выберите архивный файл, расположенный на доступных дисках. О том, как подготовить архив для этой задачи, см. статью (см. раздел "Подготовка архива для задачи Удаленное выполнение скриптов" см. стр. [1190](#)).

Файл начнет загружаться на Сервер администрирования Kaspersky Security Center.

Начнется процесс создания инсталляционного пакета.

В окне мастера отобразится информация о завершении процесса.

Если инсталляционный пакет не создан, отобразится соответствующее сообщение.

6. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования. После загрузки инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов доступных на Сервере администрирования, нажав на имя инсталляционного пакета, вы можете:

- Просмотреть следующие свойства инсталляционного пакета:
 - **Имя.** Название инсталляционного пакета.
 - **Источник.** Имя поставщика приложения.
 - **Версия.** Версия приложения.
 - **Создано.** Дата создания инсталляционного пакета.
 - **Изменено.** Дата изменения инсталляционного пакета.
 - **Путь.** Путь к пользовательскому инсталляционному пакету на Сервере администрирования.
- Изменить имя пакета и параметры командной строки. Эта функция доступна только для пакетов, которые не созданы на основе приложений "Лаборатории Касперского".

Управление клиентскими устройствами

Kaspersky Security Center позволяет управлять клиентскими устройствами:

- Просматривать параметры (см. раздел "Параметры управляемого устройства" см. стр. [1193](#)) и статусы (см. раздел "О статусах устройства" см. стр. [1205](#)) управляемых устройств, в том числе кластеров и массивов серверов (см. раздел "О кластерах и массивах серверов" см. стр. [1202](#)).
- Настраивать точки распространения (см. раздел "Настройка точек распространения и шлюзов соединений" см. стр. [685](#)).
- Управлять задачами.

Группы администрирования можно использовать для объединения клиентских устройств в набор, которым можно управлять как единым целым. Клиентское устройство может быть включено только в одну группу администрирования. Устройства могут быть автоматически отнесены к группе на основе **Условия правила**:

- Создание правил перемещения устройств (см. стр. [1197](#)).
- Копирование правил перемещения устройств (на стр. [1198](#)).
- Условия для правила перемещения устройств (на стр. [1199](#)).

Вы можете использовать выборки устройств, чтобы для фильтровать устройства по условию. Вы также можете назначать теги устройствам (см. раздел "Теги устройств" см. стр. [1231](#)) для создания выборок устройств, поиска устройств и распределения устройств между группами администрирования.

В этом разделе

Параметры управляемого устройства	1193
Создание групп администрирования ..	1194
Добавление устройств в состав группы администрирования вручную.....	1195
Перемещение устройств или кластеров в состав группы администрирования вручную.....	1196
Создание правил перемещения устройств	1197
Копирование правил перемещения устройств	1198
Условия для правила перемещения устройств	1199
О кластерах и массивах серверов	1202
Свойства кластеров или массивов серверов	1203
Просмотр и настройка действий, когда устройство неактивно	1203
О статусах устройства	1205
Настройка переключения статусов устройств	766
Удаленное подключение к рабочему столу клиентского устройства	1214
Подключение к устройствам с помощью совместного доступа к рабочему столу Windows	1216
Выборки устройств.....	1218
Теги устройств.....	1231

См. также:

Сценарий: настройка защиты сети	403

Параметры управляемого устройства

► Чтобы просмотреть параметры управляемого устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
Отобразится список управляемых устройств.
2. В списке управляемых устройств перейдите по ссылке с названием нужного устройства.
Откроется окно свойств выбранного устройства.

В верхней части окна свойств отображаются следующие вкладки, на которых представлены основные группы параметров:

- **Общие**
- **Приложения**
- **Действующие политики и профили политик**
- **Задачи**
- **События**
- **Проблемы безопасности**
- **Теги**
- **Дополнительно**

Создание групп администрирования

Сразу после установки Kaspersky Security Center в иерархии групп администрирования присутствует только одна группа администрирования – **Управляемые устройства**. При создании иерархии групп администрирования в состав папки **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы (см. рисунок ниже).

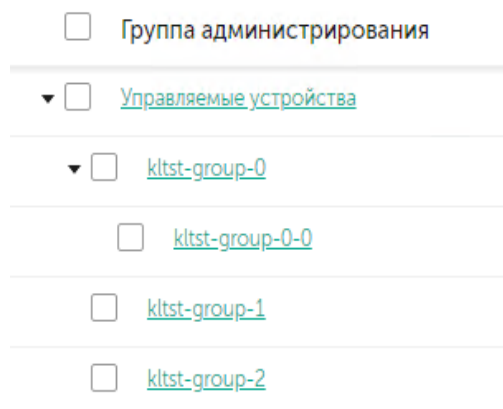


Рисунок 16. Просмотр иерархии групп администрирования

► Чтобы создать группу администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Иерархия групп**.
2. В структуре группы администрирования выберите группу администрирования, в состав которой должна входить новая группа администрирования.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне **Имя новой группы администрирования** введите имя группы и нажмите на кнопку **Добавить**.

В результате в иерархии групп администрирования появится новая группа администрирования с заданным именем.

Приложение позволяет создавать структуру групп администрирования на основе структуры Active Directory или структуры доменной сети. Также вы можете создавать структуру групп из текстового файла.

► *Чтобы создать структуру групп администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.
2. Нажмите на кнопку **Импортировать**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Добавление устройств в состав группы администрирования вручную

Вы можете перемещать устройства в группы администрирования автоматически, создавая правила перемещения устройств, или вручную, перемещая устройства из одной группы администрирования в другую, или добавляя устройства в выбранную группу администрирования. В этом разделе описано, как вручную добавить устройства в группу администрирования.

► *Чтобы вручную добавить одно или несколько устройств в состав выбранной группы администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Перейдите по ссылке **Текущий путь**: [<текущий_путь>](#) над списком.
3. В открывшемся окне выберите группу администрирования, в которую требуется добавить устройства.
4. Нажмите на кнопку **Добавить устройства**.

В результате запустится мастер перемещения устройств.

5. Составьте список устройств, которые вы хотите добавить в группу администрирования.

В список устройств могут быть добавлены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

Выберите, как вы хотите добавить устройства в список:

- Нажмите на кнопку **Добавить устройства** и укажите устройства одним из следующих способов:
 - Выберите устройства из списка устройств, обнаруженных Сервером администрирования.
 - Укажите IP-адреса устройств или IP-диапазон.
 - Укажите NetBIOS-имя устройства или DNS-имя.

Поле с именем устройства не должно содержать пробелы, а также следующие запрещенные символы: \ / * ; : ` ~ ! @ # \$ ^ & () = + [] { } | , < > %

- Нажмите на кнопку **Импортировать устройства из файла**, чтобы импортировать список устройств из файла формата TXT. Каждый адрес устройства (или имя устройства) должен располагаться в отдельной строке.

Файл не должен содержать пробелы, а также следующие запрещенные символы: \ / * ; : ` ~ ! @ # \$ ^ & () = + [] { } | , < > %

6. Просмотрите список устройств, которые будут добавлены в группу администрирования. Вы можете редактировать список, добавляя или удаляя устройства.
7. После того как вы убедитесь, что в списке нет ошибок, нажмите на кнопку **Далее**.

Мастер обрабатывает список устройств и отображает результат. После завершения работы мастера выбранные устройства включаются в состав группы администрирования и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

См. также:

Создание правил перемещения устройств	1197
Перемещение устройств или кластеров в состав группы администрирования вручную	1196

Перемещение устройств или кластеров в состав группы администрирования вручную

Устройства можно перемещать из одной группы администрирования в другую или из группы нераспределенных устройств в группу администрирования.

Также можно перемещать кластеры или массивы серверов (см. раздел "О кластерах и массивах серверов" см. стр. [1202](#)) из одной группы администрирования в другую. При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования. При выборе одного узла кластера на вкладке **Устройства**, кнопка **Переместить в группу** становится недоступной.

► Чтобы переместить одно или несколько устройств или кластеров в состав выбранной группы администрирования:

1. Откройте группу администрирования, в которую вы хотите переместить устройства. Для этого выполните одно из следующих действий:
 - Чтобы открыть группу администрирования, в главном меню перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**, перейдите по ссылке в поле **Текущий путь** и в открывшейся слева панели выберите группу администрирования.
 - Чтобы открыть группу **Нераспределенные устройства**, в главном меню перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
2. Если группа администрирования содержит кластеры или массивы серверов, раздел **Управляемые устройства** разделен на две вкладки – **Устройства** и **Кластеры и массивы серверов**. Откройте вкладку объекта, который хотите переместить.
3. Установите флажки рядом с устройствами или кластерами, которые требуется переместить в другую группу.
4. Нажмите на кнопку **Переместить в группу**.
5. В иерархии групп администрирования установите флажок рядом с группой администрирования, в которую вы хотите переместить выбранные устройства или кластеры.

6. Нажмите на кнопку **Переместить**.

Выбранные устройства или кластеры перемещаются в выбранную группу администрирования.

Создание правил перемещения устройств

Можно настроить правила перемещения устройств (см. раздел "Создание правил перемещения устройств" на стр. [1197](#)), в соответствии с которыми устройства будут распределены по группам администрирования.

► *Чтобы создать правило перемещения устройств:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Правила перемещения**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне укажите следующие данные на вкладке **Общие**:

- **Имя правила**

Укажите имя нового правила активации.

Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

- **Группа администрирования**

Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

- **Активное правило**

Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

- **Перемещать только устройства, которые не входят ни в одну группу администрирования**

Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Применить правило**

Вы можете выбрать один из следующих вариантов:

- **Выполнять один раз для каждого устройства**

Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

- **Выполнять один раз для каждого устройства и при каждой установке Агента администрирования**

Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке

Агента администрирования на этих устройствах.

- **Применять правило постоянно**

Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).

4. На вкладке **Условия правила** укажите (см. раздел "Условия для правила перемещения устройств" на стр. [1199](#)) хотя бы один критерий, по которому устройства будут перемещены в группу администрирования.

5. Нажмите на кнопку **Сохранить**.

Правило перемещения создано. Оно появится в списке правил перемещения.

Чем выше положение правила в списке, тем выше его приоритет. Чтобы повысить или понизить приоритет правила перемещения, с помощью мыши переместите правило вверх или вниз по списку соответственно.

Если выбран параметр **Применять правило постоянно**, правило перемещения применяется независимо от приоритета. Такие правила применяются по расписанию, которое Сервер администрирования устанавливает автоматически.

Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

См. также:

Добавление устройств в состав группы администрирования вручную[1195](#)

Копирование правил перемещения устройств

Можно копировать правила перемещения устройств, например, если требуется несколько одинаковых правил для разных целевых групп администрирования.

Чтобы скопировать правило перемещения устройств:

1. Выполните одно из следующих действий:
 - В главном окне приложения перейдите в раздел **Активы (Устройства) → Правила перемещения**.
 - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Правила перемещения**.

Отобразится список правил перемещения устройств.
2. Установите флажок напротив правила, которое требуется скопировать.
3. Нажмите на кнопку **Копировать**.
4. В открывшемся окне при необходимости измените данные на вкладке **Общие** либо оставьте существующие значения, если требуется только скопировать правило, без изменения параметров:
 - **Имя правила**

Укажите имя нового правила активации.

Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

- **Группа администрирования**

Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

- **Активное правило**

Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

- **Перемещать только устройства, которые не входят ни в одну группу администрирования**

Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Применить правило**

Вы можете выбрать один из следующих вариантов:

- **Выполнять один раз для каждого устройства**

Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

- **Выполнять один раз для каждого устройства и при каждой установке Агента администрирования**

Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.

- **Применять правило постоянно**

Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).

5. На вкладке **Условия правила** укажите (см. раздел "Условия для правила перемещения устройств" на стр. [1199](#)) критерии для устройств, которые требуется переместить автоматически.

6. Нажмите на кнопку **Сохранить**.

Будет создано новое правило перемещения. Оно появится в списке правил перемещения.

Условия для правила перемещения устройств

При создании (см. раздел "Создание правил перемещения устройств" см. стр. [1197](#)) или копировании (см. раздел "Копирование правил перемещения устройств" на стр. [1198](#)) правила перемещения клиентских устройств в группы администрирования на вкладке **Условия правила** вы задаете условия перемещения устройств (см. раздел "Создание правил перемещения устройств" на стр. [1197](#)). Чтобы определить, какие устройства следует перемещать, можно использовать следующие критерии:

- Теги, присвоенные клиентским устройствам.
- Параметры сети. Например, вы можете перемещать устройства с IP-адресами из указанного диапазона.
- Управляемые приложения, установленные на клиентских устройствах, например Агент администрирования или Сервер администрирования.
- Виртуальные машины, которые являются клиентскими устройствами.
- Информация об организационном подразделении Active Directory (OU) с клиентскими устройствами.
- Информация об облачном сегменте с клиентскими устройствами.

Ниже вы можете найти описание того, как указать эту информацию в правиле перемещения устройств.

Если в правиле указано несколько условий, срабатывает логический оператор AND и применяются все условия одновременно. Если вы не выберете какие-либо параметры или оставите некоторые поля пустыми, такие условия не применяются.

Вкладка Теги

На этой вкладке можно настроить поиск устройств по ключевым словам (тегам) (см. раздел "Теги устройств" см. стр. [1231](#)), которые были добавлены ранее в описания клиентских устройств. Для этого выберите необходимые теги. Кроме того, вы можете включить следующие параметры:

- **Применить к устройствам без выбранных тегов**
- **Применить, если есть хотя бы один из выбранных тегов**

Вкладка Сеть

На этой вкладке вы можете указать сетевые данные устройств, которые учитывает правило перемещения устройств:

- **Имя устройства в сети Windows**
- **Windows-домен**
- **DNS-имя устройства**
- **DNS-домен**
- **IP-диапазон**
- **IP-адрес подключения к Серверу администрирования**
- **Изменение профиля подключения**
- **Под управлением другого Сервера администрирования**

Вкладка Приложения

На этой вкладке можно настроить правило перемещения устройств на основе управляемых приложений и операционных систем, установленных на клиентских устройствах:

- **Агент администрирования установлен**
- **Приложения**
- **Версия операционной системы**
- **Архитектура операционной системы**
- **Версия пакета обновления операционной системы**

В поле можно указать версию пакета установленной операционной системы (в формате X.Y), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- Пользовательский сертификат
- Номер сборки операционной системы
- Номер выпуска операционной системы

Вкладка Виртуальные машины

На этой вкладке можно настроить параметры правила перемещения клиентских устройств в зависимости от того, являются эти устройства виртуальными машинами или частью инфраструктуры виртуальных рабочих столов (VDI):

- Является виртуальной машиной
- Тип виртуальной машины
- Часть Virtual Desktop Infrastructure

Вкладка Контроллеры домена

На этой вкладке вы можете указать, что требуется перемещать устройства, входящие в организационное подразделение домена. Вы также можете перемещать устройства из всех дочерних подразделений указанного подразделения домена:

- Устройство входит в следующее подразделение
- Включать дочерние подразделения

Если флажок установлен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

По умолчанию флажок снят.

- Перемещать устройства из дочерних подразделений в соответствующие подгруппы
- Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств
- Удалять подгруппы, отсутствующие в домене
- Устройство включено в следующую группу безопасности домена

Вкладка Облачные сегменты

На этой вкладке можно указать, что требуется перемещать устройства, которые относятся к определенным облачным сегментам:

- Устройство находится в облачном сегменте
- Включать дочерние объекты
- Перемещать устройства в соответствующие подгруппы
- Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств
- Удалять подгруппы, для которых нет соответствия в облачных сегментах
- Устройство обнаружено с помощью API

В раскрывающемся списке можно выбрать, обнаруживается ли устройство средствами API.

- **Да.** Устройство обнаруживается с помощью AWS API. Это значит, что устройство обязательно находится в облачном окружении.
- **Нет.** Устройство не обнаруживается с помощью AWS API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но по каким-то причинам недоступно для поиска с помощью AWS API.
 - **Значение не выбрано.** Критерий не применяется.

О кластерах и массивах серверов

Kaspersky Security Center поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что приложение, установленное на клиентском устройстве, является частью массива сервера, то клиентское устройство становится узлом кластера.

Если группа администрирования содержит кластеры или массивы серверов, на странице **Управляемые устройства** отображаются две вкладки: одна для отдельных устройств, другая для кластеров и массивов серверов. После обнаружения управляемых устройств в качестве узлов кластера, кластер добавляется как отдельный объект на вкладку **Кластеры и массивы серверов**.

Узлы кластера или массивы серверов перечислены на вкладке **Устройства** вместе с другими управляемыми устройствами. Вы можете просматривать свойства (см. раздел "Параметры управляемого устройства" см. стр. [1193](#)) узлов как отдельных устройств и выполнять другие операции, но удалить узел кластера или переместить его в другую группу администрирования отдельно от его кластера невозможно. Вы можете удалить или переместить только весь кластер.

Вы можете выполнять следующие операции с кластерами или массивами серверов:

- Посмотреть свойства (см. раздел "Свойства кластеров или массивов серверов" см. стр. [1203](#)).
- Переместить кластер или массив серверов в другую группу администрирования.

При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования.

- Удалить

Целесообразно удалять кластер или массив серверов только тогда, когда кластер или массив серверов больше не существует в сети организации. Если кластер по-прежнему виден в вашей сети, а Агент администрирования и приложение "Лаборатории Касперского" по-прежнему установлено на узлах кластера, Kaspersky Security Center автоматически возвращает удаленный кластер и его узлы обратно в список управляемых устройств.

См. также:

Свойства кластеров или массивов серверов [1203](#)

Свойства кластеров или массивов серверов

► Чтобы просмотреть параметры кластера или массива серверов:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Управляемые устройства → Кластеры и массивы серверов**.

Отображается список кластеров и массивов серверов.

2. Нажмите на имя нужного кластера или массива серверов.

Откроется окно свойств выбранного кластера или массива серверов.

Общие

Раздел **Общие** отображает общую информацию о кластере или массиве серверов. Информация предоставляется на основании данных, полученных в ходе последней синхронизации узлов кластера с Сервером администрирования:

- **Имя**
- **Описание**
- **Windows-домен**
- **NetBIOS-имя**
- **DNS-имя**

Задачи

На вкладке **Задачи** вы можете управлять задачами, назначенными для кластеров и массивов серверов: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять параметры задач и просматривать результаты выполнения. Перечисленные задачи относятся к приложению "Лаборатории Касперского", установленного на узлах кластера. Kaspersky Security Center получает список задач и информацию о статусе задач от узлов кластера. В случае отсутствия связи статус не отображается.

Узлы

На этой вкладке отображается список узлов, входящих в кластер или массив серверов. Вы можете нажать на имя узла, чтобы просмотреть окно свойств устройства (см. раздел "Параметры управляемого устройства" см. стр. [1193](#)).

Приложений "Лаборатории Касперского"

Окно свойств также может содержать дополнительные вкладки с информацией и параметрами, относящимися к приложению "Лаборатории Касперского", установленного на узлах кластера.

См. также:

О кластерах и массивах серверов[1202](#)

Просмотр и настройка действий, когда устройство неактивно

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

► *Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.

2. Выберите имя требуемой группы администрирования.

Откроется окно свойств группы администрирования.

3. В окне свойств перейдите на вкладку **Параметры**.

4. В разделе **Наследование** включите или выключите следующие параметры:

- **Наследовать из родительской группы**

Если флажок установлен, параметры в этом разделе будут наследоваться из родительской группы, в которую входит клиентское устройство. Если флажок установлен, параметры в блоке параметров **Активность устройств в сети** недоступны для изменения.

Этот параметр доступен только для группы администрирования, у которой есть родительская группа администрирования.

По умолчанию параметр включен.

- **Обеспечить принудительное наследование параметров для дочерних групп**

Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

По умолчанию параметр выключен.

5. В разделе **Активность устройств** включите или выключите следующие параметры:

- **Уведомлять администратора, если устройство неактивно больше (сут)**

Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

По умолчанию параметр включен.

- **Удалять устройство из группы, если оно неактивно больше (сут)**

Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. Временной интервал, установленный по умолчанию, составляет 60 дней.

По умолчанию параметр включен.

6. Нажмите на кнопку **Сохранить**.

Ваши изменения сохранены и применены.

О статусах устройства

Kaspersky Security Center присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Kaspersky Security Center учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky Security Center не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический / Видим в сети*.
- *Предупреждение* или *Предупреждение / Видим в сети*.
- *ОК* или *ОК / Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

Таблица 88. Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи <i>Поиск вредоносного ПО</i> , на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача <i>Поиск вредоносного ПО</i> , ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.

Условие	Описание условия	Доступные значения
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
Обнаружены активные угрозы	Количество необработанных объектов в папке Активные угрозы превышает указанное значение.	Более чем 0 штук.
Требуется перезагрузка	Устройство видимо в сети, но приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.

Условие	Описание условия	Доступные значения
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	- Переключатель выключен. - Переключатель включен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи <i>Поиск уязвимостей и требуемых обновлений</i> на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	- Предельный. - Высокий. - Средний. - Игнорировать, если невозможно закрыть уязвимость. - Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	- Переключатель выключен. - Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней.
Давно не выполнялась проверка обновлений Центра обновления Windows	Не выполнялась задача <i>Синхронизация обновлений Windows Update</i> больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	- Не соответствует политике из-за отказа пользователя (только для внешних устройств). - Не соответствует политике из-за ошибки. - В процессе применения политики – требуется перезагрузка. - Не задана политика шифрования. - Не поддерживается. - В процессе применения политики.

Условие	Описание условия	Доступные значения
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	- Переключатель выключен. - Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	- Переключатель выключен. - Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	- Переключатель выключен. - Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы <i>Критический</i> или <i>Предупреждение</i> меняются на статус <i>ОК</i> , когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ.
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	- Переключатель выключен. - Переключатель включен.

Условие	Описание условия	Доступные значения
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности <i>Остановлено</i> или <i>Сбой</i> и отличается от следующих: <i>Запускается</i> , <i>Выполняется</i> или <i>Приостановлено</i> .	Более чем 0 минут.
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	- Переключатель выключен. - Переключатель включен.

Kaspersky Security Center позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *ОК*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3 дней** клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Если вы обновляете Kaspersky Security Center с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Когда Kaspersky Security Center присваивает устройству статус, для некоторых условий (см. графу "Описание условий") учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *ОК*.

См. также:

Настройка переключения статусов устройств[1547](#)

Настройка переключения статусов устройств

Kaspersky Security Center позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*.

► *Чтобы изменить статус устройства на Критический:*

1. Откройте окно свойств одним из следующих способов:

- В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
 - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В открывшемся окне Свойства в панели **Разделы** выберите раздел **Статус устройства**.
 3. В блоке **Установить статус "Критический"** установите флажок для условия из списка.
 4. Для выбранного условия установите необходимое вам значение.
Не для всех условий можно задать значения.
 5. Нажмите на кнопку **ОК**.

► *Чтобы изменить статус устройства на Предупреждение:*

1. Откройте окно свойств одним из следующих способов:
 - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
 - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В открывшемся окне Свойства в панели **Разделы** выберите раздел **Статус устройства**.
3. В блоке **Установить статус "Предупреждение"** установите флажок для условия из списка.
4. Для выбранного условия установите необходимое вам значение.
Не для всех условий можно задать значения.
5. Нажмите на кнопку **ОК**.

Разным значениям одного условия могут соответствовать разные статусы. Например, при соблюдении условия **Базы устарели** со значением *Более 7 дней* клиентскому устройству присваивается статус *Предупреждение*, а со значением *Более 14 дней* – статус *Критический*.

В таблице приведены условия для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения

Таблица 89. Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Флажок установлен. • Флажок снят.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вирусов, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0

Условие	Описание условия	Доступные значения
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	- Остановлена. - Приостановлена. - Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но задача поиска вирусов не выполнялась больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня
Обнаружены активные угрозы	Количество необработанных объектов в папке Необработанные файлы превышает указанное значение.	Более чем 0 штук

Условие	Описание условия	Доступные значения
Требуется перезагрузка	Устройство видимо в сети, но приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Флажок снят. • Флажок установлен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи Поиск уязвимостей и требуемых обновлений на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если нельзя закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Флажок снят. • Флажок установлен.
Срок действия лицензии скоро истечет	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней

Условие	Описание условия	Доступные значения
Давно не выполнялась проверка обновлений Центра обновления Windows	Не выполнялась задача Синхронизация обновлений Windows Update больше указанного времени.	Более 1 дня
Указанный статус шифрования данных	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Флажок снят. • Флажок установлен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором.	• Флажок снят. • Флажок установлен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	• Флажок снят. • Флажок установлен.

Условие	Описание условия	Доступные значения
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы <i>Критический</i> или <i>Предупреждение</i> меняются на статус <i>ОК</i> , когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	- Флажок снят. - Флажок установлен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве выключено больше указанного времени.	Более чем 0 минут
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	- Флажок снят. - Флажок установлен.



Удаленное подключение к рабочему столу клиентского устройства

Администратор может получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

После подключения к устройству администратор получает полный доступ к информации на этом устройстве и может управлять приложениями, установленными на нем.

Удаленное подключение должно быть разрешено в параметрах операционной системы целевого управляемого устройства. Например, в Windows 10 этот параметр называется **Разрешить подключения удаленного помощника к этому компьютеру** (его можно найти **Панель управления** → **Система и безопасность** → **Система** → **Настройка удаленного доступа**). Если у вас есть лицензия на Системное администрирование, вы можете принудительно включить этот параметр, когда установлено соединение с управляемым устройством. Если у вас нет лицензии, включите этот параметр локально на целевом управляемом устройстве. Если этот параметр выключен, удаленное подключение невозможно.

Чтобы установить удаленное соединение с устройством, у вас должно быть две утилиты:

- Утилита klsctunnel "Лаборатории Касперского". Эта утилита должна храниться на рабочей станции администратора. Вы используете эту утилиту для туннелирования соединения между клиентским устройством и Сервером администрирования.

Kaspersky Security Center позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

- Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
- Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт сетевым экраном.
- Стандартный компонент Microsoft Windows "Подключение к удаленному рабочему столу". Подключение к удаленному рабочему столу выполняется с помощью штатной утилиты Windows mstsc.exe в соответствии с параметрами работы этой утилиты.

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. После подключения администратора к сеансу пользователь устройства будет отключен от сеанса без предварительного уведомления.

► *Чтобы удаленно подключиться к рабочему столу клиентского устройства:*

1. В Консоли администрирования на основе MMC в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования перейдите в раздел **Параметры подключения к Серверу администрирования** → **Порты подключения**.
3. Убедитесь, что параметр **Открыть RDP-порт для Kaspersky Security Center Web Console** включен.
4. В Kaspersky Security Center Web Console перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
5. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
6. В открывшейся панели слева выберите группу администрирования, содержащую устройство, к которому вы хотите получить доступ.

7. Установите флажок напротив устройства, к которому вы хотите получить доступ.
8. Нажмите на кнопку **Подключиться к удаленному рабочему столу**.
Откроется окно Удаленный рабочий стол (только Windows).
9. Включите параметр **Разрешить подключение к удаленному рабочему столу на управляемом устройстве**. В этом случае соединение будет установлено, даже если удаленные подключения в настоящее время запрещены в параметрах операционной системы на управляемом устройстве.

Этот параметр доступен только при наличии лицензии на Системное администрирование.

10. Нажмите на кнопку **Загрузить**, чтобы загрузить утилиту klsctunnel.
11. Нажмите на кнопку **Копировать в буфер обмена**, чтобы скопировать текст из текстового поля. Этот текст представляет собой двоичный объект данных (BLOB), который содержит параметры, необходимые для установления соединения между Сервером администрирования и управляемым устройством.

Объект BLOB действителен в течение 3 минут. Если срок его действия истек, снова откройте окно Удаленный рабочий стол (только Windows), чтобы сгенерировать новый объект BLOB.

12. Запустите утилиту klsctunnel.
Откроется окно утилиты.
13. Вставьте скопированный текст в текстовое поле.
14. Если вы используете прокси-сервер, установите флажок **Использовать прокси-сервер**, а затем укажите параметры подключения к прокси-серверу.
15. Нажмите на кнопку **Открыть порт**.
Откроется окно входа в систему подключения к удаленному рабочему столу.
16. Укажите учетные данные учетной записи, под которой вы в настоящий момент входите Kaspersky Security Center Web Console.
17. Нажмите на кнопку **Подключиться**.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

Подключение к устройствам с помощью совместного доступа к рабочему столу Windows

Администратор может получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

Администратор может подключиться к существующему сеансу на клиентском устройстве без отключения пользователя, работающего в этом сеансе. В этом случае у администратора и пользователя сеанса на устройстве есть совместный доступ к рабочему столу.

Чтобы установить удаленное соединение с устройством, у вас должно быть две утилиты:

- Утилита klsctunnel "Лаборатории Касперского". Эта утилита должна храниться на рабочей станции администратора. Вы используете эту утилиту для туннелирования соединения между клиентским устройством и Сервером администрирования.

Kaspersky Security Center позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

- Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
- Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт сетевым экраном.
- Совместный доступ к рабочему столу Windows. При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит запрос от администратора на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky Security Center.

Администратор может настроить аудит действий на удаленном клиентском устройстве. В ходе аудита приложение сохраняет информацию о файлах на клиентском устройстве, которые открывал и/или изменял администратор.

Для подключения к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows требуется выполнение следующих условий:

- На рабочем месте администратора установлена операционная система Microsoft Windows Vista или более поздняя версия. Тип операционной системы устройства, на котором установлен Сервер администрирования, не является ограничением для подключения с помощью совместного доступа к рабочему столу Windows.

Чтобы проверить, включена ли функция совместного доступа к рабочему столу Windows в вашей версии Windows, убедитесь, что ключ CLSID{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} включен в реестре Windows.

- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.
- Kaspersky Security Center использует лицензию на Системное администрирование.

► *Чтобы подключиться к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows:*

1. В Консоли администрирования на основе MMC в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования перейдите в раздел **Параметры подключения к Серверу администрирования** → **Порты подключения**.
3. Убедитесь, что параметр **Открыть RDP-порт для Kaspersky Security Center Web Console** включен.
4. В Kaspersky Security Center Web Console перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

5. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
6. В открывшейся панели слева выберите группу администрирования, содержащую устройство, к которому вы хотите получить доступ.
7. Установите флажок напротив устройства, к которому вы хотите получить доступ.
8. Нажмите на кнопку **Совместный доступ к рабочему столу Windows**.
Открывается мастер Совместный доступ к рабочему столу Windows.
9. Нажмите на кнопку **Загрузить**, чтобы загрузить утилиту klsctunnel, и дождитесь завершения процесса загрузки.
Если у вас уже есть утилита klsctunnel, пропустите этот шаг.
10. Нажмите на кнопку **Далее**.
11. Выберите сеанс на устройстве, к которому вы хотите подключиться, а затем нажмите на кнопку **Далее**.
12. На целевом устройстве в открывшемся окне пользователь должен разрешить сеанс совместного доступа к рабочему столу. Иначе сеанс невозможен.
После того как пользователь подтвердит сеанс совместного доступа к рабочему столу, мастер откроет следующий шаг.
13. Нажмите на кнопку **Копировать в буфер обмена**, чтобы скопировать текст из текстового поля. Этот текст представляет собой двоичный объект данных (BLOB), который содержит параметры, необходимые для установления соединения между Сервером администрирования и управляемым устройством.

Объект BLOB действителен в течение 3 минут. Если срок его действия истек, сгенерируйте объект BLOB.

14. Запустите утилиту klsctunnel.
Откроется окно утилиты.
15. Вставьте скопированный текст в текстовое поле.
16. Если вы используете прокси-сервер, установите флажок **Использовать прокси-сервер**, а затем укажите параметры подключения к прокси-серверу.
17. Нажмите на кнопку **Открыть порт**.
Совместный доступ к рабочему столу запускается в новом окне. Если вы хотите взаимодействовать с устройством, нажмите на значок меню () в верхнем левом углу окна и выберите **Интерактивный режим**.

Выборки устройств

Выборки устройств – это инструмент для фильтрации устройств в соответствии с заданными условиями. Вы можете использовать выборки устройств, чтобы управлять несколькими устройствами: например, для просмотра отчетов только о выбранных устройствах или для перемещения всех этих устройств в другую группу администрирования.

Kaspersky Security Center предоставляет широкий диапазон *предопределенных выборок устройств* (например, **Устройства со статусом "Критический"**, **Защита выключена**, **Обнаружены активные**

угрозы). Предопределенные выборки невозможно удалить. Вы можете также создавать и настраивать дополнительные *пользовательские выборки событий*.

В пользовательских выборках вы можете задать область поиска и выбрать все устройства, управляемые устройства или нераспределенные устройства. Параметры поиска задаются в условиях. В выборках устройств вы можете создать несколько условий с различными параметрами поиска. Например, вы можете создать два условия и задать различные IP-диапазоны в каждом из них. Если задано несколько условий, в выборку устройств попадут устройства, которые удовлетворяют любому из условий. Напротив, параметры поиска в одном условии накладываются друг на друга. Если в условии выборки заданы IP-диапазон и название установленного приложения, то в выборку устройств попадут только те устройства, на которых одновременно установлено указанное приложение и их IP-адреса входят в указанный диапазон.

См. также:

Использование выборок событий	1484
Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console.....	985
Сценарий: настройка защиты сети.....	403

Просмотр списка устройств из выборки устройств

Kaspersky Security Center позволяет просматривать список устройств из выборки устройств.

► Чтобы просмотреть список устройств из выборки устройств:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Выборки устройств** или в раздел **Обнаружение устройств и развертывание** → **Выборки устройств**.

2. В списке выборок нажмите на имя выборки устройств.

На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.

3. Вы можете группировать и фильтровать данные таблицы устройств следующим образом:

- Нажмите на значок параметров () и выберите столбцы для отображения в таблице.
- Нажмите на значок фильтрации (), укажите и примените критерий фильтрации в открывшемся меню.

Отобразится отфильтрованная таблица устройств.

Вы можете выбрать одно или несколько устройств в выборке устройств и нажать на кнопку **Новая задача**, чтобы создать задачу (см. раздел "Задачи" см. стр. [1172](#)), которая будет применена к этим устройствам.

Чтобы переместить выбранные устройства из выборки устройств в другую группу администрирования, нажмите на кнопку **Переместить в группу** и выберите целевую группу администрирования.

Создание выборки устройств

► Чтобы создать выборку устройств:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Выборки устройств**.

Отобразится страница со списком выборок устройств.

2. Нажмите на кнопку **Добавить**.

Откроется окно **Параметры выборки устройств**.

3. Введите имя новой выборки.

4. Укажите группу, содержащую устройства, которые будут включены в выборку устройств:

- **Искать любые устройства** – поиск устройств, соответствующих критериям выборки, в группах **Управляемые устройства** или **Нераспределенные устройства**.
- **Искать управляемые устройства** – поиск устройств, соответствующих критериям выборки, в группе **Управляемые устройства**.
- **Искать нераспределенные устройства** – поиск устройств, соответствующих критериям выборки, в группе **Нераспределенные устройства**.

Вы можете установить флажок **Включать данные подчиненных Серверов администрирования**, чтобы включить поиск устройств, отвечающих критериям выборки, на подчиненных Серверах администрирования.

5. Нажмите на кнопку **Добавить**.

6. В открывшемся окне укажите условия (см. раздел "Настройка выборки устройств" см. стр. [1220](#)), которые должны быть выполнены для включения устройств в эту выборку и нажмите на кнопку **ОК**.

7. Нажмите на кнопку **Сохранить**.

Выборка устройств создана и добавлена в список выборок устройств.

Настройка выборки устройств

► Чтобы настроить параметры выборки устройств:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Выборки устройств**.
Отобразится страница со списком выборок устройств.
2. Выберите соответствующую пользовательскую выборку устройств и нажмите на кнопку **Свойства**.
Откроется окно **Параметры выборки устройств**.
3. На вкладке **Общие** перейдите по ссылке **Новое условие**.
4. Укажите условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку.
5. Нажмите на кнопку **Сохранить**.

Параметры применены и сохранены.

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

Инвертировать условие выборки

Если флажок установлен, заданное условие выборки будет инвертировано. В

выборку попадут все устройства, не соответствующие условию.

По умолчанию флажок снят.

Инфраструктура сети

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

- **Имя устройства**

Имя устройства в сети Windows (NetBIOS-имя).

- **Домен**

Будут отображаться все устройства, входящие в указанный домен Windows.

- **Группа администрирования**

Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие** или в разделе **Заметки**.

Для описания текста в поле **Комментарий** допустимо использовать следующие символы:

- Внутри одного слова:

- *. Заменяет любую строку длиной 0 и более символов.

Пример:

Для описания слов **Сервер**, **Серверный** или **Серверная** можно использовать строку **Сервер***

- ?. Заменяет любой один символ.

Пример:

Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

Символ * или ? не может использоваться как первый символ в описании текста.

- Для связи нескольких слов:

- Пробел. Обозначает наличие в тексте хотя бы одного из слов, разделенных пробелами.

Пример:

Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

- +. При написании перед словом обозначает обязательное наличие слова в тексте.

Пример:

Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

- -. При написании перед словом обозначает обязательное отсутствие слова в тексте.

Пример:

Для описания фразы, в которой должно присутствовать слово

Подчиненный, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

- **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

Пример:

Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-диапазон**

Если флажок установлен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

По умолчанию флажок снят.

- **Под управлением другого Сервера администрирования**

В разделе **Контроллеры домена** можно настроить критерии включения устройств в выборку по членству в домене:

- **Устройство в подразделении домена**
- Это устройство является членом группы безопасности домена

В разделе **Сетевая активность** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- **Является точкой распространения**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да**. В выборку будут включены устройства, являющиеся агентами обновлений.
- **Нет**. Устройства, являющиеся агентами обновлений, не будут включены в выборку.
- **Значение не выбрано**. Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Включен**. В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
- **Выключен**. В выборку будут включаться устройства, на которых флажок **Не разрывать соединение с Сервером администрирования** снят.
- **Значение не выбрано**. Критерий не применяется.

- **Переключение профиля подключения**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Значение не выбрано**. Критерий не применяется.

- **Последнее подключение к Серверу администрирования**

С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

Если флажок установлен, то в выборку попадают только новые устройства, обнаруженные при опросе сети за количество дней, которое указано в поле **Период обнаружения (сут)**.

Если флажок снят, то в выборку попадают все устройства, обнаруженные при опросе сети.

По умолчанию флажок снят.

- **Устройство в сети**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** Приложение включает в выборку устройства, которые видимы в сети в настоящий момент.
- **Нет.** Приложение включает в выборку устройства, которые не видимы в сети в настоящий момент.
- **Значение не выбрано.** Критерий не применяется.

В разделе **Облачные сегменты** можно настроить критерии включения устройств в выборку в соответствии с облачными сегментами:

- **Устройство находится в облачном сегменте**
- **Устройство обнаружено с помощью API**

Статусы устройств

В разделе **Статус управляемых устройств** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемого приложения:

- **Статус устройства**

Раскрывающийся список, в котором можно выбрать один из статусов устройства: *ОК, Критический, Предупреждение*.

- **Статус постоянной защиты**

Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

- **Описание статуса устройства**

В этом поле можно установить флажки для условий, при соблюдении которых

устройству будет присваиваться выбранный статус: *ОК, Критический, Предупреждение*.

В разделе **Статусы компонентов управляемых приложений** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых приложений:

- **Статус защиты данных от утечек**

Поиск устройств по статусу компонента защиты от утечки данных (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус защиты для серверов совместной работы**

Поиск устройств по статусу компонента защиты для серверов совместной работы (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу компонента антивирусной защиты почтовых серверов (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

В разделе **Проблемы, связанные со статусом управляемых приложений** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемым приложением. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких приложений, у вас есть возможность автоматически выбрать эту проблему во всех списках.

Вы можете установить флажки для описаний статусов от управляемого приложения, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких приложений, у вас есть возможность автоматически выбрать этот статус во всех списках.

Сведения о системе

В разделе **Операционная система** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы.

- **Тип платформы**

Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Версия пакета обновления операционной системы**

В поле можно указать версию пакета установленной операционной системы (в формате X.Y), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Архитектура операционной системы**

В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Неизвестно, x86, AMD64, IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Номер сборки операционной системы**

Этот параметр применим только для операционных систем Windows.

Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Номер выпуска операционной системы**

Этот параметр применим только для операционных систем Windows.

Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**
- **Тип виртуальной машины**

В раскрываемом списке можно выбрать производителя виртуальной машины.

Раскрываемый список доступен, если в раскрываемом списке **Является виртуальной машиной** указано значение **Да**.

- **Часть Virtual Desktop Infrastructure**

В разделе **Реестр оборудования** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

- **Устройство**

В раскрываемом списке можно выбрать тип оборудования, которое должно быть установлено на клиентском устройстве, чтобы оно отображалось в результатах поиска.

В поле поддерживается полнотекстовый поиск.

- **Поставщик**

В раскрываемом списке можно выбрать производителя оборудования, которое должно быть установлено на устройстве, чтобы устройство отображалось в результатах поиска.

В поле поддерживается полнотекстовый поиск.

- **Имя устройства**

Имя устройства в Windows-сети. Устройство с указанным именем будет включено в выборку.

- **Описание**

Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Поставщик устройства**

Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

Название производителя можно ввести в окне свойств устройства.

- **Серийный номер**

Оборудование с серийным номером, указанным в поле, будет включено в выборку.

- **Инвентарный номер**

Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Пользователь**

Оборудование пользователя, указанного в поле, будет включено в выборку.

- **Расположение**

Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

- **Частота процессора (МГц) от**
- **Частота процессора (МГц) до**
- **Количество виртуальных ядер процессора от**
- **Количество виртуальных ядер процессора до**
- **Объем жесткого диска (ГБ), от**
- **Объем жесткого диска (ГБ), до**
- **Объем оперативной памяти (МБ) от**
- **Объем оперативной памяти (МБ) до**

Информация о приложениях сторонних производителей

В разделе **Реестр приложений** можно настроить критерии включения устройств в выборку в зависимости от того, какие приложения на них установлены:

- **Название приложения**

Раскрывающийся список, в котором можно выбрать приложение. Устройства, на которых установлено указанное приложение, будут включены в выборку.

- **Версия приложения**

Поле ввода, в котором указывается версия выбранного приложения.

- **Поставщик**

Раскрывающийся список, в котором можно выбрать производителя установленного на устройстве приложения.

- **Статус приложения**

Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

Если флажок установлен, поиск будет выполняться по данным об обновлении приложений, установленных на искомым устройствах. После установки флажка названия полей ввода **Название приложения** и **Версия приложения** меняются на **Имя обновления** и **Версия обновления**.

По умолчанию флажок снят.

- **Название несовместимого приложения безопасности**

Раскрывающийся список, в котором можно выбрать приложения защиты сторонних производителей. Во время поиска устройства, на которых установлено выбранное приложение, будут включены в выборку.

- **Тег приложения**

В раскрываемом списке можно выбрать тег приложения. Все устройства, на которых установлены приложения, имеющие выбранный тег в описании, включаются в выборку устройств.

- **Применить к устройствам без выбранных тегов**

Если флажок установлен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

Если флажок снят, критерий не применяется.

По умолчанию флажок снят.

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Центра обновления Windows:

WUA переключен на Сервер администрирования

В раскрываемом списке можно выбрать один из следующих вариантов поиска:

- **Да.** Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Windows Update с Сервера администрирования.
- **Нет.** Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Windows Update из другого источника.

Информация о приложениях "Лаборатории Касперского"

В разделе **Приложения "Лаборатории Касперского"** можно настроить критерии включения устройств в выборку на основании выбранного управляемого приложения:

- **Название приложения**

В раскрываемом списке можно выбрать критерий включения устройств в состав

выборки при поиске по наименованию приложения "Лаборатории Касперского".

В списке представлены названия только тех приложений, для которых на рабочем месте администратора установлены плагины управления.

Если приложение не выбрано, то критерий не применяется.

- **Версия приложения**

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии приложений "Лаборатории Касперского".

Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для приложения наименованию или номеру пакета обновления.

Если поле не заполнено, то критерий не применяется.

- **Выбор периода последнего обновления модулей**

С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей приложений, установленных на устройствах.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей приложений, установленных на устройствах.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Устройство находится под управлением Сервера администрирования**

В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

- **Да.** Приложение включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
- **Нет.** Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
- **Значение не выбрано.** Критерий не применяется.

- **Приложение безопасности установлено**

В раскрывающемся списке можно включить в состав выборки устройства, на которых установлено приложение защиты:

- **Да.** Приложение включает в выборку устройства, на которых установлено приложение защиты.
- **Нет.** Приложение включает в выборку устройств, на которых не установлено приложение защиты.
- **Значение не выбрано.** Критерий не применяется.

В разделе **Антивирусная защита** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

Если флажок установлен, поиск клиентских устройств выполняется по дате выпуска баз. В полях ввода можно задать временной интервал, на основании которого

будет выполняться поиск.

По умолчанию флажок снят.

- **Количество записей в базах**

Если флажок установлен, поиск клиентских устройств выполняется по количеству записей в базах. В полях ввода можно задать нижнее и верхнее значения количества записей.

По умолчанию флажок снят.

- **Последняя проверка**

Если флажок установлен, поиск клиентских устройств выполняется по времени последнего поиска вирусов. В полях ввода можно указать интервал, в течение которого поиск вирусов выполнялся в последний раз.

По умолчанию флажок снят.

- **Обнаружены угрозы**

Если флажок установлен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

По умолчанию флажок снят.

В подразделе **Шифрование** можно настроить критерии включения устройств в выборку на основе выбранного алгоритма шифрования:

Алгоритм шифрования

Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Возможные значения: *AES56, AES128, AES192, AES256*.

Подраздел **Компоненты приложения** содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в Kaspersky Security Center Web Console.

В разделе **Компоненты приложения** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранному приложению:

- **Статус**
- **Версия**

Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, 3.4.1.0, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

Теги

В разделе **Теги** можно настроить критерии включения устройств в выборку по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

Применить, если есть хотя бы один из выбранных тегов

Если флажок установлен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если флажок снят, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию флажок снят.

Чтобы добавить теги к критерию, нажмите на кнопку **Добавить** и выберите теги, нажав на поле ввода **Тег**. Укажите, следует ли включать или исключать устройства с выбранными тегами в выборку устройств.

- **Все устройства, имеющие этот тег**

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

По умолчанию выбран этот вариант.

- **Все устройства, не имеющие этого тега**

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Пользователи

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**
- **Пользователь, уже выполнявший вход в систему**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Экспорт списка устройств из выборки устройств

Kaspersky Security Center позволяет сохранять информацию об этих устройствах из выборки устройств и экспортировать ее в файл CSV или TXT.

► Чтобы экспортировать список устройств из выборки устройств:

1. Откройте таблицу с устройствами (см. раздел "Просмотр списка устройств из выборки устройств" см. стр. [1219](#)) из выборки устройств.
2. Используйте один из следующих способов для выбора устройств, которые вы хотите экспортировать:
 - Чтобы выбрать определенные устройства, установите флажки рядом с ними.
 - Чтобы выбрать все устройства на текущей странице таблицы, установите флажок в заголовке таблицы устройств, а затем установите флажок **Выбрать все на текущей странице**.
 - Чтобы выбрать все устройства из таблицы, установите флажок в заголовке таблицы устройств, а затем выберите **Выбрать все**.

3. Нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**. Вся информация о выбранных устройствах, включенных в таблицу, будет экспортирована.

Обратите внимание, если вы отфильтровали таблицу устройств, будут экспортированы только отфильтрованные данные отображаемых столбцов.

Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

► Чтобы удалить устройства из групп администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Выборки устройств** или **Обнаружение устройств и развертывание → Выборки устройств**.

2. В списке выборок нажмите на имя выборки устройств.

На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.

3. Выберите устройства, которые вы хотите удалить и нажмите на кнопку **Удалить**.

В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Теги устройств

Kaspersky Security Center позволяет назначать *теги* устройствам. Тег представляет собой идентификатор устройства, который можно использовать для группировки, описания, поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств (см. раздел "Выборки устройств" на стр. [1218](#)), при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Теги можно назначать вручную, если требуется отметить отдельные устройства. Автоматическое назначение тегов выполняется Kaspersky Security Center в соответствии с заданными правилами назначения тегов.

Автоматическое назначение тегов устройствам происходит при выполнении определенных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве приложениям и другим свойствам устройства. Например, если используется гибридная инфраструктура, состоящая из физических устройств, инстансов Amazon EC2 и виртуальных машин Microsoft Azure, можно настроить правило, в соответствии с которым всем виртуальным машинам Microsoft Azure будет назначен тег [\[Azure\]](#). Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать все виртуальные машины Microsoft Azure и назначить им задачу.

Тег автоматически удаляется с устройства в следующих случаях:

- Устройство перестает удовлетворять условиям правила назначения тега.
- Правило назначения тега выключено или удалено.

Списки тегов и списки правил для каждого Сервера администрирования являются независимыми для всех Серверов администрирования, включая главный Сервер администрирования и подчиненные виртуальные

Серверы администрирования. Правило применяется только к устройствам под управлением того Сервера администрирования, на котором оно создано.

См. также:

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985
Сценарий: обнаружение сетевых устройств	1109
Настройка и распространение политик: подход, ориентированный на устройства	405

Создание тегов устройств

► Чтобы создать тег устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. Нажмите на кнопку **Добавить**.
Отобразится окно создания тега.
3. В поле **Тег** введите название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.
Новый созданный тег появляется в списке тегов устройства.

См. также:

Сценарий: обнаружение сетевых устройств	1109

Изменение тегов устройств

► Чтобы переименовать тег устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. Выделите тег, который требуется переименовать.
Откроется окно свойств тега.
3. В поле **Тег** измените название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.
Обновленный тег появится в списке тегов устройства.

См. также:

Сценарий: обнаружение сетевых устройств	1109

Удаление тегов устройств

► Чтобы удалить тег устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. В списке выберите теги устройства, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **Да**.

Выбранный тег устройства удален. Удаленный тег автоматически снимается со всех устройств, которым он был назначен.

Тег, который вы удалили, не удаляется автоматически из правил автоматического назначения тегов. После удаления тега он будет назначен новому устройству только при первом совпадении параметров устройства с условиями правила назначения тегов. Удаленный тег не удаляется автоматически с устройства, если этот тег назначен устройству приложением или Агентом администрирования. Чтобы удалить тег с вашего устройства, используйте утилиту klscflag (см. раздел "Удаление тега устройства" на стр. [1239](#)).

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Просмотр устройств, которым назначен тег

► Чтобы просмотреть устройства с назначенными тегами:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. Перейдите по ссылке **Просмотреть устройства** рядом с названием тега, для которого вы хотите посмотреть список назначенных устройств.

Вы будете перенаправлены в раздел **Управляемые устройства** главного меню с устройствами, отфильтрованными по тегу, для которого вы нажали ссылку **Просмотреть устройства**.

3. Если вы хотите вернуться к списку тегов устройства, нажмите на кнопку **Назад** в браузере.

После просмотра устройств, которым назначен тег, вы можете создать и назначить новый тег или назначить существующий тег другим устройствам (см. раздел "Назначение тегов устройству вручную" см. стр. [1234](#)). В этом случае вам придется удалить фильтр по тегу, выбрать устройства и назначить тег.

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Просмотр тегов, назначенных устройству

► Чтобы просмотреть теги, назначенные устройству:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В открывшемся окне свойств устройства выберите вкладку **Теги**.

Отобразится список тегов, назначенных выбранному устройству. В столбце **Назначенный тег** вы можете просмотреть, как был назначен тег (см. раздел "Теги устройств" см. стр. [1231](#)).

Можно назначить другой тег (см. раздел "Назначение тегов устройству вручную" см. стр. [1234](#)) устройству или удалить назначенный ранее тег (см. раздел "Удаление назначенного тега с устройства" см. стр. [1234](#)). Можно также просмотреть все теги устройств, которые существуют на Сервере администрирования.

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Назначение тегов устройству вручную

► Чтобы вручную назначить тег устройству:

1. Просмотрите теги, уже назначенные устройству, которому вы хотите назначить тег (см. раздел "Просмотр тегов, назначенных устройству" см. стр. [1234](#)).
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне выполните одно из следующих действий:
 - Чтобы создать и добавить новый тег, выберите пункт **Создать тег** и укажите имя тега.
 - Чтобы выбрать существующий тег, выберите пункт **Назначить существующий тег** и в раскрывающемся списке выберите нужный тег.
4. Нажмите на кнопку **ОК**, чтобы применить изменения.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Выбранный тег будет назначен устройству.

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Удаление назначенного тега с устройства

► Чтобы снять назначенный тег с устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

2. Выберите устройство, теги которого требуется просмотреть.
3. В открывшемся окне свойств устройства выберите вкладку **Теги**.
4. Установите флажок напротив тега, который требуется снять.
5. В верхней части списка нажмите на кнопку **Отменить назначение тега?**.
6. В появившемся окне нажмите на кнопку **Да**.

Тег будет снят с устройства.

Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную (см. раздел "Удаление тегов устройств" см. стр. [1233](#)).

Вы не можете вручную удалить теги, назначенные устройству приложениями или Агентом администрирования. Чтобы удалить эти теги, используйте утилиту klscflag (см. раздел "Удаление тега устройства" на стр. [1239](#)).

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Просмотр правил автоматического назначения тегов устройствам

- Чтобы просмотреть правила автоматического назначения тегов устройствам,

Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Активы (Устройства) → Теги → Правила автоматического назначения тегов**.
- В главном окне приложения перейдите в раздел **Активы (Устройства) → Теги → Теги устройств**, а затем перейдите по ссылке **Настроить правила автоматического назначения тегов**.
- Перейдите к просмотру тегов, назначенных устройству (см. раздел "Просмотр тегов, назначенных устройству" см. стр. [1234](#)), и нажмите на кнопку **Параметры**.

Отобразится список правил автоматического назначения тегов устройствам.

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Изменение правил автоматического назначения тегов устройствам

- Чтобы изменить правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам (см. раздел "Просмотр правил автоматического назначения тегов устройствам" см. стр. [1235](#)).

2. Выберите правило, которое требуется изменить.
Откроется окно с параметрами правила.
3. Измените основные параметры правила:
 - d. В поле **Имя правила** измените название правила.
Название не должно быть длиннее 256 символов.
 - e. Выполните одно из следующих действий:
 - Включите правило, установив переключатель в положение **Правило включено**.
 - Выключите правило, установив переключатель в положение **Правило выключено**.
4. Выполните одно из следующих действий:
 - Если вы хотите добавить новое условие, нажмите на кнопку **Добавить** и в открывшемся окне укажите параметры нового условия (см. раздел "Создание правил автоматического назначения тегов устройствам" см. стр. [1236](#)).
 - Если вы хотите изменить существующее условие, выделите условие, которое требуется изменить, и измените его параметры (см. раздел "Создание правил автоматического назначения тегов устройствам" см. стр. [1236](#)).
 - Если вы хотите удалить условие, установите флажок рядом с именем условия, которое требуется удалить, и нажмите на кнопку **Удалить**.
5. В окне с параметрами условий нажмите на кнопку **ОК**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.
Измененное правило отображается в списке.

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Создание правил автоматического назначения тегов устройствам

► Чтобы создать правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам (см. раздел "Просмотр правил автоматического назначения тегов устройствам" см. стр. [1235](#)).
2. Нажмите на кнопку **Добавить**.
Откроется окно с параметрами нового правила.
3. Укажите основные параметры правила:
 - a. В поле **Имя правила** введите название правила.
Название не должно быть длиннее 256 символов.
 - b. Выполните одно из следующих действий:
 - Включите правило, установив переключатель в положение **Правило включено**.
 - Выключите правило, установив переключатель в положение **Правило выключено**.

- с. В поле **Тег** укажите новое название тега устройства или выберите существующий тег устройства из списка.

Название не должно быть длиннее 256 символов.

4. В поле выбора условия нажмите на кнопку **Добавить**, чтобы добавить новое условие.

Откроется окно с параметрами нового условия.

5. Укажите название условия.

Название не должно быть длиннее 256 символов. Название условия должно быть уникальным в рамках одного правила.

6. Настройте срабатывание правила по следующим условиям: Можно выбрать несколько условий.

- **Сеть** – сетевые свойства устройства (например, имя устройства в сети Windows, принадлежность устройства к домену или к IP-подсети).

Если для базы данных, которую вы используете для Kaspersky Security Center, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

- **Приложения** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.
- **Виртуальные машины** – принадлежность устройства к определенному типу виртуальных машин.
- **Контроллеры домена** – нахождение устройства в подразделении Active Directory и членство устройства в группе Active Directory.
- **Реестр приложений** – наличие на устройстве приложений различных производителей.

7. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

При необходимости можно задать несколько условий для одного правила. В этом случае тег будет назначен устройствам, если для них выполняется хотя бы одно из условий.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданное правило выполняется на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

В дальнейшем правило применяется в следующих случаях:

- Автоматически, регулярно, в зависимости от загрузки сервера.
- После изменения правила (см. раздел "Изменение правил автоматического назначения тегов устройствам" см. стр. [1235](#)).
- После выполнения правила вручную (см. раздел "Выполнение правил автоматического назначения тегов устройствам" см. стр. [1238](#)).
- После того как Сервер администрирования обнаружит изменения, которые соответствуют условиям правила, в параметрах устройства или в параметрах группы, которая содержит это устройство.

Вы можете создать несколько правил назначения тегов. Одному устройству может быть назначено несколько тегов, в случае если вы создали несколько правил назначения тегов и условия этих правил выполняются одновременно. Вы можете просмотреть список всех назначенных тегов (см. раздел "Просмотр тегов, назначенных устройству" см. стр. [1234](#)) в свойствах устройства.

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Выполнение правил автоматического назначения тегов устройствам

Когда выполняется правило, тег, указанный в свойствах этого правила, назначается устройству, которое соответствует условиям, указанным в свойствах правила. Можно выполнять только активные правила.

► *Чтобы выполнить правила автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. раздел "Просмотр правил автоматического назначения тегов устройствам" см. стр. [1235](#)).
2. Установите флажки напротив активных правил, которые требуется выполнить.
3. Нажмите на кнопку **Выполнить правило**.

Выбранные правила будут выполнены.

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Удаление правил автоматического назначения тегов с устройств

► *Чтобы удалить правило автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. раздел "Просмотр правил автоматического назначения тегов устройствам" см. стр. [1235](#)).
2. Установите флажок напротив правила, которое требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **Удалить** еще раз.

Выбранное правило будет удалено. Тег, указанный в свойствах этого правила, будет снят со всех устройств, которым он был назначен.

Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную (см. раздел "Удаление тегов устройств" см. стр. [1233](#)).

См. также:

Сценарий: обнаружение сетевых устройств[1109](#)

Управление тегами устройств с помощью утилиты klscflag

В этом разделе содержится информация о том, как назначать или удалять теги устройств с помощью утилиты klscflag.

В этом разделе

Назначение тега устройству	1239
Удаление тега устройства.....	1239

Назначение тега устройству

Обратите внимание, что вам нужно запустить утилиту klscflag на клиентском устройстве, которому вы хотите назначить тег.

► Чтобы назначить тег вашему устройству с помощью утилиты klscflag:

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Агента администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\NetworkAgent.
2. Введите следующую команду:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n  
KLCONN_HOST_TAGS -sv "[\"TAG NAME\"]" -svt ARRAY_T -ss "|ss_type =  
\"SS_PRODINFO\";"
```

где TAG NAME — это имя тега, который вы хотите назначить устройству, например:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n  
KLCONN_HOST_TAGS -sv "[\"ENTERPRISE\"]" -svt ARRAY_T -ss "|ss_type =  
\"SS_PRODINFO\";"
```

3. Перезапустите службу Агента администрирования.

Указанный тег будет назначен вашему устройству. Чтобы убедиться, что тег назначен успешно, просмотрите теги, назначенные устройству (см. раздел "Просмотр тегов, назначенных устройству" на стр. [1234](#)).

Также можно назначать теги устройств вручную (см. раздел "Назначение тегов устройству вручную" см. стр. [1234](#)).

Удаление тега устройства

Если тег назначен устройству приложением или Агентом администрирования, вы не сможете удалить этот тег вручную. В этом случае используйте утилиту klscflag для удаления назначенного тега с устройства.

Обратите внимание, что вам нужно запустить утилиту klscflag на клиентском устройстве, с которого вы хотите удалить тег.

► Чтобы удалить тег с устройства с помощью утилиты klscflag:

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки

Агента администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\NetworkAgent.

2. Введите следующую команду:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n  
KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type =  
\"SS_PRODINFO\"";"
```

3. Перезапустите службу Агента администрирования.

Тег будет снят с устройства.

Политики и профили политик

В Kaspersky Security Center Web Console можно создавать политики для приложений "Лаборатории Касперского". В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

В этом разделе

О политиках и профилях политик.....	1241
Блокировка (замок) и заблокированные параметры	1242
Наследование политик и профилей политик.....	1244
Управление политиками.....	1251
Управление профилями политик	1261

См. также:

Сценарий: настройка защиты сети	403

О политиках и профилях политик

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования и ее подгруппе. Вы можете установить несколько приложений "Лаборатории Касперского" на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов (см. таблицу ниже):

Таблица 90. Статус политики

Состояние	Описание
Активная	Это текущая политика, которая применяется к устройству. Для приложения "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики приложения "Лаборатории Касперского" применяются к устройству.
Неактивная	Политика, которая в настоящее время не применяется к устройству.
Для автономных пользователей	Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

Политики действуют по следующим правилам:

- Для одного приложения можно настроить несколько политик с различными значениями.
- Для одного приложения может быть активна только одна политика.

- Вы можете активировать неактивную политику при возникновении определенного события. Например, в период вирусных атак можно включить параметры для усиленной антивирусной защиты.
- Политика может иметь дочерние политики.

Вы можете использовать политики для подготовки к экстренным ситуациям, например, к вирусной атаке. Например, если происходит атака через флеш-накопители USB, можно активировать политику, блокирующую доступ к флеш-накопителям. В этом случае текущая активная политика автоматически становится неактивной.

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

Профиль политики – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров локального приложения, которые в настоящее время применяются к устройству.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей.

См. также:

Наследование политик и профилей политик [1244](#)

Блокировка (замок) и заблокированные параметры

У каждого параметра политики есть значок замка (🔒). В таблице ниже показаны состояния значка замка:

Таблица 91. Статусы значка замка

Состояние	Описание
 Не определено 	Если рядом с параметром отображается значок открытого замка и переключатель выключен, параметр не указан в политике. Пользователь может изменить эти параметры в интерфейсе управляемого приложения. Такие параметры называются <i>разблокированными</i> .
 Принудительно 	Если рядом с параметром отображается закрытый значок замка и переключатель включен, параметр применяется к устройствам, на которых применяется политика. Пользователь не может изменять значения этих параметров в интерфейсе управляемого приложения. Такие параметры называются <i>заблокированными</i> .

Рекомендуется заблокировать параметры политики, которые вы хотите применить к управляемым устройствам. Разблокированные параметры политики могут быть переназначены параметрами приложения "Лаборатории Касперского" на управляемом устройстве.

Вы можете использовать значок замка для выполнения следующих действий:

- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров приложения "Лаборатории Касперского" на управляемом устройстве.

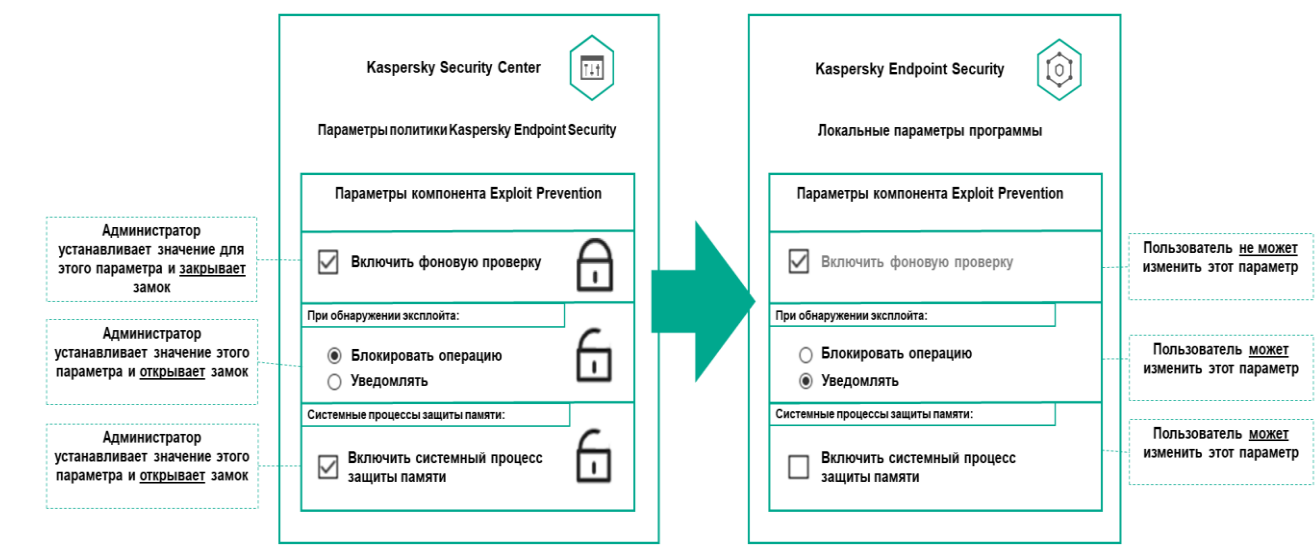
Таким образом, заблокированный параметр используется в эффективных параметрах на управляемом устройстве.

Применение эффективных параметров включает в себя следующие действия:

- Управляемое устройство применяет значения параметров приложения "Лаборатории Касперского".
- Управляемое устройство применяет заблокированные значения параметров политики.

Политика и управляемое приложение "Лаборатории Касперского" содержат одинаковый набор параметров. При настройке параметров политики параметры приложения "Лаборатории Касперского" меняют значения

на управляемом устройстве. Вы не можете изменить заблокированные параметры на управляемом устройстве (см. рисунок ниже):



См. также:

Профили политик в иерархии политик.....	1245
Иерархия политик	1244

Наследование политик и профилей политик

В этом разделе представлена информация об иерархии и наследовании политик и профилей политик.

Иерархия политик

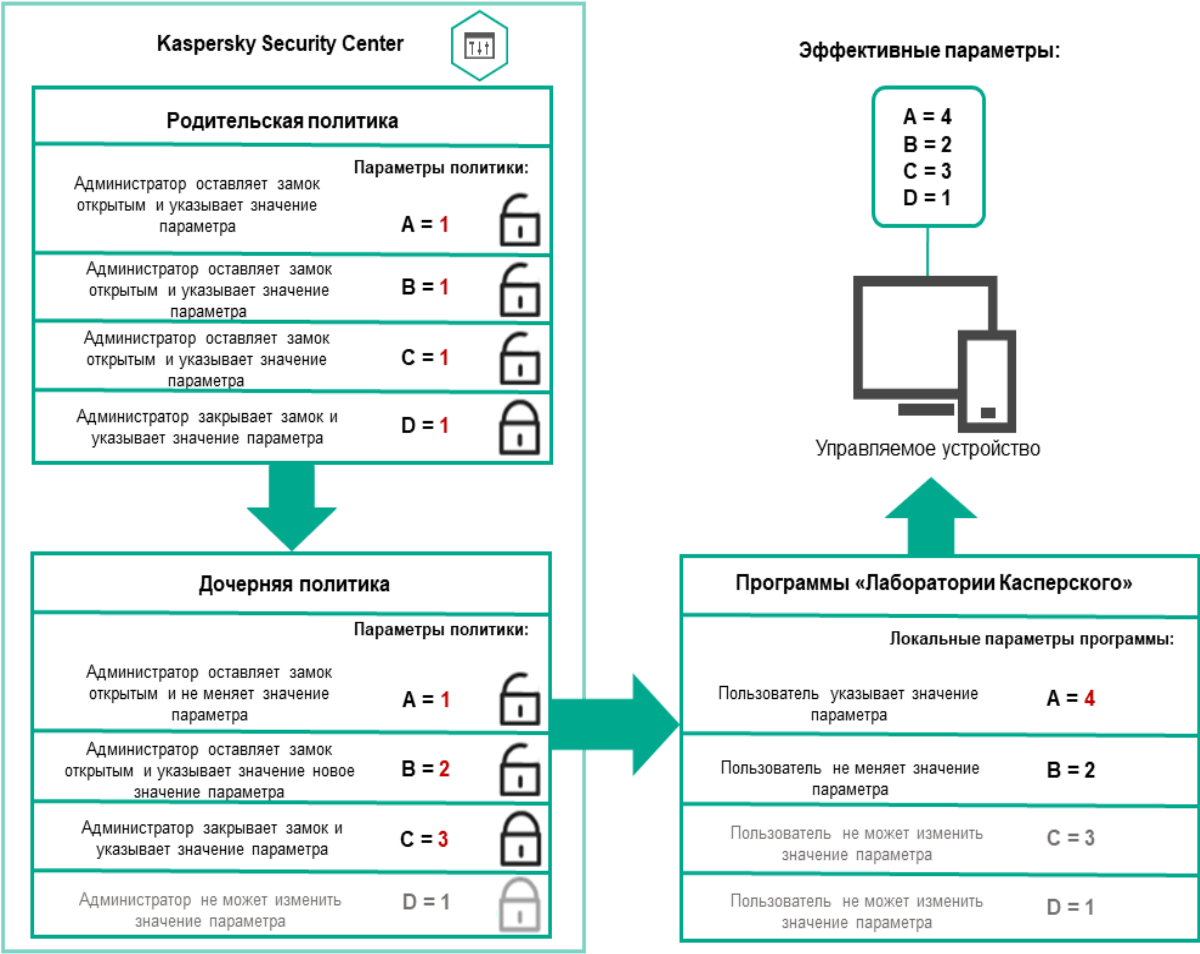
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

Вы можете указать политику для отдельной группы администрирования. Параметры политики можно *унаследовать*. Наследование – это получение значений параметров политики в подгруппах (дочерних группах) от вышестоящей политики (родительской) группы администрирования.

Политика, созданная для родительской группы, также называется *родительской политикой*. Политика, созданная для подгруппы (дочерней группы), также называется *дочерней политикой*.

По умолчанию на Сервере администрирования существует как минимум одна группа администрирования управляемых устройств. Если вы хотите создать группы администрирования, они создаются как подгруппы (дочерние группы) в группе Управляемые устройства.

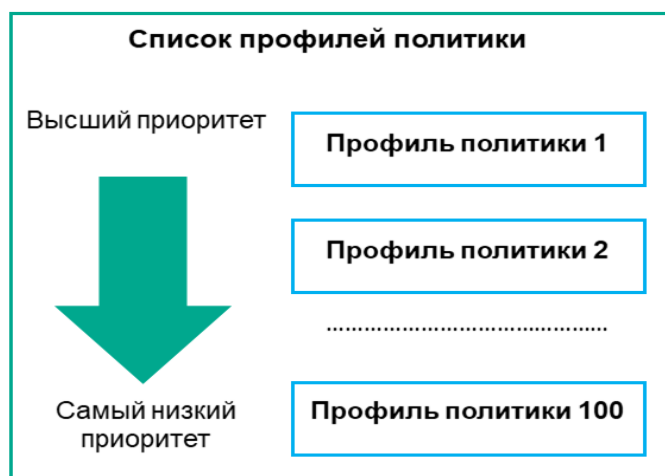
Политики одного и того же приложения действуют друг на друга по иерархии групп администрирования. Заблокированные параметры из политики вышестоящей (родительской) группы администрирования будут переназначать значения параметров политики подгруппы (см. рисунок ниже).



Профили политик в иерархии политик

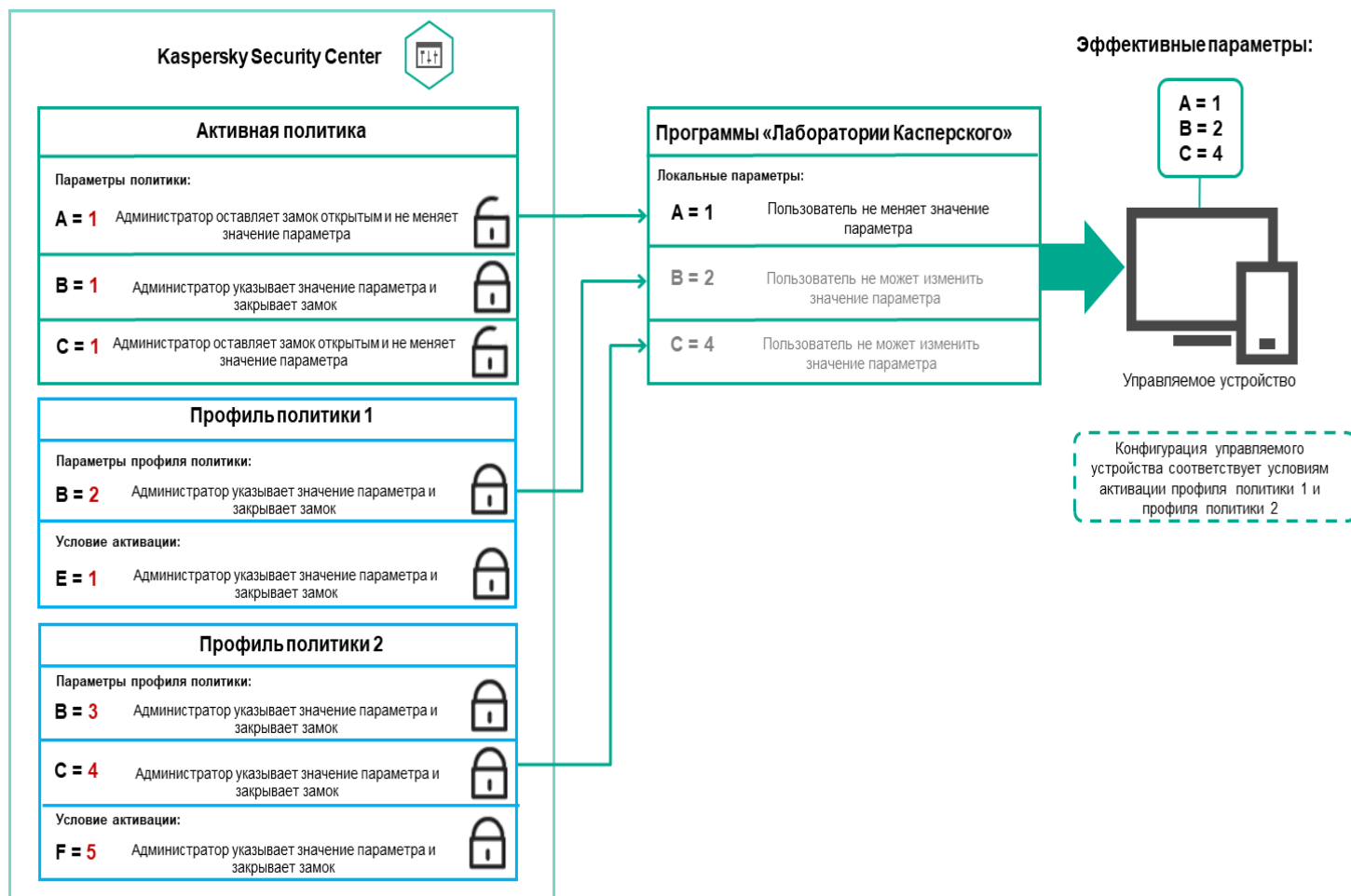
Профили политики имеют следующие условия назначения приоритета:

- Положение профиля в списке профилей политики обозначает его приоритет. Вы можете изменить приоритет профиля политики. Самая высокая позиция в списке обозначает самый высокий приоритет (см. рисунок ниже).



- Условия активации профилей политик не зависят друг от друга. Одновременно можно активировать несколько профилей политик. Если несколько профилей политики влияют на один и тот же

параметр, устройство использует значение параметра из профиля политики с наивысшим приоритетом (см. рисунок ниже).

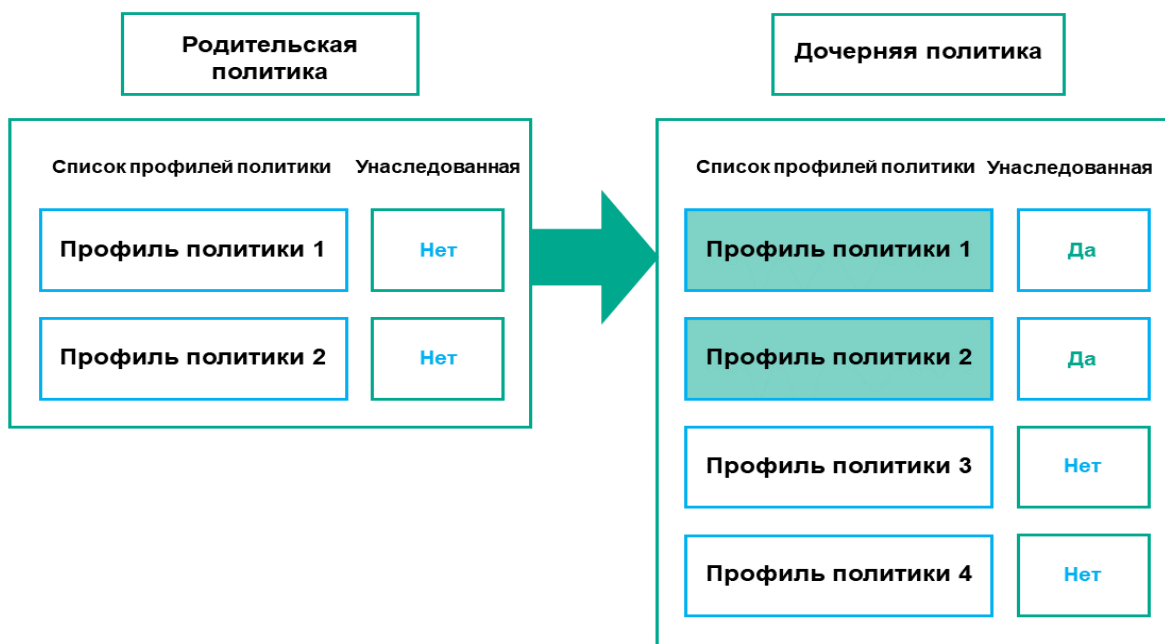


Профили политик в иерархии наследования

Профили политик из политик разных уровней иерархии соответствуют следующим условиям:

- Политика нижнего уровня наследует профили политики из политики более высокого уровня. Профиль политики, унаследованный от политики более высокого уровня, получает более высокий приоритет, чем уровень исходного профиля политики.

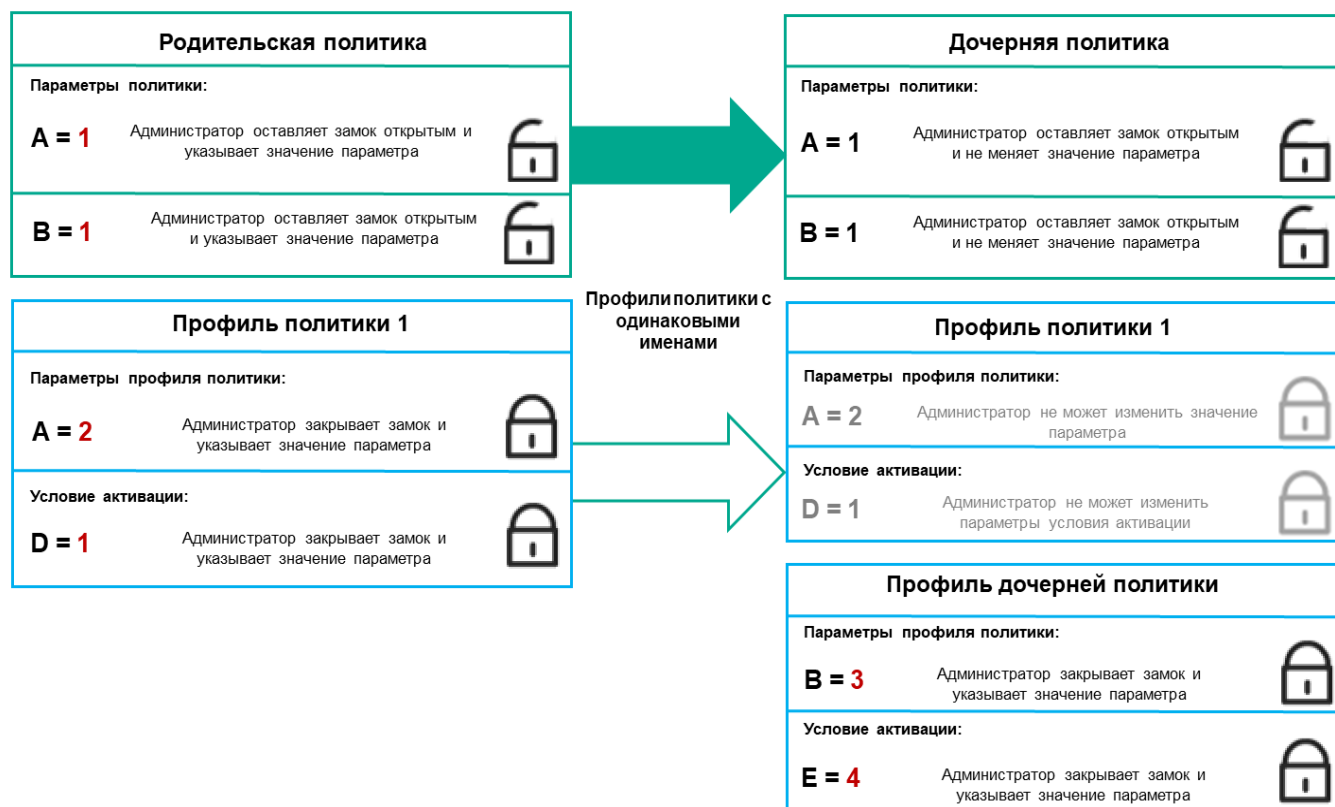
- Вы не можете изменить приоритет унаследованного профиля политики (см. рисунок ниже).



Профили политики с одинаковыми именами

Если на разных уровнях иерархии есть две политики с одинаковыми именами, эти политики работают в соответствии со следующими правилами:

- Заблокированные параметры и условие активации профиля для профиля политики более высокого уровня изменяют параметры и условие активации профиля для профиля политики более низкого уровня (см. рисунок ниже).



- Разблокированные параметры и условие активации профиля для профиля политики более высокого уровня не изменяют параметры и условие активации профиля для профиля политики более низкого уровня.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства[405](#)

Как параметры реализованы на управляемом устройстве

Применения эффективных параметров на управляемом устройстве можно описать следующим образом:

- Значения всех незаблокированных параметров берутся из политики.
- Затем они перезаписываются значениями параметров управляемого приложения.
- Далее применяются заблокированные значения параметров из действующей политики. Значения заблокированных параметров изменяют значения разблокированных действующих параметров.

См. также:

О политиках и профилях политик.....	1241
Блокировка (замок) и заблокированные параметры	1242
Иерархия политик	1244
Профили политик в иерархии политик.....	1245

Управление политиками

В этом разделе описывается управление политиками и предоставляется информация о просмотре списка политик, создании политики, изменении политики, копировании политики, перемещении политики, принудительной синхронизации, просмотре диаграммы состояния распространения политики и удалении политики.

В этом разделе

Просмотр списка политик.....	1251
Создание политики	1251
Изменение политики	1253
Общие параметры политик	1253
Enabling and disabling a policy inheritance option.....	1255
Копирование политики	1256
Перемещение политики	1256
Экспорт политики	1257
Импорт политики	1258
Просмотр диаграммы состояния применения политики	1258
Автоматическая активация политики по событию "Вирусная атака"	1259
Удаление политики	1260

Просмотр списка политик

Вы можете просмотреть список политик, созданных на Сервере администрирования или в любой группе администрирования.

► Чтобы просмотреть список политик:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.
2. В списке групп администрирования выберите группу администрирования, для которой вы хотите просмотреть список политик.

Политики отобразятся в виде таблицы. Если политик нет, отобразится пустая таблица. Вы можете отображать или скрывать столбцы таблицы, изменять их порядок, просматривать только строки, которые содержат указанное вами значение, или использовать поиск.

См. также:

Сценарий: настройка защиты сети.....	403

Создание политики

Вы можете создавать политики; вы можете также изменять или удалять существующие политики.

► *Чтобы создать политику:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Выберите группу администрирования, для которой нужно создать политику:
 - Для корневой группы.
В этом случае вы можете перейти к следующему шагу.
 - Для подгруппы:
 - a. Перейдите по ссылке текущего пути в верхней части окна.
 - b. В открывшейся панели перейдите по ссылке с названием нужной подгруппы.
Текущий путь изменится в соответствии с выбранной подгруппой.
3. Нажмите на кнопку **Добавить**.
Откроется окно **Выберите приложение**.
4. Выберите приложение, для которого требуется создать политику.
5. Нажмите на кнопку **Далее**.
Откроется окно параметров новой политики на вкладке **Общие**.
6. При желании вы можете изменить следующие параметры политики, заданные по умолчанию: имя, состояние и наследование.
7. Выберите вкладку **Параметры приложения**.
Или нажмите на кнопку **Сохранить**, чтобы выйти. Политика появится в списке политик, и вы сможете изменить ее свойства позже.
8. В левой области вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры политики. Вы можете изменить параметры политики в каждом разделе.
Набор параметров зависит от приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:
 - Настройка Сервера администрирования (см. стр. [1016](#))
 - Параметры политики Агента администрирования
 - Документация Kaspersky Endpoint Security для Windows
<https://support.kaspersky.com/KESWin/12.6/en-US/>Подробнее о параметрах других приложений безопасности см. в документации к соответствующему приложению.
Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.
9. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения политики.
В результате добавленная политика отображается в списке политик.

См. также:

Сценарий: развертывание приложений "Лаборатории Касперского"	1084
Настройка и распространение политик: подход, ориентированный на устройства	405
Сценарий: настройка защиты сети.....	403

Изменение политики

► Чтобы изменить политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Выберите политику, которую требуется изменить.
Откроется окно свойств политики.
3. Укажите общие параметры (см. раздел "Общие параметры политик" см. стр. [1253](#)) и параметры приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:
 - Настройка Сервера администрирования (см. стр. [1016](#))
 - Параметры политики Агента администрирования
 - Документация Kaspersky Endpoint Security для Windows
<https://support.kaspersky.com/KESWin/12.6/en-US/>Подробнее о параметрах других приложений безопасности см. в документации к этим приложениям.
4. Нажмите на кнопку **Сохранить**.
Изменения политики будут сохранены в свойствах политики и будут отображаться в разделе **История ревизий**.

См. также:

Сценарий: настройка защиты сети.....	403

Общие параметры политик

Общие

На вкладке **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
 - **Активна**
Если выбран этот вариант, политика становится активной.
По умолчанию выбран этот вариант.
 - **Для автономных пользователей**

Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации. Политика для автономных пользователей доступна только для Антивируса Касперского для Windows Workstations версии 6.0 MP3 и выше.

- **Неактивна**

Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

- В блоке **Наследование параметров** можно настроить параметры наследования политики:

- **Наследовать параметры родительской политики**

Если флажок установлен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

По умолчанию флажок установлен.

- **Обеспечить принудительное наследование параметров для дочерних политик**

Если флажок установлен, после применения изменений в политике будут выполнены следующие действия:

- значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
- в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически установлен флажок **Наследовать параметры политики верхнего уровня**.

Когда флажок установлен, значения параметров дочерних политик недоступны для изменения.

По умолчанию флажок снят.

Настройка событий

На вкладке **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на вкладках:

- **Критическое**
Раздел **Критическое** не отображается в свойствах политики Агента администрирования.
- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). Нажав на тип события, вы можете указать следующие параметры:

- **Регистрация событий**

Вы можете указать количество дней хранения событий и выбрать, где хранить события:

- **Экспортировать в SIEM-систему по протоколу Syslog**
- **Хранить в журнале событий ОС на устройстве**
- **Хранить в журнале событий ОС на Сервере администрирования**
- **Уведомления о событиях**

Вы можете выбрать способ уведомления о событии:

- Уведомлять по электронной почте
- Уведомлять по SMS
- Уведомлять запуском исполняемого файла или скрипта
- Уведомлять по SNMP

По умолчанию используются параметры уведомлений, указанные на вкладке свойств Сервера администрирования (например, адрес получателя). Если вы хотите, измените эти параметры на вкладках **Электронная почта**, **SMS** и **Исполняемый файл для запуска**.

История ревизий

На вкладке **История ревизий** вы можете просмотреть список ревизий политики и изменения, для которых был выполнен откат (см. раздел "Откат изменений объекта к предыдущей ревизии" см. стр. [1323](#)).

См. также:

Сценарий: настройка защиты сети.....[403](#)

Включение и выключение параметра наследования политики

► Чтобы включить или выключить параметр наследования в политике:

1. Откройте требуемую политику.
2. Откройте вкладку **Общие**.
3. Включение или выключение наследования политики:
 - Если вы включили параметр **Наследовать параметры родительской политики** для дочерней группы и администратор заблокировал некоторые параметры в родительской политике, то вы не можете изменить эти параметры политики для дочерней политики.
 - Если вы выключили параметр **Наследовать параметры родительской политики** для дочерней политики, то вы можете изменить все параметры в дочерней политике, даже если некоторые параметры "заблокированы" в родительской политике.
 - Если в родительской группе включен параметр **Обеспечить принудительное наследование параметров для дочерних политик**, это включит параметр **Наследовать параметры родительской политики** для каждой дочерней политики. В этом случае вы не можете выключить этот параметр для дочерних политик. Все параметры, которые заблокированы в родительской политике, принудительно наследуются в дочерних группах, и вы не можете изменить эти параметры в дочерних группах.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, или нажмите на кнопку **Отмена**, чтобы отклонить изменения.

По умолчанию, параметр **Наследовать параметры родительской политики** включен для новой политики.

Если у политики имеются профили, все дочерние политики наследуют эти профили.

См. также:

Иерархия политик	1244
Сценарий: настройка защиты сети.....	403

Копирование политики

Вы можете копировать политики из одной группы администрирования в другую.

► *Чтобы скопировать политику в другую группу администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок напротив политики (или политик), которую требуется скопировать.
3. Нажмите на кнопку **Копировать**.
В правой части экрана отображается дерево групп администрирования.
4. В дереве выберите целевую группу, то есть группу, в которую вы хотите скопировать политику (или политики).
5. Нажмите на кнопку **Копировать** внизу экрана.
6. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Политика (политики) и все ее профили скопированы в целевую группу администрирования. Каждая скопированная политика в целевой группе принимает статус **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

См. также:

Сценарий: настройка защиты сети.....	403

Перемещение политики

Вы можете перемещать политики из одной группы администрирования в другую. Например, вы хотите удалить одну группу администрирования, но использовать ее политики для другой группы администрирования. В этом случае вам может потребоваться, перед удалением старой группы администрирования, переместить политику из старой группы администрирования в новую.

► *Чтобы переместить политику в другую группу администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок напротив политики (или политик), которую требуется переместить.

3. Нажмите на кнопку **Переместить**.

В правой части экрана отображается дерево групп администрирования.

4. В дереве выберите целевую группу администрирования, то есть группу, в которую вы хотите переместить политику (или политики).
5. Нажмите на кнопку **Переместить** внизу экрана.
6. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Если политика не унаследована из группы источника, она будет перемещена в целевую группу со всем профилями политики. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если политика унаследована из группы источника, она останется в группе источника. Политика скопирована в целевую группу со всеми ее профилями. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

См. также:

Сценарий: настройка защиты сети.....[403](#)

Экспорт политики

Kaspersky Security Center позволяет сохранить политику, ее параметры и профили политики в файл KLP. Вы можете использовать файл KLP для импорта сохраненной политики (см. раздел "Импорт политики" на стр. [1258](#)) как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

► Чтобы экспортировать политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок рядом с политикой, которую вы хотите экспортировать.
Невозможно экспортировать несколько политик одновременно. Если вы выберете более одной политики, кнопка **Экспортировать** будет неактивна.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя файла политики и путь. Нажмите на кнопку **Сохранить**.

Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл политики автоматически сохраняется в папку **Загрузки**.

Импорт политики

Kaspersky Security Center позволяет импортировать политику из файла KLP. Файл KLP содержит экспортированную политику (см. раздел "Экспорт политики" см. стр. [1257](#)), ее параметры и профили политики.

► Чтобы импортировать политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на кнопку **Импортировать**.
3. Нажмите на кнопку **Обзор**, чтобы выбрать файл политики, который вы хотите импортировать.
4. В открывшемся окне укажите путь к файлу политики KLP и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл политики.
Начнется обработка политики.
5. После успешной обработки политики выберите группу администрирования, к которой вы хотите применить политику.
6. Нажмите на кнопку **Завершить**, чтобы завершить импорт политики.

Появится уведомление с результатами импорта. Если политика успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств политики.

После успешного импорта политика отображается в списке политик. Также импортируются параметры и профили политики. Независимо от статуса политики, выбранной при экспорте, импортируемая политика неактивна. Вы можете изменить статус политики в свойствах политики.

Если имя новой импортированной политики идентично имени существующей политики, имя импортированной политики расширяется с помощью окончания вида (**<порядковый номер>**), например: **(1)**, **(2)**.

Просмотр диаграммы состояния применения политики

В Kaspersky Security Center вы можете просматривать состояние применения политики на каждом устройстве на диаграмме.

► Чтобы просмотреть статус применения политики на каждом устройстве:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок рядом с именем политики, для которой вы хотите просмотреть состояние применения на устройстве.
3. В появившемся меню выберите ссылку **Результаты применения**.
Откроется окно **Результат распространения <название политики>**.
4. В открывшемся окне **Результат распространения <название политики>** отображается **Описание статуса**.

Вы можете изменить количество результатов, отображаемых в списке результатов применения политики. Максимальное количество устройств равно 100 000.

► *Чтобы изменить количество устройств, отображаемых в списке с результатами применения политики:*

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса**.
2. В поле **Максимальное количество устройств, отображаемых в результатах распространения политики** введите количество устройств (до 100 000).
По умолчанию количество устройств равно 5000.
3. Нажмите на кнопку **Сохранить**.
Параметры сохранены и применены.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Автоматическая активация политики по событию "Вирусная атака"

► *Чтобы политика активировалась автоматически при наступлении события "Вирусная атака":*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования на вкладке **Общие**.
2. Выберите раздел **Вирусная атака**.
3. В правой панели нажмите на ссылку **Настроить активацию политик по возникновению события "Вирусная атака"**.
Откроется окно **Активация политик**.
4. В разделе, к которому относится компонент обнаруживший вирусную атаку (антивирусы для рабочих станций и файловых серверов, антивирусы для почтовых серверов, антивирусы защиты периметра), выберите нужную вам запись и затем нажмите на кнопку **Добавить**.
Откроется окно с группой администрирования **Управляемые устройства**.
5. Нажмите на значок шеврона () рядом с **Управляемые устройства**.
Отобразится иерархия групп администрирования и их политик.
6. В иерархии групп администрирования и их политик нажмите на имя политики (или политик), которая активируется при возникновении вирусной атаки.
Чтобы выбрать все политики в списке или в группе, установите флажок рядом с требуемым именем.
7. Нажмите на кнопку **Сохранить**.
Окно с иерархией групп администрирования и их политиками закрыто.

Выбранные политики добавляются в список политик, которые активируются при возникновении вирусной атаки. Выбранные политики активируются во время вирусной атаки независимо от того, активны они или неактивны.

В случае активации политики по событию Вирусная атака вернуться к предыдущей политике можно только вручную.

См. также:

Сценарий: мониторинг и отчеты.....	1466
Сценарий: настройка защиты сети.....	403

Удаление политики

Вы можете удалить политику, если она больше не нужна. Вы можете удалить только неунаследованную политику в выбранной группе администрирования. Если политика унаследована, вы можете удалить ее только в группе администрирования, в которой она была создана.

► Чтобы удалить политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Установите флажок рядом с именем политики, которую вы хотите удалить, и нажмите на кнопку **Удалить**.
Кнопка **Удалить** становится неактивной (серой), если вы выбрали унаследованную политику.
3. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.
Политика и все ее профили политики удалены.

См. также:

Сценарий: настройка защиты сети.....	403

Управление профилями политик

В этом разделе описывается управление профилями политики и предоставляется информация о просмотре профилей политики, изменении приоритета профиля политики, создании профиля политики, изменении профиля политики, копировании профиля политики, создании правила активации профиля политики и удалении профиля политики.

В этом разделе

Просмотр профилей политики	1261
Изменение приоритета профиля политики	1261
Создание профиля политики	1262
Изменение профиля политики	1263
Копирование профиля политики	1263
Создание правила активации профиля политики	1264
Удаление профиля политики	1267

Просмотр профилей политики

► Чтобы просмотреть профили политики:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Выберите политику, профили которой требуется просмотреть.
Откроется окно свойств политики на вкладке **Общие**.
3. Откройте вкладку **Профили политики**.

Профили политики отобразятся в виде таблицы. Если у политики нет профилей политики, отобразится пустая таблица.

См. также:

Сценарий: настройка защиты сети	403

Изменение приоритета профиля политики

► Чтобы изменить приоритет профиля политики:

1. Перейдите к списку профилей выбранной политики (см. раздел "Просмотр профилей политики" на стр. [1261](#)).
Откроется список профилей политики.

2. На вкладке **Профили политики** установите флажок рядом с профилем политики, для которого требуется изменить приоритет.
3. Установите профиль политики на новую позицию в списке с помощью кнопок **Повысить приоритет** или **Понизить приоритет**.

Чем выше расположен профиль политики в списке, тем выше его приоритет.

4. Нажмите на кнопку **Сохранить**.

Приоритет выбранного профиля политики изменен и применен.

См. также:

Профили политик в иерархии политик.....	1245
Наследование политик и профилей политик	1244
Сценарий: настройка защиты сети.....	403

Создание профиля политики

► Чтобы создать профиль политики:

1. Перейдите к списку профилей выбранной политики (см. раздел "Просмотр профилей политики" на стр. [1261](#)).
Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.
2. Нажмите на кнопку **Добавить**.
3. Если необходимо, измените заданные по умолчанию имя и параметры наследования профиля политики.
4. Выберите вкладку **Параметры приложения**.
Можно также нажать на кнопку **Сохранить**, чтобы выйти. Созданный профиль политики отобразится в списке профилей политики, и вы сможете изменить его свойства позже.
5. В левой области вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры профиля политики. Вы можете изменить параметры профиля политики в каждом разделе.
Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения профиля.
Профиль политики отобразится в списке профилей политики.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства	405
Сценарий: настройка защиты сети.....	403

Изменение профиля политики

Изменение профиля доступно только для политик Kaspersky Endpoint Security для Windows.

► Чтобы изменить профиль политики:

1. Перейдите к списку профилей выбранной политики (см. раздел "Просмотр профилей политики" на стр. [1261](#)).

Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, который вы хотите изменить.
В результате откроется окно свойств профиля политики.

3. В окне свойств настройте параметры профиля:

- Если необходимо, на вкладке **Общие** измените имя профиля политики и включите или выключите профиль.
- Измените правила активации профиля политики (см. раздел "Создание правила активации профиля политики" см. стр. [1264](#)).
- Измените остальные параметры.

Подробнее о параметрах приложений безопасности см. в документации к соответствующему приложению.

4. Нажмите на кнопку **Сохранить**.

Измененные параметры начнут действовать после синхронизации устройства с Сервером администрирования (если профиль политики активен) либо после выполнения правила активации (если профиль политики неактивен).

См. также:

Сценарий: настройка защиты сети.....[403](#)

Копирование профиля политики

Вы можете скопировать профиль политики в текущую политику или в другую политику, например, если вы хотите иметь идентичные профили политик для разных политик. Вы также можете использовать копирование, если хотите иметь два или более профилей политики, которые отличаются небольшим количеством параметров.

► Чтобы скопировать профиль политики:

1. Перейдите к списку профилей выбранной политики (см. раздел "Просмотр профилей политики" на стр. [1261](#)).

Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.

2. На вкладке **Профили политики** выберите профиль, который требуется скопировать.
3. Нажмите на кнопку **Копировать**.

4. В открывшемся окне выберите политику, в которую требуется скопировать профиль политики.

Вы можете скопировать профиль политики в эту же политику или в политику, которую вы выбрали.

5. Нажмите на кнопку **Копировать**.

Профиль политики скопирован в политику, которую вы выбрали. Новый скопированный профиль политики имеет самый низкий приоритет. Если вы скопировали профиль политики в эту же политику, к имени такого профиля добавляется окончание вида (<порядковый номер>), например: (1), (2).

Позже вы можете изменить параметры профиля политики, включая его имя и приоритет. В этом случае исходный профиль политики не будет изменен.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Создание правила активации профиля политики

► Чтобы создать правило активации профиля политики:

1. Перейдите к списку профилей выбранной политики (см. раздел "Просмотр профилей политики" на стр. [1261](#)).

Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, для которого требуется создать правило активации.

Если список профилей политики пуст, вы можете создать профиль политики (см. раздел "Создание профиля политики" см. стр. [1262](#)).

3. На вкладке **Правила активации** нажмите на кнопку **Добавить**.

Откроется окно с правилами активации профиля политики.

4. Укажите имя правила активации.
5. Установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

- **Общие правила активации профиля политики**

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

Для этого параметра на следующем шаге укажите:

- **Статус устройства**

Определяет условие присутствия устройства в сети:

- **В сети** – устройство находится в сети, Сервер администрирования доступен.
- **Не в сети** – устройство находится во внешней сети, то есть Сервер администрирования недоступен.
- **Неизвестно** – критерий не применяется.

- **Правило подключения к Серверу администрирования активно на этом устройстве**

Выберите условие для активации профиля политики (независимо от того, выполняется ли это правило или нет) и выберите имя правила.

Правило определяется сетевым местоположением устройства для подключения к Серверу администрирования, при выполнении или невыполнении условий которого профиль политики будет активирован.

Описание сетевого местоположения устройств для подключения к Серверу администрирования можно создать или настроить в правиле переключения Агента администрирования.

- **Правила для выбранного владельца устройства**

Для этого параметра на следующем шаге укажите:

- **Владелец устройства**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- устройство принадлежит указанному владельцу (знак "=");
- устройство не принадлежит указанному владельцу (знак "≠").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Владелец устройства включен во внутреннюю группу безопасности**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky Security Center. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- владелец устройства является членом указанной группы безопасности (знак "=");
- владелец устройства не является членом указанной группы безопасности (знак "≠").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky Security Center, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Правила для характеристик оборудования**

Установите флажок, чтобы настроить условие активации на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

Для этого параметра на следующем шаге укажите:

- **Объем оперативной памяти (МБ)**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- объем оперативной памяти устройства меньше указанного значения (знак "<");
- объем оперативной памяти устройства больше указанного значения (знак ">").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной

памяти устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Количество логических процессоров**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- количество логических процессоров устройства меньше или равно указанному значению (знак "<");
- количество логических процессоров устройства больше или равно указанному значению (знак ">").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Правила для назначения роли**

Для этого параметра на следующем шаге укажите:

Активировать профиль политики по наличию роли у владельца устройства

Включите этот параметр, чтобы настроить и включить правило активации профиля политики на устройстве в зависимости от наличия определенной роли у его владельца. Добавить роль вручную из списка существующих ролей.

Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием.

- **Правила для использования тега**

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от тегов, назначенных устройству. Вы можете активировать профиль политики либо на устройствах, которые имеют выбранные теги, либо не имеют их.

Для этого параметра на следующем шаге укажите:

- **Тег**

В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

- **Применить к устройствам без выбранных тегов**

Установите флажок, если необходимо инвертировать выбор тегов.

Если флажок установлен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если флажок снят, критерий не применяется. По умолчанию флажок снят.

- **Правила для использования Active Directory**

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от размещения устройства в подразделении Active

Directory или же от членства устройства или его владельца в группе безопасности Active Directory.

Для этого параметра на следующем шаге укажите:

- **Членство владельца устройства в группе безопасности Active Directory**

Если флажок установлен, профиль политики активируется на устройстве, владелец которого является членом указанной группы безопасности или членом групп безопасности, входящих в указанную группу. Вы можете указать группу безопасности Active Directory, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Членство устройства в группе безопасности Active Directory**

Если флажок установлен, профиль политики активируется на устройстве, которое является членом указанной группы безопасности или членом групп безопасности, входящих в указанную группу. Вы можете указать группу безопасности Active Directory, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Размещение устройства в подразделении Active Directory**

Если флажок установлен, профиль политики активируется на устройстве, которое явно или неявно входит в указанное подразделение Active Directory. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.

6. Проверьте список настроенных параметров. Если список верен, нажмите на кнопку **Создать**.

В результате профиль будет сохранен. Профиль будет активирован на устройстве, когда будут выполнены правила активации.

Правила активации профиля политики, созданные для профиля, отображаются в свойствах профиля политики на вкладке **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства	405
Сценарий: настройка защиты сети.....	403

Удаление профиля политики

► Чтобы удалить профиль политики:

1. Перейдите к списку профилей выбранной политики (см. раздел "Просмотр профилей политики" на стр. [1261](#)).

Откроется список профилей политики.

2. На странице **Профили политики** установите флажок рядом с профилем политики, который вы хотите удалить, и нажмите на кнопку **Удалить**.
3. В появившемся окне нажмите на кнопку **Удалить** еще раз.

Профиль политики удален. Если политика наследуется группой более низкого уровня, профиль политики остается в этой группе, но становится профилем политики этой группы. Это позволяет уменьшить изменения в параметрах управляемых приложений, установленных на устройствах групп нижнего уровня.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Шифрование и защита данных.

Шифрование данных снижает риски непреднамеренной утечки информации в случае кражи/утери портативного устройства или жесткого диска, или при доступе к данным неавторизованных пользователей и приложений.

Шифрование поддерживают следующие приложения «Лаборатории Касперского»:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Mac

Вы можете отобразить или скрыть некоторые элементы интерфейса, связанные с управлением шифрованием, с помощью параметров пользовательского интерфейса (см. раздел "Настройка интерфейса" на стр. [1024](#)).

Шифрование данных в Kaspersky Endpoint Security для Windows

Можно управлять следующими типами шифрования:

- шифрование диска BitLocker на устройствах под управлением операционной системы Windows для серверов;
- шифрование диска Kaspersky на устройствах под управлением операционной системы Windows для рабочих станций.

С помощью этих компонентов Kaspersky Endpoint Security для Windows вы можете, например, включать или выключать шифрование, просматривать список зашифрованных жестких дисков, формировать и просматривать отчеты о шифровании.

Вы управляете шифрованием, настраивая политики Kaspersky Endpoint Security для Windows в Kaspersky Security Center. Kaspersky Endpoint Security для Windows выполняет шифрование и расшифровку в соответствии с активной политикой. Подробные инструкции по настройке правил и описание особенностей шифрования см. в онлайн-справке Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/KESWin/12.6/en-US/196002.htm>.

Шифрование данных в Kaspersky Endpoint Security для Mac

Вы можете использовать шифрование FileVault на устройствах с операционными системами macOS. При работе с Kaspersky Endpoint Security для Mac вы можете включить или выключить это шифрование.

Вы управляете шифрованием, настраивая политики Kaspersky Endpoint Security для Mac в Kaspersky Security Center. Kaspersky Endpoint Security для Mac выполняет шифрование и расшифровку в соответствии с активной политикой. Подробное описание функций шифрования см. в онлайн-справке Kaspersky Endpoint Security для Mac https://support.kaspersky.com/KESMac/11.2.1_adminguide/en-US/159877.htm.

См. также:

Сценарий: настройка защиты сети.....[403](#)

В этом разделе

Просмотр списка зашифрованных жестких дисков[1269](#)

Просмотр списка событий шифрования[1269](#)

Формирование и просмотр отчетов о шифровании.....[1270](#)

Предоставление доступа к зашифрованному жесткому диску в автономном режиме[1271](#)

Просмотр списка зашифрованных жестких дисков

В Kaspersky Security Center вы можете просмотреть информацию о зашифрованных жестких дисках и об устройствах, зашифрованных на уровне дисков. После того, как информация на диске будет расшифрована, диск будет автоматически удален из списка.

► Чтобы просмотреть список зашифрованных жестких дисков,

В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса (см. раздел "Настройка интерфейса" на стр. [1024](#)) включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Просмотр списка событий шифрования

В процессе выполнения задач шифрования или расшифровки данных на устройствах Kaspersky Endpoint Security для Windows отправляет в Kaspersky Security Center информацию о возникающих событиях следующих типов:

- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за нехватки места на диске;

- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за проблем с лицензией;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за отсутствия прав доступа;
- приложению запрещен доступ к зашифрованному файлу;
- неизвестные ошибки.

► *Чтобы просмотреть список событий, возникших при шифровании данных на устройствах:*

В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **События шифрования**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса (см. раздел "Настройка интерфейса" на стр. [1024](#)) включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Также можно просмотреть список событий шифрования для каждого управляемого устройства.

► *Чтобы просмотреть события шифрования управляемого устройства:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя управляемого устройства.
3. На вкладке **Общие** перейдите в раздел **Защита**.
4. Перейдите по ссылке **Просмотреть ошибки шифрования данных**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Формирование и просмотр отчетов о шифровании

Вы можете формировать следующие отчеты:

- Отчет о статусе шифрования управляемых устройств. В этом отчете представлены сведения о шифровании данных различных управляемых устройств. Например, в отчете показано количество устройств, к которым применяется политика с настроенными правилами шифрования. Также можно узнать, например, сколько устройств нужно перезагрузить. Отчет также содержит информацию о технологии и алгоритме шифрования для каждого устройства.
- Отчет о статусе шифрования запоминающих устройств. Этот отчет содержит похожую информацию, что и отчет о состоянии шифрования управляемых устройств, но предоставляет данные только для запоминающих устройств и съемных дисков.
- Отчет о правах доступа к зашифрованным дискам. Этот отчет показывает, какие учетные записи пользователей имеют доступ к зашифрованным жестким дискам.

- Отчет об ошибках шифрования файлов. Отчет содержит информацию об ошибках, которые возникли при выполнении задач шифрования или расшифровки данных на устройствах.
- Отчет о блокировании доступа к зашифрованным файлам. Отчет содержит информацию о блокировке доступа приложений к зашифрованным файлам. Этот отчет полезен, если неавторизованный пользователь или приложение пытается получить доступ к зашифрованным файлам или жестким дискам.

Вы можете сгенерировать любой отчет (см. раздел "Генерация и просмотр отчета" см. стр. [1479](#)) в разделе **Мониторинг и отчеты** → **Отчеты**. Также в разделе **Операции** → **Шифрование и защита данных**, можно создавать следующие отчеты о шифровании:

- Отчет о статусе шифрования запоминающих устройств
- Отчет о правах доступа к зашифрованным дискам
- Отчет об ошибках шифрования файлов

► *Чтобы сгенерировать отчет шифрования в разделе **Шифрование и защита данных**:*

1. Убедитесь, что параметр **Показать раздел "Шифрование и защита данных"** в параметрах интерфейса (см. раздел "Настройка интерфейса" на стр. [1024](#)) включен.
2. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных**.
3. Откройте один из следующих разделов:
 - **Зашифрованные жесткие диски** – формирует отчет о состоянии шифрования запоминающих устройств или отчет о правах доступа к зашифрованным жестким дискам.
 - **События шифрования** – формирует отчет об ошибках шифрования файлов.
4. Выберите название отчета, который требуется сгенерировать.

Запустится процесс формирования отчета.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Предоставление доступа к зашифрованному жесткому диску в автономном режиме

Пользователь может запросить доступ к зашифрованному устройству, например, если Kaspersky Endpoint Security для Windows не установлен на управляемом устройстве. После получения запроса вы можете создать файл ключа доступа и отправить его пользователю. Все варианты использования и подробные инструкции приведены в онлайн-справке Kaspersky Endpoint Security для Windows.

► *Чтобы предоставить доступ к зашифрованному жесткому диску в автономном режиме:*

1. Получите файл запроса доступа от пользователя (файл с расширением FDERTC). Следуйте инструкциям в онлайн-справке Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/KESWin/12.6/en-US/130941.htm>, чтобы сгенерировать файл в Kaspersky Endpoint Security для Windows.
2. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

Отобразится список зашифрованных жестких дисков.

3. Выберите диск, у которому пользователь запросил доступ.
4. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
5. В открывшемся окне выберите плагин, соответствующий приложению "Лаборатории Касперского", которое использовалось для шифрования выбранного диска.

Если жесткий диск зашифрован с помощью приложения "Лаборатории Касперского", которое не поддерживается Kaspersky Security Center Web Console, используйте Консоль администрирования на основе консоли управления Microsoft Management Console (MMC), чтобы предоставить доступ к диску в автономном режиме.

6. Следуйте инструкциям, приведенным в онлайн-справке Kaspersky Endpoint Security для Windows <https://support.kaspersky.com/KESWin/12.6/en-US/130941.htm> (см. раскрывающиеся блоки в конце раздела).

После этого пользователь может использовать полученный файл для доступа к зашифрованному жесткому диску и чтения данных, хранящихся на диске.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Пользователи и роли пользователей

В этом разделе описана работа с пользователями и ролями пользователей, а также приведены инструкции по их созданию и изменению, назначению пользователям ролей и групп и связи профилей политики с ролями.

В этом разделе

О ролях пользователей	1274
Просмотр учетных записей и сеансов пользователей.....	1274
Настройка прав доступа к функциям приложения Управление доступом на основе ролей	1275
Добавление учетной записи внутреннего пользователя.....	1308
Создание группы безопасности	1309
Изменение учетной записи внутреннего пользователя.....	1310
Изменение группы безопасности	1310
Назначение роли пользователю или группе безопасности	1311
Добавление учетных записей пользователей во внутреннюю группу безопасности	1311
Назначение пользователя владельцем устройства	1313
Удаление пользователей или групп безопасности	1313
Изменение пароля учетной записи пользователя.....	1314
Создание роли пользователя	1316
Изменение роли пользователя.....	1316
Изменение области для роли пользователя.....	1317
Удаление роли пользователя	1318
Связь профилей политики с ролями ...	1318
Смена пароля учетной записи	1319
Отзыв прав локального администратора	1321

См. также:

Сценарий: настройка защиты сети	403

О ролях пользователей

Роль пользователя (далее также *роль*) это объект, содержащий набор прав и разрешений. Роль может быть связана с параметрами приложений "Лаборатории Касперского", которые установлены на устройстве пользователя. Вы можете назначить роль набору пользователей или набору групп безопасности на любом уровне иерархии групп администрирования, Серверов администрирования либо на уровне конкретных объектов (см. раздел "Назначение прав доступа к набору объектов" см. стр. [1305](#)).

Если вы управляете устройствами с помощью иерархии Серверов администрирования, в которую входят виртуальные Серверы администрирования, обратите внимание, что вы можете создавать, изменять и удалять пользовательские роли только на физическом Сервере администрирования. Затем вы можете распространить пользовательские роли на подчиненные Серверы администрирования, в том числе виртуальные Серверы.

Вы можете связывать роли с профилями политик. Если пользователю назначена роль, этот пользователь получает параметры безопасности, требуемые для выполнения служебных обязанностей.

Роль пользователя может быть связана с устройствами пользователей заданной группы администрирования

Область роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Преимущество использования ролей

Преимущество использования ролей заключается в том, что вам не нужно указывать параметры безопасности для каждого управляемого устройства или для каждого из пользователей отдельно. Количество пользователей и устройств в компании может быть большим, но количество различных функций работы, требующих разных настроек безопасности, значительно меньше.

Отличия от использования профилей политики

Профили политики – это свойства политики, созданной для каждого приложения "Лаборатории Касперского" отдельно. Роль связана со многими профилями политики, которые созданы для разных приложений. Таким образом, роль – это метод объединения параметров для определенного типа пользователя.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Просмотр учетных записей и сеансов пользователей

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами учетных записей. Приложение поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих пользователей при опросе сети организации.

- Учетные записи внутренних пользователей. Применяются для работы с виртуальными Серверами администрирования. Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center.

Вы можете просмотреть список учетных записей и сеансов пользователей одним из следующих способов:

- В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
- В главном меню перейдите в раздел **Активы (Устройства)** → **Управляемые устройства** → ссылка <название устройства> → вкладка **Общие** → раздел **Общие** → блок **Сеансы**.

В разделе **Сеансы** отображаются учетные записи пользователей с активными сеансами на устройствах под управлением Windows.

Список учетных записей и сеансов пользователей отображается правильно, если выполнены следующие требования:

- Используется Агент администрирования той же версии, что и Сервер администрирования, или выше.
- Опрос Active Directory включен для отображения учетных записей пользователей домена.
- На управляемых устройствах под управлением Windows работает служба **Сервера (LanmanServer)**.

Настройка прав доступа к функциям приложения Управление доступом на основе ролей

Kaspersky Security Center предоставляет доступ на основе ролей к функциям Kaspersky Security Center и к функциям управляемых приложений «Лаборатории Касперского».

Вы можете настроить права доступа к функциям приложения (на стр. [1276](#)) для пользователей Kaspersky Security Center одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей (см. раздел "О ролях пользователей" на стр. [1274](#)) с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

Применение ролей пользователей облегчает и сокращает рутинные действия по настройке прав доступа пользователей к приложению. Права доступа в роли настраивают в соответствии с типовыми задачами и служебными обязанностями пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В приложении можно создавать неограниченное количество ролей.

Вы можете использовать предопределенные роли (см. раздел "Предопределенные роли пользователей" на стр. [1301](#)) пользователей с уже настроенным набором прав или создавать роли (см. раздел "Создание роли пользователя" на стр. [1316](#)) и самостоятельно настраивать необходимые права.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Права доступа к функциям приложения

В таблице ниже приведены функции Kaspersky Security Center с правами доступа для управления задачами, отчетами, параметрами и для выполнения действий пользователя.

Для выполнения действий пользователя, перечисленных в таблице, у пользователя должно быть право, указанное рядом с действием.

Права на **Чтение**, **Запись** и **Выполнение** применимы к любой задаче, отчету или параметрам. В дополнение к этим правам у пользователя должно быть право **Выполнение операций с выборками устройств** для управления задачами, отчетами или изменения параметров выборок устройств.

Функциональная область **Общие функции: Доступ к объектам независимо от их списков ACL** предназначена для аудита. Когда пользователям предоставляется право **Чтение** в этой функциональной области, они получают полный доступ на **Чтение** ко всем объектам и могут выполнять любые созданные задачи на выбранных устройствах, подключенных к Серверу администрирования через Агент администрирования с правами локального администратора (root для Linux). Рекомендуется предоставлять эти права ограниченному кругу пользователей, которым они нужны для выполнения своих служебных обязанностей. Все задачи, отчеты, параметры и инсталляционные пакеты, отсутствующие в таблице, относятся к области **Общие функции: Базовая функциональность**.

Таблица 92. Права доступа к функциям приложения

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Управление группами администрирования	Запись.	- Добавление устройства в группу администрирования: Запись. - Удаление устройства из состава группы администрирования: Запись. - Добавление группы администрирования в другую группу администрирования: Запись. - Удаление группы администрирования из другой группы администрирования: Запись.	Отсутствует.	Отсутствует.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Доступ к объектам независимо от их списков ACL	Чтение.	Получение доступа на чтение ко всем объектам: Чтение.	Отсутствует.	Отсутствует.	Доступ предоставляется независимо от других прав, даже если они запрещают доступ на чтение к определенным объектам.

Общие функции: Базовая функциональность	• Чтение. • Запись. • Выполнение. • Выполнение действий над выборками и устройств.	• Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: Запись, Выполнение действий над выборками и устройств. • Получение мобильного протокола пользователя сертификата (LWNGT): Чтение. • Установка мобильного протокола пользователя сертификата (LWNGT): Запись. • Получить список сетей, определенных NLA: Чтение. • Добавить, изменить или удалить список сетей, определенных NLA: Запись. • Просмотр списка контроля	• Загрузка обновлений в хранилище Сервера администрирования. • Рассылка отчетов. • Распространение инсталляционных пакетов. • Установка приложений на подчиненные Серверы администрирования.	• Отчет о состоянии защиты. • Отчет об угрозах. • Отчет о наиболее зараженных устройствах. • Отчет о статусе антивирусных баз. • Отчет об ошибках. • Отчет о сетевых атаках. • Сводный отчет о приложениях для защиты почтовых систем. • Сводный отчет о приложениях для защиты периметра. • Сводный отчет о типах установленных приложений. • Отчет о пользователях зараженных устройств. • Отчет об инцидентах. • Отчет о событиях.	Отсутствует.

		доступа групп: Чтение. Просмотрите журнал событий Kaspersky Event Log: Чтение.		- Отчет о работе точек распространения. - Отчет о подчиненных Серверах администрирования. - Отчет о событиях Контроля устройств. - Отчет об уязвимостях. - Отчет о запрещенных приложениях. - Отчет о работе Веб-Контроля. - Отчет о статусе шифрования управляемых устройств. - Отчет о статусе шифрования запоминающих устройств. - Отчет об ошибках шифрования файлов. - Отчет о блокировании доступа к зашифрованным файлам.	

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
				- Отчет о правах доступа к зашифрованным устройствам. - Отчет об эффективных правах пользователя. - Отчет о правах.	
Общие функции: Удаленные объекты	- Чтение. - Запись.	- Просмотр удаленных объектов в корзине: Чтение. - Удаление объектов из корзины: Запись.	Отсутствует.	Отсутствует.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Обработка событий	- Удаление событий. - Изменение параметра в уведомлении о событиях. - Изменение параметра в записи событий в журнал событий. - Запись.	- Изменение параметра в регистрации и событий: Изменение параметра в записи событий в журнал событий. - Изменение параметра в уведомлении о событиях: Изменение параметра в уведомлении о событиях. - Удаление событий: Удаление событий.	Отсутствует.	Отсутствует.	Параметры: - Параметры вирусной атаки: количество обнаружений вирусов, необходимое для создания события вирусной атаки. - Параметры вирусной атаки: период для оценки обнаружения вирусов. - Максимальное количество событий, хранящихся в базе данных. - Период хранения событий удаленных устройств.

Общие функции: Операции с Сервером администрирования	• Чтение. • Запись. • Выполнение. • Изменение списков ACL объекта. • Выполнение действий над выборкам и устройств.	• Изменение портов Сервера администрирования для подключения Агента администрирования: Запись. • Изменение портов прокси-сервера активации, запущенного на Сервере администрирования: Запись. • Изменение портов прокси-сервера активации для мобильных устройств, запускаемых на Сервере администрирования: Запись. • Изменение портов Веб-сервера для распространения автономных пакетов: Запись. • Изменение портов Веб-сервера для распространения iOS	• Резервное копирование данных Сервера администрирования. • Обслуживание базы данных.	Отсутствует.	Отсутствует.

		MDM-профилей: Запись. • Изменение SSL-портов Сервера администрирования для подключения с помощью Kaspersky Security Center Web Console: Запись. • Изменение портов Сервера администрирования для подключения мобильных устройств: Запись. • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования: Запись. • Укажите максимальное количество событий, которое может отправлять Сервер администрирования: Запись.			

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
		Изменение периода, в течение которого Сервер администрирования может отправлять события: Запись.			

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Развертывание приложений "Лаборатории Касперского"	- Управление патчами "Лаборатории Касперского". - Чтение. - Запись. - Выполнение. - Выполнение действий над выборками и устройств.	Одобрить или отклонить установку патча: Управление патчами "Лаборатории Касперского".	Отсутствует.	- Отчет об использовании лицензионных ключей виртуальным Сервером администрирования. - Отчет о версиях приложений "Лаборатории Касперского". - Отчет о несовместимых приложениях. - Отчет о версиях обновлений модулей приложений "Лаборатории Касперского". - Отчет о развертывании защиты.	Инсталляционный пакет: "Приложения Лаборатории Касперского"

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Управление лицензионными ключами	- Экспорт файл ключа. - Запись.	- Экспорт файл ключа: Экспорт файл ключа. - Изменение параметра в лицензионного ключа Сервера администрирования: Запись.	Отсутствует.	Отсутствует.	Отсутствует.
Общие функции: Управление отчетами	- Чтение. - Запись.	- Создание отчетов для объектов независимо от их списков ACL: Запись. - Выполнять отчеты независимо от их списков ACLs: Чтение.	Отсутствует.	Отсутствует.	Отсутствует.
Общие функции: Иерархия Серверов администрирования	Настройка иерархии Серверов администрирования	Добавление, обновление или удаление подчиненных Серверов администрирования: Настройка иерархии Серверов администрирования.	Отсутствует.	Отсутствует.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: Права пользователя	Изменение списков ACL объекта.	- Изменение свойств Безопасности любого объекта: Изменение списков ACL объекта. - Управление ролями пользователей: Изменение списков ACL объекта. - Управление внутренними пользователями: Изменение списков ACL объекта. - Управление группами безопасности: Изменение списков ACL объекта. - Управление псевдонимами: Изменение списков ACL объекта.	Отсутствует.	Отсутствует.	Отсутствует.

Общие функции: Виртуальные Серверы администрирования	• Управление виртуальными Серверами и администрирования. • Чтение. • Запись. • Выполнение. • Выполнение действий над выборками и устройств.	• Получение списка виртуальных Серверов администрирования: Чтение. • Получение информации о виртуальном Сервере администрирования: Чтение. • Создание, обновление или удаление виртуального Сервера администрирования: Управление виртуальными Серверами и администрирования. • Перемещение виртуального Сервера администрирования в другую группу: Управление виртуальными Серверами и администрирования. • Установка прав доступа к виртуальному Серверу администр	Отсутствует.	Отчет о результатах установки обновлений стороннего ПО.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
		ирования: Управление виртуальными Серверами и администрирования.			
Общие функции: Управление ключами шифрования	Запись.	Импорт ключей шифрования: Запись.	Отсутствует.	Отсутствует.	Отсутствует.

Управление мобильным и устройствам и: Общие	• Подключение новых устройств. • Отправка только информационных команд на мобильные устройства. • Отправка команд на мобильные устройства. • Управление сертификатами • Чтение. • Запись.	• Получение восстановленных данных службы управления ключами: Чтение. • Удаление сертификатов пользователей: Управление сертификатами. • Получение публичной части сертификата пользователя: Чтение. • Проверка, включены ли инфраструктура открытых ключей: Чтение. • Проверка учетной записи инфраструктуры открытых ключей: Чтение. • Получение шаблонов инфраструктуры открытых ключей: Чтение. • Получение шаблонов инфраструктуры открытых ключей с	Отсутствует.	Отсутствует.	Отсутствует.

		помощью расширенн ого использова ния ключа (EКУ) сертификат а: Чтение. • Проверка, не отозван ли сертификат инфраструк туры открытых ключей: Чтение. • Обновлени е параметро в выпуска сертификат ов пользовате ля: Управлени е сертифика тами. • Получение параметро в выпуска сертификат ов пользовате ля: Чтение. • Получение пакетов по названию и версиям приложени й: Чтение. • Установка или отмена сертификат ов пользовате ля: Управлени е сертифика тами.			

Функциональная область	Право	Действие пользователя: право, необходимо для выполнения действия	Задача	Отчет	Другое
		- Обновление сертификата пользователя: Управление сертификатами. - Установка тега для сертификата пользователя: Управление сертификатами. - Запуск генерации инсталляционного пакета, содержащего iOS MDM-профиль; отмена генерации инсталляционного пакета, содержащего iOS MDM-профиль: Подключение новых устройств.			

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Управление системой: Подключения	- Запуск RDP-сессий. - Подключение к существующим RDP-сессиям. - Туннелирование. - Сохранение файлов с устройств на рабочем месте администратора. - Чтение. - Запись. - Выполнение. - Выполнение действий над выборками и устройств.	- Создание сеанса совместного доступа к рабочему столу: Право на создание сеанса совместного доступа к рабочему столу. - Создание RDP-сессии: Подключение к существующим RDP-сессиям. - Создание туннеля: Туннелирование. - Сохранение списка сетей: Сохранение файлов с устройств на рабочем месте администратора.	Отсутствует.	Отчет о пользователях устройства.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Управление системой: Инвентаризация оборудования	- Чтение. - Запись. - Выполнение. - Выполнение действий над выборками и устройств.	- Получение или экспорт объектов инвентаризации оборудования: Чтение. - Добавление, установка или удаление объектов инвентаризации оборудования: Запись.	Отсутствует.	- Отчет о реестре оборудования. - Отчет об изменении конфигурации. - Отчет об оборудовании.	Отсутствует.
Управление системой: Управление доступом в сеть	- Чтение. - Запись.	- Просмотр параметра в Cisco: Чтение. - Изменение параметра в Cisco: Запись.	Отсутствует.	Отсутствует.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимо для выполнения действия	Задача	Отчет	Другое
Управление системой: Развертывание операционной системы	- Развертывание PXE-серверов. - Чтение. - Запись. - Выполнение. - Выполнение действий над выборками и устройств.	- Развертывание PXE-серверов: Развертывание PXE-серверов. - Просмотр списка PXE-серверов: Чтение. - Запуск или остановка процесс установки на PXE-клиентах: Выполнение. - Управление драйверами для среды WinPE и образов операционной системы: Запись.	Создание инсталляционного пакета на основе образа ОС эталонного устройства.	Отсутствует.	Инсталляционный пакет: Образ операционной системы.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Управление системой: Системное администрирование	- Чтение. - Запись. - Выполнение. - Выполнение действий над выборками и устройств.	- Просмотр свойства патчей сторонних производителей: Чтение. - Изменение свойства патчей сторонних производителей: Запись.	- Выполнение синхронизации обновлений Центра обновлений Windows. - Установка обновлений Центра обновлений Windows. - Закрытие уязвимостей. - Установка требуемых обновлений и закрытия уязвимостей.	Отчет об обновлениях ПО.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Управление системой: Удаленная установка	• Чтение. • Запись. • Выполнение. • Выполнение действий над выборками и устройств.	• Просмотр Системного администрирования стороннего производителя на основе свойств инсталляционного пакета: Чтение. • Изменение Системного администрирования на основе свойств инсталляционного пакета: Запись.	Отсутствует.	Отсутствует.	Инсталляционные пакеты: • Пользовательское приложение. • Пакет VAPM.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Управление системой: Инвентаризация приложений	• Чтение. • Запись. • Выполнение. • Выполнение действий над выборками и устройств.	Отсутствует.	Отсутствует.	• Отчет об установленных приложениях. • Отчет об истории реестра приложений. • Отчет о состоянии групп лицензионных приложений. • Отчет о лицензионных ключах сторонних приложений.	Отсутствует.

Управление системой: Удаленное выполнение скриптов	• Чтение. • Запись. • Выполнение. • Выполнение действий над выборками и устройств.	Пользователь может просматривать свойства задачи: Чтение. Пользователь может создать, удалить или изменить инсталляционный пакет: Запись. Пользователь может запустить задачу: Запись. На клиентских устройствах с операционной системой Linux скрипты выполняются с правами root. Пользователь может запустить задачу или запланировать ее запуск: Выполнение. Пользователь может запустить задачу на выбранных устройствах: Выполнение действий над выборками устройств.	"Удаленное выполнение скриптов"	Отсутствует.	Отсутствует.

См. также:

Сценарий: настройка защиты сети.....403

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center, предоставляют им набор прав доступа к функциям приложения.

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права. Некоторые из предопределенных ролей пользователей, доступных в Kaspersky Security Center, могут быть связаны с определенными должностями, например, **Аудитор**, **Специалист по безопасности**, **Контролер** (эти роли присутствуют в Kaspersky Security Center начиная с версии 11). Права доступа этих ролей предварительно настраиваются в соответствии со стандартными задачами и обязанностями соответствующих должностей. В таблице ниже показано как роли могут быть связаны с определенными должностями.

Таблица 93. Примеры ролей для определенных должностей

Роль	Комментарий
Аудитор	Разрешено выполнение любых операций со всеми типами отчетов, а также всех операций просмотра, включая просмотр удаленных объектов (предоставлены права Чтение и Запись для области Удаленные объекты). Другие операции не разрешены. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.
Контролер	Разрешен просмотр всех операций, не разрешены другие операции. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Специалист по безопасности	Разрешены всех операции просмотра, разрешено управление отчетами; предоставлены ограниченные права в области Управление системой: Подключения . Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.

В таблице ниже приведены права для каждой предопределенной роли пользователя.

Таблица 94. Права предопределенных ролей пользователей

Роль	Описание
Администратор Сервера администрирования	Разрешает все операции в следующих функциональных областях: • Общие функции: • Базовая функциональность. • Обработка событий. • Иерархия Серверов администрирования. • Виртуальные Серверы администрирования. • Управление системой: • Подключения. • Инвентаризация оборудования. • Инвентаризация приложений. Предоставляет права на Чтение и Запись в области Общие функции: Управление ключами шифрования.
Оператор Сервера администрирования	Предоставляет права на Чтение и Выполнение во всех следующих функциональных областях: • Общие функции: • Базовая функциональность. • Виртуальные Серверы администрирования. • Управление системой: • Подключения. • Инвентаризация оборудования. • Инвентаризация приложений.
Аудитор	Разрешает все операции в функциональной области Общий функционал: • Доступ к объектам независимо от их списков ACL. • Удаленные объекты. • Управление отчетами. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.

Роль	Описание
Администратор установки приложений	Разрешает все операции в следующих функциональных областях: • Общие функции: • Базовая функциональность. • Развертывание приложений "Лаборатории Касперского". • Управление лицензионными ключами. • Управление системой: • Развертывание операционной системы. • Системное администрирование. • Удаленная установка. • Инвентаризация приложений. Предоставляет права на Чтение и Выполнение в области Общий функционал: Базовая функциональность.
Оператор установки приложений	Предоставляет права на Чтение и Выполнение во всех следующих функциональных областях: • Общие функции: • Базовая функциональность. • Развертывание приложений "Лаборатории Касперского" (также предоставляет права на Управление патчами "Лаборатории Касперского" в этой же области). • Виртуальные Серверы администрирования. • Управление системой: • Развертывание операционной системы. • Системное администрирование. • Удаленная установка. • Инвентаризация приложений.
Администратор Kaspersky Endpoint Security	Разрешает все операции в следующих функциональных областях: • Общие функции: Базовая функциональность. • Область Kaspersky Endpoint Security, включая все функции. Предоставляет права на Чтение и Запись в области Общие функции: Управление ключами шифрования.
Оператор Kaspersky Endpoint Security	Предоставляет права на Чтение и Выполнение во всех следующих функциональных областях: • Общие функции: Базовая функциональность. • Область Kaspersky Endpoint Security, включая все функции.

Роль	Описание
Главный администратор	Разрешает все операции в функциональных областях, за исключением следующих областей: Общие функции: • Доступ к объектам независимо от их списков ACL. • Управление отчетами. Предоставляет права на Чтение и Запись в области Общие функции: Управление ключами шифрования.
Главный оператор	Предоставляет права на Чтение и Выполнение (если применимо) во всех следующих функциональных областях: • Общие функции: • Базовая функциональность. • Удаленные объекты. • Операции с Сервером администрирования. • Развертывание приложений "Лаборатории Касперского" • Виртуальные Серверы администрирования. • Управление мобильными устройствами: Общие • Управление системой, включая все функции. • Область Kaspersky Endpoint Security, включая все функции.
Администратор управления мобильными устройствами	Разрешает все операции в следующих функциональных областях: • Общие функции: Базовая функциональность. • Управление мобильными устройствами: Общие.
Оператор управления мобильными устройствами	Предоставляет права на Чтение и Выполнение в области Общие функции: Базовая функциональность. Предоставляет права на Чтение и Отправление только информационных команд на мобильные устройства в функциональной области: Управление мобильными устройствами: Общие.
Специалист по безопасности	Разрешает все операции в следующих функциональных областях: Общие функции: • Доступ к объектам независимо от их списков ACL. • Управление отчетами. Предоставляет права на Чтение, Запись, Выполнение, Сохранение файлов с устройств на рабочем месте администратора и Выполнение операций с выборками устройств в области Управление системой: Подключения. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.

Роль	Описание
Пользователь Self Service Portal	Разрешает все операции в области Управление мобильными устройствами: Self Service Portal . Эта функция не поддерживается в версиях приложения Kaspersky Security Center 11 и выше.
Контролер	Предоставляет права на Чтение в области Общие функции: Доступ к объектам независимо от их списков ACL и Общие функции: функциональная область Управление отчетами . Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Администратор Системного администрирования	Разрешает все операции в области Общие функции: Базовая функциональность и Управление системой (включая все функции).
Оператор Системного администрирования	Предоставляет права на Чтение и Выполнение (если применимо) в области Общие функции: Базовая функциональность и Управление системой (включая все функции).

См. также:

Сценарий: настройка защиты сети.....[403](#)

Назначение прав доступа к набору объектов

В дополнение к назначению прав доступа на уровне сервера (см. раздел "Права доступа к функциям приложения" на стр. [1276](#)), вы можете настроить доступ к конкретным объектам, например, к требуемой задаче. Приложение позволяет указать права доступа к следующим типам объектов:

- Группы администрирования
- Задачи
- Отчеты
- Выборки устройств
- Выборки событий

► Чтобы назначить права доступа к конкретному объекту:

1. В зависимости от типа объекта в главном меню перейдите в соответствующий раздел:
 - **Активы (Устройства)** → **Иерархия групп**.
 - **Активы (Устройства)** → **Задачи**.
 - **Мониторинг и отчеты** → **Отчеты**.

- **Активы (Устройства) → Выборки устройств.**
 - **Мониторинг и отчеты → Выборки событий.**
2. Откройте свойства объекта, к которому вы хотите настроить права доступа.
Чтобы открыть окно свойств группы администрирования или задачи, нажмите на название объекта. Свойства других объектов можно открыть с помощью кнопки в панели инструментов.
 3. В окне свойств откройте раздел **Права доступа**.
Откроется список пользователей. Перечисленные пользователи и группы безопасности имеют права доступа к объекту. Если вы используете иерархию групп администрирования или Серверов, список и права доступа по умолчанию наследуются от родительской группы администрирования или главного Сервера.
 4. Чтобы иметь возможность изменять список, включите параметр **Использовать права пользователей**.
 5. Настройте права доступа:
 - Используйте кнопки **Добавить** и **Удалить** для изменения списка.
 - Укажите права доступа для пользователя или группы безопасности. Выполните одно из следующих действий:
 - Если вы хотите указать права доступа вручную, выберите пользователя или группу безопасности, нажмите на кнопку **Права доступа** и укажите права доступа.
 - Если вы хотите назначить пользовательскую роль (см. раздел "О ролях пользователей" см. стр. [1274](#)) пользователю или группе безопасности, выберите пользователя или группу безопасности, нажмите на кнопку **Роли** и выберите роль для назначения.
 6. Нажмите на кнопку **Сохранить**.
- Права доступа к объекту настроены.

См. также:

Настройка прав доступа к функциям приложения Управление доступом на основе ролей.....	1275
Права доступа к функциям приложения	1276
Предопределенные роли пользователей.....	1301

Назначение прав пользователям или группам безопасности

Вы можете назначить права доступа пользователям или группам безопасности, чтобы использовать различные возможности Сервера администрирования, например Kaspersky Endpoint Security для Linux.

► *Чтобы назначить права доступа пользователю или группе безопасности:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которым нужно назначить права, а затем нажмите на кнопку **Права доступа**.

Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Права доступа** будет неактивна.

3. Настройте набор прав для пользователя или группы:

- a. Разверните узел с функциями Сервера администрирования или другого приложения "Лаборатории Касперского".
- b. Установите флажок **Разрешить** или **Запретить** рядом с нужной функцией или правом доступа.

Пример 1: Установите флажок **Разрешить** рядом с узлом **Интеграции приложения**, чтобы предоставить пользователю или группе все доступные права доступа к функции интеграции приложения (**Чтение**, **Запись** и **Выполнение**).

Пример 2: Разверните узел **Управление ключами шифрования** и установите флажок **Разрешить** рядом с разрешением **Запись**, чтобы предоставить пользователю или группе право доступа на **Запись** к функции управления ключами шифрования.

4. После настройки набора прав доступа нажмите на кнопку **ОК**.

Набор прав для пользователя или группа пользователей настроен.

Права Сервера администрирования (или группы администрирования) разделены на следующие области:

- Общие функции:
 - Управление группами администрирования
 - Доступ к объектам независимо от их списков ACL
 - Базовая функциональность
 - Удаленные объекты
 - Управление ключами шифрования
 - Обработка событий
 - Операции с Сервером администрирования (только в окне свойств Сервера администрирования)
 - Теги устройств
 - Развертывание приложений "Лаборатории Касперского"
 - Управление лицензионными ключами
 - Интеграция приложения
 - Управление отчетами
 - Иерархия Серверов администрирования
 - Права пользователей
 - Виртуальные Серверы администрирования
- Управление мобильными устройствами:
 - Общие
 - Self Service Portal
- Управление системой:
 - Подключения
 - Удаленное выполнение скриптов

- Инвентаризация оборудования
- Network Access Control
- Развертывание операционной системы
- Системное администрирование
- Удаленная установка
- Инвентаризация приложений

Если для права не выбрано ни **Разрешить**, ни **Запретить**, оно считается *неопределенным*: право отклоняется до тех пор, пока оно не будет явно отклонено или разрешено для пользователя.

Права пользователей являются суммой следующего:

- собственных прав пользователя;
- прав всех ролей, назначенных пользователю;
- прав всех групп безопасности, в которые входит пользователь;
- прав всех ролей, назначенных группам, в которые входит пользователь.

Если хотя бы в одном наборе прав есть запрещенное право (для права установлен флажок **Запретить**), тогда для пользователя это право запрещено, даже если в других наборах прав оно разрешено или не определено.

Также вы можете добавить пользователей и группы безопасности (см. раздел "Изменение области для роли пользователя" см. стр. [1317](#)) в область пользовательской роли, чтобы использовать различные возможности Сервера администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Добавление учетной записи внутреннего пользователя

Если вы хотите добавить учетную запись пользователя, убедитесь, что у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области Общий функционал: Права пользователей.

► Чтобы добавить новую учетную запись пользователя Kaspersky Security Center:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Добавить пользователя** укажите параметры нового пользователя:
 - **Имя**
 - **Пароль**

Пароль должен соответствовать следующим правилам:

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп списка ниже:
 - верхний регистр (A-Z);
 - нижний регистр (A-Z) (a-z);
 - числа (0-9);
 - специальные символы (@ # \$ % ^ & * - _ ! + = [] { } | : ' , . ? / \ ` ~ " () ;)
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

Чтобы посмотреть введенный пароль, нажмите на кнопку .

Вы можете включить параметр **Пользователю надо сменить пароль при первом входе**, чтобы принудительно изменить пароль при первой аутентификации пользователя.

4. Сохраните изменения для завершения создания учетной записи пользователя.

Учетная запись пользователей добавлена в список пользователей.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Создание группы безопасности

► Чтобы создать группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Создать группу безопасности** укажите следующие параметры новой группы безопасности:
 - **Имя группы**
 - **Описание**
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Группа безопасности добавлена в список групп.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Изменение учетной записи внутреннего пользователя

Если вы хотите изменить учетную запись пользователя, убедитесь, что у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области Общий функционал: Права пользователей.

► Чтобы изменить учетную запись внутреннего пользователя Kaspersky Security Center:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
 2. Выберите учетную запись пользователя, которую требуется изменить.
 3. В открывшемся окне на вкладке **Общие** измените параметры учетной записи пользователя:
 - **Статус пользователя**
 - **Имя**
 - **Полное имя**
 - **Описание**
 - **Адрес электронной почты**
 - **Основной телефон**
 - **Пароль**
 4. На вкладке **Дополнительные настройки безопасности** вы можете указать параметры безопасности для этой учетной записи.
 5. На вкладке **Группы** можно добавить пользователя или группу безопасности.
 6. На вкладке **Устройства** можно назначить устройства (см. раздел "Назначение пользователя владельцем устройства" см. стр. [1313](#)) пользователю.
 7. На вкладке **Роли** можно назначить роль (см. раздел "Изменение области для роли пользователя" см. стр. [1317](#)) пользователю.
 8. Сохраните изменения для завершения изменения учетной записи пользователя.
- Измененная учетная запись пользователя отобразится в списке пользователей.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Изменение группы безопасности

► Чтобы изменить группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Выберите группу безопасности, которую требуется изменить.

3. В открывшемся окне измените параметры группы безопасности:

- На вкладке **Общие** можно изменить параметры **Имя** и **Описание**. Эти параметры доступны только для внутренних групп безопасности.
- На вкладке **Пользователи** можно добавить пользователей в группу безопасности (см. раздел "Добавление учетных записей пользователей во внутреннюю группу безопасности" см. стр. [1311](#)). Эти параметры доступны только для внутренних пользователей и внутренних групп безопасности.
- На вкладке **Роли** можно назначить роль группе безопасности.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Изменения применены к группе безопасности.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Назначение роли пользователю или группе безопасности

► Чтобы назначить роли пользователю или группе безопасности:

1. В главном окне приложения перейдите в раздел **У Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.
2. Выберите имя пользователя или группы безопасности, которой нужно назначить роль.
Можно выбрать несколько имен.
3. В меню нажмите на кнопку **Назначить роль**.
Будет запущен мастер назначения роли.
4. Следуйте инструкциям мастера: выберите роль, которую вы хотите назначить выбранным пользователям или группам безопасности, и выберите область действия роли.
Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

В результате роль с набором прав для работы с Сервером администрирования будет назначена пользователю (или пользователям, или группе безопасности). В списке пользователей или групп безопасности отображается флажок в столбце **Имеет назначенные роли**.

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Добавление учетных записей пользователей во внутреннюю группу безопасности

Учетные записи внутренних пользователей можно добавлять только во внутреннюю группу безопасности.

► *Чтобы добавить учетные записи пользователей в группу безопасности:*

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Установите флажки напротив учетных записей пользователей, которые требуется добавить в группу безопасности.
3. Нажмите на кнопку **Назначить группу**.
4. В открывшемся окне **Назначить группу** выберите группу безопасности, в которую требуется добавить учетные записи пользователей.
5. Нажмите на кнопку **Сохранить**.

Учетные записи пользователей добавлены в группу безопасности. Также можно добавить внутренних пользователей в группу безопасности, используя параметры группы (см. раздел "Изменение группы безопасности" см. стр. [1310](#)).

См. также:

| Сценарий: настройка защиты сети.....[403](#)

Назначение пользователя владельцем устройства

Информацию о назначении пользователя владельцем мобильного устройства см. в справке Kaspersky Security для мобильных устройств <https://support.kaspersky.com/KESMob/10SP4MR3/en-US/214537.htm>.

► Чтобы назначить пользователя владельцем устройства:

1. Если вы хотите назначить владельца устройства, подключенного к виртуальному Серверу администрирования, сначала переключитесь на виртуальный Сервер администрирования:
 - а. В главном меню нажмите на значок шеврона (▶) справа от текущего имени Сервера администрирования.
 - б. Выберите требуемый Сервер администрирования.
2. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

Откроется список пользователей. Если вы в данный момент подключены к виртуальному Серверу администрирования, в список входят пользователи текущего виртуального Сервера администрирования и главного Сервера администрирования.
3. Нажмите на учетную запись пользователя, которую требуется назначить в качестве владельца устройству.
4. В открывшемся окне свойств пользователя выберите вкладку **Устройства**.
5. Нажмите на кнопку **Добавить**.
6. Из списка устройств выберите устройство, которое вы хотите назначить пользователю.
7. Нажмите на кнопку **ОК**.

Выбранное устройство добавляется в список устройств, назначенных пользователю.

Также можно выполнить эту операцию в группе **Активы (Устройства)** → **Управляемые устройства**, выбрав имя устройства, которое вы хотите назначить, и перейдя по ссылке **Сменить владельца устройства**.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Удаление пользователей или групп безопасности

Можно удалять только внутренних пользователей или группы безопасности.

► Удаление пользователей или групп безопасности:

1. В главном окне приложения перейдите в раздел **У Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.
2. Установите флажок рядом с именем пользователя или группы безопасности, которую требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Пользователь или группа безопасности удалены.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Изменение пароля учетной записи пользователя

Вам может потребоваться изменить пароль своей учетной записи или учетной записи другого пользователя, если срок действия текущего пароля истекает или если вы хотите сменить его на более надежный.

Пароль должен соответствовать следующим правилам:

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп списка ниже:
 - верхний регистр (A-Z);
 - нижний регистр (a-z);
 - числа (0-9);
 - специальные символы (@ # \$ % ^ & * - _ ! + = [] { } | : ' , . ? / \ ` ~ " () ;)
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

Изменение пароля своей учетной записи

► Чтобы изменить пароль вашей учетной записи:

1. В главном меню перейдите в параметры своей учетной записи и выберите **Изменение пароля**.
2. Введите текущий пароль и укажите новый пароль для подключения к Kaspersky Security Center.
Чтобы посмотреть введенный пароль, нажмите на кнопку .
3. Если ваша учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите учетные данные вашей учетной записи или учетной записи, у которой есть право Изменение списков управления доступом объектов в функциональной области Общий функционал: Права пользователей.

4. Если двухэтапная проверка включена для учетной записи (см. раздел "Включение двухэтапной проверки для вашей учетной записи" на стр. [1036](#)), которую вы использовали на предыдущем шаге, введите код безопасности, сгенерированный приложением для аутентификации на мобильном устройстве.

Изменение пароля учетной записи внутреннего пользователя

► Чтобы изменить пароль учетной записи внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Выберите учетную запись пользователя, которую требуется изменить.
3. В открывшемся окне свойств пользователя на вкладке **Общие** нажмите на кнопку **Изменение пароля**.
4. Установите новый пароль для подключения пользователя к Kaspersky Security Center.
Чтобы посмотреть введенный пароль, нажмите на кнопку .
5. При необходимости включите параметр **Пользователю надо сменить пароль при первом входе**, чтобы принудительно изменить пароль при следующей аутентификации пользователя.
6. Если учетная запись пользователя защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите учетные данные учетной записи, у которой есть право Изменение списков управления доступом объектов в функциональной области Общий функционал: Права пользователей.

Настройка параметров изменения пароля с помощью флагов сервера

Используя утилиту klscflag, вы можете настроить изменение пароля с помощью следующих команд:

- Настройка периода замены пароля (флаг LP_SplPwdChangePeriodDays).

```
klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <rotation_period>
```

где <rotation_period> – это период в днях, по истечении которого срок действия пароля пользователя истекает. Возможные значения: 0–730. Если значение параметра указано 0, смена пароля выключена.

- Настройка времени предыдущего предупреждения о необходимости изменения пароля (флаг LP_SplPwdChangeNotificationHours).

```
klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <warning_time>
```

где <warning_time> – это период в часах, перед тем как срок действия пароля пользователя истечет. В течение этого времени отображается уведомление о необходимости изменить пароль. Возможные значения: 0–17520. Если значение параметра указано 0, время предупреждения составляет 25% от периода замены пароля.

Чтобы просмотреть текущее значение флага, выполните следующую команду:

```
klscflag.exe -fget -pv klserver -n <flag> -t d
```

где <flag> – это флаг LP_SplPwdChangePeriodDays или флаг LP_SplPwdChangeNotificationHours.

Создание роли пользователя

► Чтобы создать роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
 2. Нажмите на кнопку **Добавить**.
 3. В открывшемся окне **Имя новой роли** укажите имя новой роли.
 4. Нажмите на кнопку **ОК**, чтобы применить изменения.
 5. В открывшемся окне измените параметры роли:
 - На вкладке **Общие** измените имя роли.
Вы не можете изменять имена предопределенных ролей.
 - На вкладке **Параметры** измените область действия роли (см. раздел "Изменение области для роли пользователя" см. стр. [1317](#)), а также политики и профили политик, связанные с ролью.
 - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".
 6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.
- Созданная роль появится в списке ролей пользователей.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Изменение роли пользователя

► Чтобы изменить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
 2. Выберите роль, которую требуется изменить.
 3. В открывшемся окне измените параметры роли:
 - На вкладке **Общие** измените имя роли.
Вы не можете изменять имена предопределенных ролей.
 - На вкладке **Параметры** измените область действия роли (см. раздел "Изменение области для роли пользователя" см. стр. [1317](#)), а также политики и профили политик, связанные с ролью.
 - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".
 4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.
- Обновленная роль появится в списке ролей пользователей.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Изменение области для роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

► Чтобы добавить пользователей, группы безопасности и группы администрирования в область роли пользователя, воспользуйтесь одним из следующих способов:

► *Способ 1:*

1. В главном окне приложения перейдите в раздел **У Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.
2. Установите флажки напротив имен пользователей или групп безопасности, которые требуется добавить в область роли.
3. Нажмите на кнопку **Назначить роль**.
Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. На шаге **Выбор роли** выберите роль, которую требуется назначить.
5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.
6. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

► *Способ 2:*

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, для которой требуется задать область.
3. В открывшемся окне свойств роли выберите вкладку **Параметры**.
4. В разделе **Область действия роли** нажмите на кнопку **Добавить**.
Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.
5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.
6. На шаге **Выбор пользователей** выберите пользователей и группы безопасности, которые требуется добавить в область роли.
7. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.
8. Нажмите на кнопку **Закрыть** (X), чтобы закрыть окно свойств.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

► Способ 3:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которым вы хотите добавить область пользовательской роли, и нажмите на кнопку **Роли**.

Вы не можете выбрать нескольких пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Роли** будет неактивна.

3. В окне **Роли** выберите пользовательскую роль, которую вы хотите назначить, примените и сохраните изменения.

Выбранные пользователи или группы безопасности добавлены в область роли.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Удаление роли пользователя

► Чтобы удалить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Установите флажок напротив роли, которую требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Роль пользователя будет удалена.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Связь профилей политики с ролями

Вы можете связывать роли с профилями политик. В этом случае правило активации для профиля политики определяется в зависимости от роли: профиль политики становится активным для пользователя с определенной ролью.

Например, политика запрещает запуск приложений городской навигации для всех устройств группы администрирования. Приложения городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". В этом случае можно назначить роль (см. раздел "О ролях пользователей" см. стр. [1274](#)) "Курьер" владельцу этого устройства и создать профиль политики, разрешающий использовать приложения городской навигации на устройствах, владельцам которых назначена роль "Курьер". Все остальные параметры политики остаются

без изменений. Только пользователям с ролью "Курьер" разрешено использовать приложения городской навигации. Затем, если другому сотруднику будет назначена роль "Курьер", этот сотрудник также сможет использовать приложения городской навигации на устройстве, принадлежащем вашей организации. Однако использование приложений городской навигации будет запрещено на других устройствах этой группы администрирования.

► *Чтобы связать роль с профилем политики:*

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется связать с профилем политики.
Откроется окно свойств роли на вкладке **Общие**.
3. Перейдите на вкладку **Параметры** и прокрутите вниз до раздела **Политики и профили политик**.
4. Нажмите на кнопку **Изменить**.
5. Чтобы связать роль с:
 - **Существующим профилем политики** – нажмите на значок (>) рядом с именем требуемой политики, а затем установите флажок рядом с профилем политики, с которым вы хотите связать роль.
 - **Новым профилем политики:**
 - a. Установите флажок около политики, для которой вы хотите создать профиль политики.
 - b. Нажмите на кнопку **Новый профиль политики**.
 - c. Укажите имя нового профиля политики и настройте параметры профиля политики.
 - d. Нажмите на кнопку **Сохранить**.
 - e. Установите флажок рядом с новым профилем политики.
6. Нажмите на кнопку **Назначить роли**.

Выбранный профиль политики связывается с ролью и появляется в свойствах роли. Профиль автоматически применяется ко всем устройствам, владельцам которых назначена эта роль.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Смена пароля учетной записи

Вы можете изменить пароль локальной учетной записи, например, когда пользователь забыл пароль локальной учетной записи или чтобы изменить пароль по расписанию.

Изменение пароля будет применяться, даже если пользователь не вошел в учетную запись. Вы также можете изменить пароль для локальной учетной записи root.

Эту задачу можно выполнять только на устройствах под управлением Linux.

► Чтобы изменить пароль локальной учетной записи на определенных устройствах:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Изменить пароль учетной записи (только для Linux)**.
4. Выберите один из следующих вариантов:

- **Назначить задачу группе администрирования**

Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- **Задать адреса устройств вручную или импортировать из списка**

Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Задача *Изменить пароль учетной записи (только для Linux)* создается для указанных устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На шаге **Введите имя учетной записи и новый пароль** укажите следующие параметры:

- В поле **Имя учетной записи** укажите имя учетной записи, для которой вы хотите изменить пароль.
- В поле **Новый пароль** укажите пароль, который будет установлен для учетной записи, указанной в предыдущем поле.

Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

- При необходимости установите флажок **Установить в качестве одноразового пароля (пользователь должен изменить пароль после первого входа в систему)**.
 - **Установить в качестве одноразового пароля (пользователь должен изменить пароль после первого входа в систему)**

7. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

8. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

Когда задача изменения пароля учетной записи завершится, пароль будет изменен для указанной локальной учетной записи на выбранных устройствах.

Чтобы обеспечить корректную работу задач изменения пароля учетной записи, на пользовательском устройстве должен быть выключен SELinux.

Отзыв прав локального администратора

Вы можете отозвать права локального администратора для учетных записей. Это дает вам дополнительный уровень контроля учетных записей пользователей. Например, вы можете отозвать права локального администратора после завершения разового назначения.

При запуске этой задачи указанная локальная учетная запись проверяется на принадлежность к локальным группам администраторов, которые определены в параметрах политики Агента (см. раздел "Параметры политики Агента администрирования" на стр. [1145](#)) администрирования. Вы можете настроить список локальных групп администраторов в параметрах политики Агента администрирования. Вы также можете проверить список учетных записей привилегированных пользователей, используя **Отчет о привилегированных пользователях устройств (только для Linux)**.

Эту задачу можно выполнять только на устройствах под управлением Linux.

► Чтобы отозвать права локального администратора на определенных устройствах:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Отозвать права локального администратора (только для Linux)**.
4. Выберите один из следующих вариантов:
 - **Назначить задачу группе администрирования**

Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- **Задать адреса устройств вручную или импортировать из списка**

Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Для указанных устройств создается задача *Отозвать права локального администратора (только для Linux)*. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На этом шаге мастера укажите следующие параметры:

- В группе параметров **Режим работы** выберите режим работы:
 - **Отозвать права локального администратора для перечисленных учетных записей**
 - **Исключить перечисленные учетные записи из списка отзыва прав локального администратора**
- Укажите локальные учетные записи:
 - Нажмите на кнопку **Добавить**.
 - В открывшемся окне выполните одно из следующих действий:
 - В поле **Имя учетной записи** укажите имя локальной учетной записи.
 - В группе параметров **Действие учетной записи** (доступно, если выбран параметр **Отозвать права локального администратора для перечисленных учетных записей**) выберите действие.
 - **Сохранить учетную запись**
 - **Удалить учетную запись**

7. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

8. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

После завершения задачи права локального администратора отозваны для указанных локальных учетных записей на выбранных устройствах.

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов. Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия*. Каждая ревизия имеет номер.

Объекты приложения, которые поддерживают работу с ревизиями:

- свойства Сервера администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- просматривать выбранную ревизию (см. раздел "Просмотр и сохранение ревизии политики" см. стр. [1324](#)) (доступно только для политик);
- откатывать изменения объекта (см. раздел "Откат изменений объекта к предыдущей ревизии" см. стр. [1323](#)) к выбранной ревизии;
- сохранять ревизии в виде файла JSON (см. раздел "Просмотр и сохранение ревизии политики" см. стр. [1324](#)) (доступно только для политик).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- **Ревизия** – номер ревизии объекта.
- **Время** – дата и время изменения объекта.
- **Пользователь** – имя пользователя, изменившего объект.
- **IP-адрес устройства пользователя** – IP-адрес устройства, с которого был изменен объект.
- **IP-адрес Web Console** – IP-адрес приложения Kaspersky Security Center Web Console, с помощью которого был изменен объект.
- **Действие** – выполненное действие с объектом.
- **Описание** – описание ревизии (см. раздел "Добавление описания ревизии" см. стр. [1324](#)) изменения параметров объекта.

По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

► *Чтобы откатить изменения объекта:*

1. В окне свойств объекта перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, к которой нужно откатить изменения.
3. Нажмите на кнопку **Откатить**.
4. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Операция отката доступна только для политик и задач.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Добавление описания ревизии

Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается ревизия. Каждая ревизия имеет номер.

Вы можете добавить описание для ревизии, чтобы в дальнейшем было проще найти необходимую ревизию в списке.

► *Чтобы добавить описание ревизии:*

1. В окне свойств объекта (см. раздел "Работа с ревизиями объектов" на стр. [1323](#)) перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, для которой нужно добавить описание.
3. Нажмите на кнопку **Изменить описание**.
Откроется окно **Описание**.
4. В окне **Описание** введите текст описания ревизии.
По умолчанию описание ревизии объекта не заполнено.
5. Сохраните описание ревизии.

Описание добавлено для ревизии объекта.

Просмотр и сохранение ревизии политики

Kaspersky Security Center позволяет просмотреть, какие изменения были внесены в политику за определенный период, и сохранить информацию об этих изменениях в файле.

Просмотр и сохранение ревизии политики доступны, если соответствующий веб-плагин управления поддерживает эту функцию.

► *Чтобы просмотреть ревизию политики:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на ревизию политики, которую вы хотите просмотреть и перейдите в раздел **История ревизий**.
3. В списке ревизий политики нажмите на номер ревизии, которую вы хотите просмотреть.

Если размер ревизии превышает 10 МБ, просмотреть ее с помощью Kaspersky Security Center Web Console невозможно. Вам будет предложено сохранить выбранную ревизию в файл JSON.

Если размер ревизии не превышает 10 МБ, отображается отчет в формате HTML с параметрами выбранной ревизии политики. Так как отчет отображается во всплывающем окне, убедитесь, что в вашем браузере разрешены всплывающие окна.

► *Чтобы сохранить ревизию политики в файл JSON,*

В списке ревизий политики выберите ревизию, которую вы хотите сохранить и нажмите кнопку **Сохранить в файл**.

Ревизия сохранена в файле JSON.

Удаление объектов

В этом разделе описано, как удалять объекты и просматривать информацию объектов после того, как они были удалены.

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователей;
- группы безопасности;
- группы администрирования.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения информации удаленных объектов такой же, как и срок хранения ревизий объектов (рекомендуемый срок 90 дней). Можно изменить время хранения только при наличии **права** на Изменение для области **Удаленные объекты**.

Об удалении клиентских устройств

При удалении управляемого устройства из группы администрирования приложение перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные приложения

"Лаборатории Касперского" – Агент администрирования и приложение безопасности, например Kaspersky Endpoint Security, – остаются на устройстве.

Kaspersky Security Center обрабатывает устройства из группы Нераспределенные устройства по следующим правилам:

- Если вы настроили правила перемещения устройств (см. раздел "Создание правил перемещения устройств" см. стр. [1197](#)) и устройство соответствует критериям правила перемещения, устройство автоматически перемещается в группу администрирования в соответствии с правилом.
- Устройство сохраняется в группе Нераспределенные устройства и автоматически удаляется из группы в соответствии с правилами хранения устройств (см. раздел "Настройка правил хранения для нераспределенных устройств" см. стр. [1121](#)).

Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования (см. раздел "Шифрование и защита данных." на стр. [1268](#)). Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

При удалении устройства с зашифрованным жестким диском данные, необходимые для расшифровки диска, также удаляются. Если вы установите флажок **Я понимаю риск и хочу удалить выбранные устройства** в окне подтверждения, которое открывается при удалении таких устройств (из группы **Нераспределенные устройства** или из группы **Управляемые устройства**), это означает, что вы знаете о последующем удалении данных.

В этом случае для расшифровки диска требуется выполнение следующих условий:

- Устройство повторно подключается к Серверу администрирования для восстановления данных, необходимых для расшифровки диска.
- Пользователь устройства помнит пароль для расшифровки.
- Приложение безопасности, которое использовалось для шифрования диска, например Kaspersky Endpoint Security для Windows, установлено на устройстве.

Если диск был зашифрован с помощью технологии Kaspersky Disk Encryption, вы также можете попробовать восстановить данные с помощью утилиты FDERT Restore

<https://support.kaspersky.com/KESWin/12.6/en-US/130941.htm>.

При удалении устройства из группы Нераспределенные устройства вручную приложение удаляет устройство из списка. После удаления устройства установленные приложения "Лаборатории Касперского" (если они есть) остаются на устройстве. Затем, если устройство по-прежнему видно Серверу администрирования и вы настроили регулярный опрос сети, Kaspersky Security Center Linux обнаружит устройство во время опроса сети и снова добавит его в группу Нераспределенные устройства. Поэтому удалять устройство вручную целесообразно только в том случае, если оно невидимо для Сервера администрирования.

Kaspersky Security Network и Kaspersky Private Security Network

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN) и Kaspersky Private Security Network (KPSN). Приведена информация о KSN и KPSN, а также инструкции по включению KPSN, настройке доступа к KPSN, по просмотру статистики использования прокси-сервера KSN.

В этом разделе

О KSN и KPSN	873
Настройка доступа к KSN	1328
Включение и выключение использования KSN	1330
Просмотр принятого Положения о KSN	1331
Принятие обновленного Положения о KSN	1332
Проверка, работает ли точка распространения как прокси-сервер KSN	878

О KSN и KPSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о приложениях, установленных на клиентских устройствах.

Участвуя в KSN, вы в соответствии с Положением о KSN соглашаетесь в автоматическом режиме передавать в "Лабораторию Касперского" информацию о работе приложений "Лаборатории Касперского", установленных на клиентских устройствах под управлением Kaspersky Security Center. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN.

Приложение предлагает присоединиться к KSN во время установки приложения и во время работы мастера первоначальной настройки. Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с приложением.

Использование Kaspersky Security Network приводит к выходу приложения из сертифицированного состояния. Необходимо использовать Kaspersky Private Security Network или отказаться от использования KSN.

Вы можете использовать Kaspersky Private Security Network (далее также KPSN) вместо Kaspersky Security Network, чтобы не использовать отправку данных вашей организации за пределы локальной сети организации.

Kaspersky Private Security Network (KPSN) – это решение, позволяющее получать доступ к данным Kaspersky Security Network через сервер, размещенный внутри сети вашей организации. KPSN позволяет приложениям "Лаборатории Касперского" получать доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсах и программном обеспечении. KPSN не передает статистику

и файлы в "Лабораторию Касперского". Для получения подробной информации см. *"Kaspersky Private Security Network. Подготовительные процедуры и руководство по эксплуатации"*.

Служба Kaspersky Private Security Network разработана для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

- отсутствия подключения серверов к интернету;
- законодательного запрета на отправку любых данных за пределы страны;
- требований корпоративной безопасности на отправку любых данных за пределы локальной сети организации.

Клиентские устройства, находящиеся под управлением Сервера администрирования, для взаимодействия с KSN или KPSN могут использовать службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет и серверам KPSN.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования.

Настройка доступа к KSN

Можно задать доступ к Kaspersky Security Network (KSN) с Сервера администрирования и с точки распространения.

► *Чтобы настроить доступ Сервера администрирования к KSN:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

Если этот параметр включен, прокси-сервер KSN отправляет данные в KSN для повышения эффективности работы компонентов Kaspersky Security Center и приложений "Лаборатории Касперского". Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если переключатель выключен, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

4. Переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.

Если параметр включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". При включении этого параметра убедитесь, что вы прочитали и принимаете условия Положения о KSN.

Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network Включено** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями rkcs7 и rem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

При включении KPSN обратите внимание на точки распространения настроенные на отправку KSN запросов напрямую облачной-службе KSN. Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к облачной-службе KSN. Чтобы перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения. Вы можете включить этот параметр в свойствах точки распространения или политики Агента администрирования.

При переводе переключателя в положение **Использовать Kaspersky Private Security Network Включено** появится сообщение с подробной информацией о KPSN.

KPSN поддерживают следующие приложения "Лаборатории Касперского":

- Kaspersky Security Center
- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2
- Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент

Если вы включите KPSN в Kaspersky Security Center, эти приложения получают об этом информацию о поддержке KPSN. В окне свойств приложения в подразделе **Kaspersky Security Network** раздела **Продвинутая защита** отображается поставщик KSN: KSN или KPSN.

Если для работы с KPSN вы используете версии приложений ниже Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2 или ниже Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, рекомендуется использовать подчиненные Серверы администрирования, для которых не настроено использование KPSN. Kaspersky Security Center не отправляет статистику Kaspersky Security Network, если настроен KPSN в окне свойств Сервера администрирования в разделе **Параметры прокси-сервера KSN**.

5. Установите флажок **Игнорировать параметры прокси-сервера для подключения к KPSN**, если параметры прокси-сервера настроены в свойствах Сервера администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.
6. Настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:
 - В блоке **Параметры подключения**, в поле ввода **TCP-порт**, укажите номер TCP-порта, через который будет выполняться подключение к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через порт 13111.
 - Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, выберите параметр **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр выключен, используется порт TCP. Если параметр включен, по умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

7. Переведите переключатель в положение **Подключать подчиненные Серверы администрирования к KSN через главный Сервер Включено**.

Если этот параметр включен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KSN. Если этот параметр выключен, подчиненные Серверы администрирования подключаются к KSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Параметры прокси-сервера KSN** также переключатель переведен в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

8. Нажмите на кнопку **Сохранить**.

В результате параметры доступа к KSN будут сохранены.

Можно также настроить доступ к KSN со стороны точки распространения, например, если необходимо снизить нагрузку на Сервер администрирования. Точка распространения, выполняющая роль прокси-сервера KSN, отправляет KSN запросы от управляемых устройств напрямую в "Лабораторию Касперского", минуя Сервер администрирования.

► *Чтобы настроить доступ точки распространения к Kaspersky Security Network (KSN):*

1. Убедитесь, что точка распространения была назначена вручную (см. раздел "Назначение точек распространения вручную" см. стр. [1370](#)).

2. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

3. На вкладке **Общие** выберите раздел **Точки распространения**.
4. Нажмите на имя точки распространения, чтобы открыть окно ее свойств.
5. В окне свойств точки распространения в разделе **Прокси-сервер KSN**, включите параметр **Включить прокси-сервер KSN на стороне точки распространения** и параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.
6. Нажмите на кнопку **ОК**.

Точка распространения будет исполнять роль прокси-сервера KSN.

Включение и выключение использования KSN

► *Чтобы включить использование KSN:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.

3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

Прокси-сервер KSN включен и отправляет данные в KSN для повышения эффективности работы компонентов Kaspersky Security Center и приложений "Лаборатории Касперского".

4. В зависимости от используемого решения инфраструктуры KSN (см. раздел "О KSN и KPSN" на стр. [873](#)), включите соответствующие переключатели.
 - Если вы используете Глобальный KSN, переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.
Теперь доступна отправка данных в KSN. При включении этого параметра, вам нужно прочитать и принять условия Положения о KSN.
 - Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network Включено** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями rkcs7 и rem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.
При переводе переключателя в положение **Использовать Kaspersky Private Security Network Включено** появится сообщение с подробной информацией о KPSN.
5. Нажмите на кнопку **Сохранить**.

► *Чтобы выключить использование KSN:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Переключите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Выключено**, чтобы выключить службу прокси-сервера KSN.
4. Нажмите на кнопку **Сохранить**.

Просмотр принятого Положения о KSN

При включении Kaspersky Security Network (KSN) вам нужно прочитать и принять Положение о KSN. Вы можете просмотреть принятое Положение о KSN в любое время.

► *Чтобы просмотреть принятое Положение о KSN:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Перейдите по ссылке **Просмотреть Положение о Kaspersky Security Network**.
В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN (см. раздел "Просмотр принятого Положения о KSN" см. стр. [1331](#)), которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с версией Положения о KSN, которую вы приняли ранее.

После обновления Сервера администрирования с предыдущей версии, обновленное Положение о KSN отображается автоматически. Если вы отклоните обновленное Положение о KSN, вы все равно сможете просмотреть и принять его позже.

► Чтобы просмотреть и принять или отклонить обновленное Положение о KSN:

1. Нажмите на значок **Просмотреть уведомления о событиях** в правом верхнем углу главного окна приложения.

Откроется окно **Уведомления**.

2. Перейдите по ссылке **Просмотреть обновленное Положение о KSN**.

Откроется окно **Обновление Положения о Kaspersky Security Network**.

3. Прочтите Положение о KSN, а затем примите решение, нажав одну из следующих кнопок:

- **Я принимаю условия обновленного Положения о KSN**
- **Использовать KSN со старым Положением о KSN**

В зависимости от вашего выбора KSN продолжит работу в соответствии с условиями текущего или обновленного Положения о KSN. Вы можете в любой момент просмотреть текст принятого Положения о KSN (см. раздел "Просмотр принятого Положения о KSN" см. стр. [1331](#)) в свойствах Сервера администрирования.

Проверка, работает ли точка распространения как прокси-сервер KSN

На управляемом устройстве, которое выполняет роль точки распространения, вы можете включить прокси-сервер KSN. Управляемое устройство работает как прокси-сервер KSN, если на нем запущена служба ksnproxу. Вы можете проверить включить или выключить эту службу на устройстве локально.

Вы можете назначить устройство с операционной системой Windows или Linux в качестве точки распространения. Способ проверки точки распространения зависит от операционной системы этой точки распространения.

► Чтобы проверить, работает ли точка распространения с операционной системой Windows как прокси-сервер KSN:

1. На устройстве, которое выполняет роль точки распространения, в Windows откройте окно **Службы (Все приложения → Администрирование → Службы)**.
2. В списке служб проверьте, запущена ли служба прокси-сервера KSN – ksnproxу.

Если служба ksnproxу запущена, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN Proху для управляемых устройств, входящих в область действия точки распространения.

При необходимости службу ksnproxy можно выключить. В этом случае Агент администрирования на точке распространения больше не участвует в Kaspersky Security Network. Для этого требуются права локального администратора.

► *Чтобы проверить, работает ли точка распространения с операционной системой Linux как прокси-сервер KSN:*

1. На устройстве, выполняющем роль точки распространения, отобразится список запущенных процессов.
2. В списке запущенных процессов проверьте запущен ли процесс `/opt/kaspersky/ksc64/sbin/ksnproxy`.

Если процесс `/opt/kaspersky/ksc64/sbin/ksnproxy` запущен, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN для управляемых устройств, входящих в область действия точки распространения.

Сценарий: обновление Kaspersky Security Center и управляемых приложений безопасности

В этом разделе описан основной сценарий обновления приложения Kaspersky Security Center и управляемых приложений безопасности.

Обновление Kaspersky Security Center и управляемых приложений безопасности состоит из следующих этапов:

a. Проверка требований к оборудованию и программному обеспечению

Убедитесь, что ваше оборудование соответствует требованиям, и установите необходимые обновления.

b. Планирование ресурсов

Оцените, сколько дискового пространства занимает ваша база данных. Убедитесь, что на жестком диске имеется достаточно свободного места для хранения резервной копии данных Сервера администрирования.

c. Получение файла установки Kaspersky Security Center

Получите исполняемый файл для текущей версии Kaspersky Security Center и сохраните его на устройство, выполняющее роль Сервера администрирования. Ознакомьтесь с информацией о выпуске для версии Kaspersky Security Center, которую вы используете.

d. Создание резервной копии предыдущей версии

С помощью утилиты резервного копирования и восстановления данных создайте резервную копию данных Сервера администрирования. Вы также можете создать задачу резервного копирования.

Рекомендуется экспортировать список установленных плагинов.

e. Запуск установщика

Запустите исполняемый файл для последней версии Kaspersky Security Center. После запуска файла укажите, что была создана резервная копия, а также путь к ней. Будет выполнено восстановление данных из резервной копии.

f. Обновление управляемых приложений

Можно обновить приложение, если доступна новая версия. Ознакомьтесь со списком поддерживаемых приложений "Лаборатории Касперского" и убедитесь, что ваша версия Kaspersky Security Center совместима с этим приложением. Затем обновите приложение, как описано в информации о выпуске.

Результаты

После завершения сценария обновления убедитесь, что новая версия Сервера администрирования успешно установлена в Консоли управления (MMC). В меню выберите **Справка** → **О Kaspersky Security Center**. Отобразится номер версии приложения.

Убедитесь, что вы используете последнюю версию Сервера администрирования в Kaspersky Security Center

Web Console, в верхней части экрана нажмите значок параметров () рядом с именем Сервера администрирования. В открывшемся окне свойств Сервер администрирования на вкладке **Общие** выберите раздел **Общие**. Отобразится номер версии приложения.

Если вам нужно восстановить данные Сервера администрирования, выполните действия, описанные в следующем разделе: Резервное копирование и восстановление данных в интерактивном режиме.

Если вы обновили управляемое приложение безопасности, убедитесь, что она установлена правильно на управляемых устройствах. Дополнительную информацию см. в документации к этому приложению.

Обновление баз и приложений "Лаборатории Касперского"

В этом разделе описаны шаги, которые вам нужно выполнить для регулярных обновлений:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложений безопасности.

В этом разделе

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455
Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"	460
Создание задачи Загрузка обновлений в хранилище Сервера администрирования	1347
Проверка полученных обновлений	1353
Создание задачи загрузки обновлений в хранилища точек распространения	1355
Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center	1360
Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows	1361
Одобрение и отклонение обновлений программного обеспечения	1363
Обновление Сервера администрирования	1364
Включение и выключение офлайн-модели получения обновлений	1364
Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах	1365
Резервное копирование и восстановление веб-плагинов	1366
Настройка точек распространения и шлюзов соединений	685

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, модулей приложений и приложений "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации (см. раздел "Сценарий: настройка защиты сети" см. стр. [403](#)), вам нужно поддерживать надежность системы защиты, чтобы обеспечить защиту Серверов администрирования и управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Защита сети поддерживается обновленной с помощью регулярных обновлений следующего:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложений безопасности.

Когда вы завершите этот сценарий, вы можете быть уверены, что:

- Ваша сеть защищена самым последним программным обеспечением "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложения безопасности.
- Антивирусные базы и другие базы данных "Лаборатории Касперского", критически важные для безопасности сети, всегда актуальны.

Предварительные требования

Управляемые устройства должны иметь соединение с Сервером администрирования. Если у устройств нет соединения, рассмотрите возможность обновления баз, программных модулей и программ «Лаборатории Касперского» вручную (см. раздел "Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах" см. стр. [1365](#)) или напрямую с серверов обновлений «Лаборатории Касперского».

Сервер администрирования должен иметь подключение к интернету.

Прежде чем приступить, убедитесь, что вы выполнили следующее:

1. Развернуты приложения безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console (см. раздел "Сценарий: развертывание приложений "Лаборатории Касперского"" см. стр. [1084](#)).
2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети (см. раздел "Сценарий: настройка защиты сети" см. стр. [403](#)).
3. Назначено соответствующее количество точек распространения в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и приложений «Лаборатории Касперского» состоит из следующих этапов:

а. Выбор схемы обновления

Существует несколько схем (см. раздел "Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"" см. стр. [460](#)), которые вы можете использовать для установки обновлений компонентов Kaspersky Security Center и приложений безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

б. Создание задачи для загрузки обновлений в хранилище Сервера администрирования

Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, создайте задачу сейчас.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования, а также обновления баз и модулей приложений для Kaspersky Security Center. После загрузки обновлений их можно распространять на управляемые устройства.

Если в вашей сети назначены точки распространения, обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. В этом случае управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.

Инструкции:

- Консоль администрирования: Создание задачи для загрузки обновлений в хранилище Сервера администрирования.

- Kaspersky Security Center Web Console: Создание задачи для загрузки обновлений в хранилище Сервера администрирования (см. раздел "Создание задачи Загрузка обновлений в хранилище Сервера администрирования" см. стр. [1347](#))

c. Создание задачи загрузки обновлений в хранилища точек распространения (если требуется)

По умолчанию обновления загружаются в хранилища точек распространения из хранилища Сервера администрирования. Вы можете настроить Kaspersky Security Center так, чтобы точки распространения загружали обновления непосредственно с серверов обновлений "Лаборатории Касперского". Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Когда вашей сети назначены точки распространения и создана задача *Загрузка обновлений в хранилища точек распространения*, точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Инструкции:

- Консоль администрирования: Создание задачи загрузки обновлений в хранилища точек распространения.
- Kaspersky Security Center Web Console: Создание задачи загрузки обновлений в хранилища точек распространения (см. стр. [1355](#)).

d. Настройка точек распространения

Если в вашей сети назначены точки распространения, убедитесь, что параметр **Распространять обновления** включен в свойствах всех требуемых точек распространения. Если этот параметр выключен для точки распространения, устройства, включенные в область действия точки распространения, загружают обновления из хранилища Сервера администрирования.

Если вы хотите, чтобы управляемые устройства получали обновления только от точек распространения, включите параметр **Распространять файлы только через точки распространения** в политике Агента администрирования.

e. Оптимизация процесса обновления с использованием офлайн-модели получения обновлений или загрузки файлов различий (если требуется)

Вы можете оптимизировать процесс обновления, используя офлайн-модель загрузки обновлений (включена по умолчанию), или используя файлы различий. Для каждого сегмента сети вам нужно выбрать, какую из этих двух функций включить, так как они не могут работать одновременно.

Когда офлайн-модель получения обновлений включена, Агент администрирования загружает необходимые обновления на управляемое устройство после загрузки обновлений в хранилище Сервера администрирования, прежде чем приложение безопасности запросит обновления. Это повышает надежность процесса обновления. Чтобы использовать эту функцию, включите параметр **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)** в свойствах задачи Политика Агента администрирования.

Если вы не используете офлайн-модель загрузки обновлений, вы можете оптимизировать трафик между Сервером администрирования и управляемыми устройствами, используя файлы различий. Когда эта функция включена, Сервер администрирования или точка распространения загружает файлы различий вместо целых файлов баз данных или модулей приложений "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Загрузить файлы различий в**

свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

Инструкции:

- Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского".
- Консоль администрирования: Включение и выключение офлайн-модели получения обновлений.
- Kaspersky Security Center Web Console: Консоль администрирования: Включение и выключение офлайн-модели получения обновлений (см. раздел "Включение и выключение офлайн-модели получения обновлений" см. стр. [1364](#)).

f. Проверка полученных обновлений (если требуется)

Перед установкой загруженных обновлений вы можете проверить обновления с помощью задачи *Проверка обновлений*. Эта задача последовательно запускает задачи обновления устройства и задачи поиска вредоносного ПО, настроенные с помощью параметров для указанного набора тестовых устройств. После получения результатов задачи Сервер администрирования запустит или заблокирует распространение обновлений на оставшиеся устройства.

Задача *Проверка обновлений* может быть выполнена как часть задачи *Загрузка обновлений в хранилище Сервера администрирования*. В свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* включите параметр **Выполнять проверку обновлений перед распространением** в Консоли администрирования или параметр **Выполнить проверку обновлений** в Kaspersky Security Center Web Console.

Инструкции:

- Консоль администрирования: Проверка полученных обновлений.
- Kaspersky Security Center Web Console: Проверка полученных обновлений (см. стр. [1353](#)).

g. Одобрение и отклонение обновлений программного обеспечения

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус обновления на *Одобрено* или *Отклонено*. Одобренные обновления всегда устанавливаются. Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Неопределенные обновления могут быть установлены только на Агента администрирования и других компонентах Kaspersky Security Center в соответствии с параметрами политики Агента администрирования. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для приложения безопасности было установлено, Kaspersky Security Center попытается удалить обновления со всех устройств. Обновления для компонентов Kaspersky Security Center не могут быть удалены.

Инструкции:

- Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения.
- Kaspersky Security Center Web Console: Одобрение и отклонение обновлений программного обеспечения (см. стр. [1363](#)).

h. Настройка автоматической установки обновлений и патчей для компонентов Kaspersky Security Center

Загруженные обновления и патчи для Агента администрирования и других компонентов Kaspersky Security Center устанавливаются автоматически. Если вы оставили включенным параметр **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** в свойствах Агента администрирования, тогда все обновления будут

установлены автоматически после их загрузки в хранилище (или несколько хранилищ). Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрено*.

Инструкции:

- Консоль администрирования: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center.
- Kaspersky Security Center Web Console: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center (см. стр. [1360](#)).

i. Установка обновлений для Сервера администрирования

Обновления программного обеспечения для Сервера администрирования не зависят от статусов обновлений. Они не устанавливаются автоматически и должны быть предварительно одобрены администратором на вкладке **Мониторинг** в Консоли администрирования (**Сервер администрирования** <имя Сервера> → **Мониторинг**) или в разделе **Уведомления** в Kaspersky Security Center Web Console (**Мониторинг и отчеты** → **Уведомления**). После этого администратор должен явно запустить установку обновлений.

j. Настройка автоматической установки обновлений для приложений безопасности

Создайте задачу *Обновление* для управляемых приложений, чтобы обеспечить своевременное обновление приложений, модулей приложений и баз данных "Лаборатории Касперского", в том числе антивирусных баз. Рекомендуется выбрать параметр **При загрузке обновлений в хранилище** при настройке расписания задач (см. раздел "Общие параметры задач" см. стр. [1176](#)) для своевременного обновления.

Если в вашей сети есть устройства, поддерживающие только IPv6, и вы хотите регулярно обновлять приложения безопасности, установленные на этих устройствах, убедитесь, что на управляемых устройствах установлены Сервер администрирования (версии 13.2 или выше) и Агент администрирования (версии 13.2 или выше).

По умолчанию обновления для Kaspersky Endpoint Security для Windows и для Kaspersky Endpoint Security для Linux устанавливаются только после изменения статуса обновления на *Одобрено*. Вы можете изменить параметры обновления в задаче *Обновление*.

Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства.

Инструкции:

- Консоль администрирования: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства.
- Kaspersky Security Center Web Console: Консоль администрирования: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства (см. раздел "Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows" см. стр. [1361](#)).

Результаты

По завершении сценария Kaspersky Security Center настроен для обновления баз "Лаборатории Касперского" и установленных приложений "Лаборатории Касперского" после загрузки обновлений в хранилище Сервера администрирования или в хранилища точек распространения. Теперь вы можете приступить к мониторингу состояния сети.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вам нужно своевременно предоставлять обновления следующего:

- Баз и модулей приложений "Лаборатории Касперского".

Kaspersky Security Center проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и модулей приложений "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы. Это необходимо для обновления антивирусных баз и поддержания уровня безопасности управляемых устройств.

- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложений безопасности.

В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- С помощью одной задачи: *Загрузка обновлений в хранилище Сервера администрирования*
- С помощью двух задач:
 - Задача *Загрузка обновлений в хранилище Сервера администрирования*.
 - Задача *Загрузка обновлений в хранилища точек распространения*.
- Вручную через локальную папку, общую папку или FTP-сервер
- Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах
- Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

Использование задачи *Загрузка обновлений в хранилище Сервера администрирования*

В этой схеме Kaspersky Security Center загружает обновления с помощью задачи *Загрузка обновлений в хранилище Сервера администрирования*. В небольших сетях, которые содержат менее 300 управляемых устройств в одном сегменте сети или менее десяти управляемых устройств в каждом сегменте, обновления

распространяются на управляемые устройства непосредственно из хранилища Сервера администрирования (см. рисунок ниже).

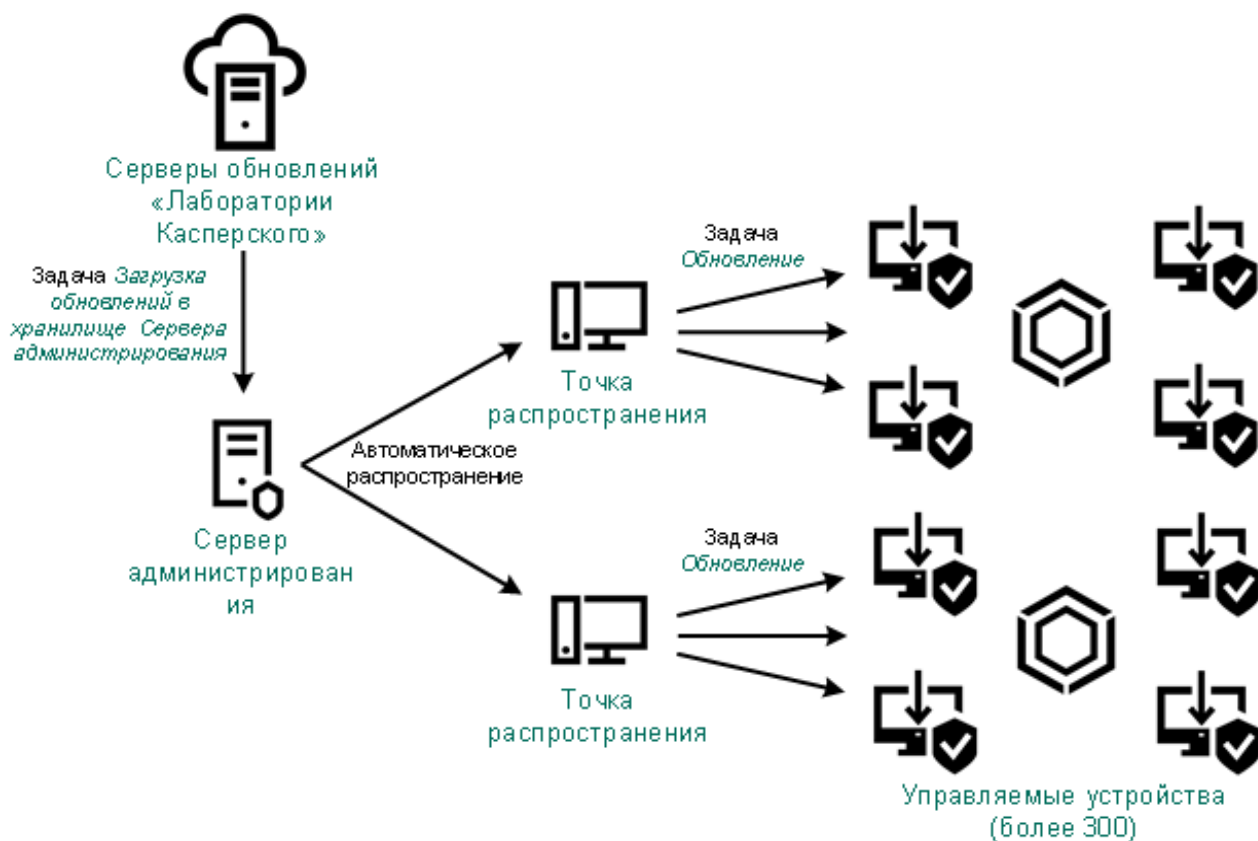


По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

Если ваша сеть содержит более 300 управляемых устройств в одном сегменте сети или ваша сеть содержит несколько сегментов, в которых больше девяти управляемых устройств, мы рекомендуем использовать точки распространения для распространения обновлений на управляемые устройства (см. рисунок ниже). Точки распространения уменьшают загрузку Сервера администрирования и оптимизируют трафик между Сервером администрирования и управляемыми устройствами. Вы можете рассчитать количество точек распространения и их конфигурацию, необходимые для вашей сети.

В этой схеме обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. Управляемые устройства, входящие в область действия точки

распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.



После завершения задачи *Загрузка обновлений в хранилище Сервера администрирования* следующие обновления загружаются в хранилище Сервера администрирования:

- Базы и модули приложений "Лаборатории Касперского" для Kaspersky Security Center.
Эти обновления устанавливаются автоматически.
- Базы и модули приложений "Лаборатории Касперского" для приложений безопасности на управляемых устройствах.
Эти обновления устанавливаются с помощью задачи Обновление Kaspersky Endpoint Security для Windows (см. раздел "Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows" см. стр. [1361](#)).
- Обновления для Сервера администрирования.
Эти обновления не устанавливаются автоматически. Администратор должен явно одобрить обновления и запустить установку обновлений.

Для установки патчей на Сервере администрирования требуются права локального администратора.

- Обновления для компонентов Kaspersky Security Center.

По умолчанию эти обновления устанавливаются автоматически. Вы можете изменить параметры политики Агента администрирования (см. раздел "Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center" см. стр. [1360](#)).

- Обновления для приложений безопасности.

По умолчанию приложение Kaspersky Endpoint Security для Windows устанавливает только те обновления, которые вы одобрили. (Вы можете одобрить обновления с помощью Консоли администрирования или Kaspersky Security Center Web Console (см. раздел "Одобрение и отклонение обновлений программного обеспечения" см. стр. [1363](#))). Обновления устанавливаются с помощью задачи *Обновление* и могут быть настроены в свойствах этой задачи.

*Задача **Загрузка обновлений в хранилище Сервера администрирования** недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.*

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

Каждое управляемое приложение "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются приложениями. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и модулей приложений "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

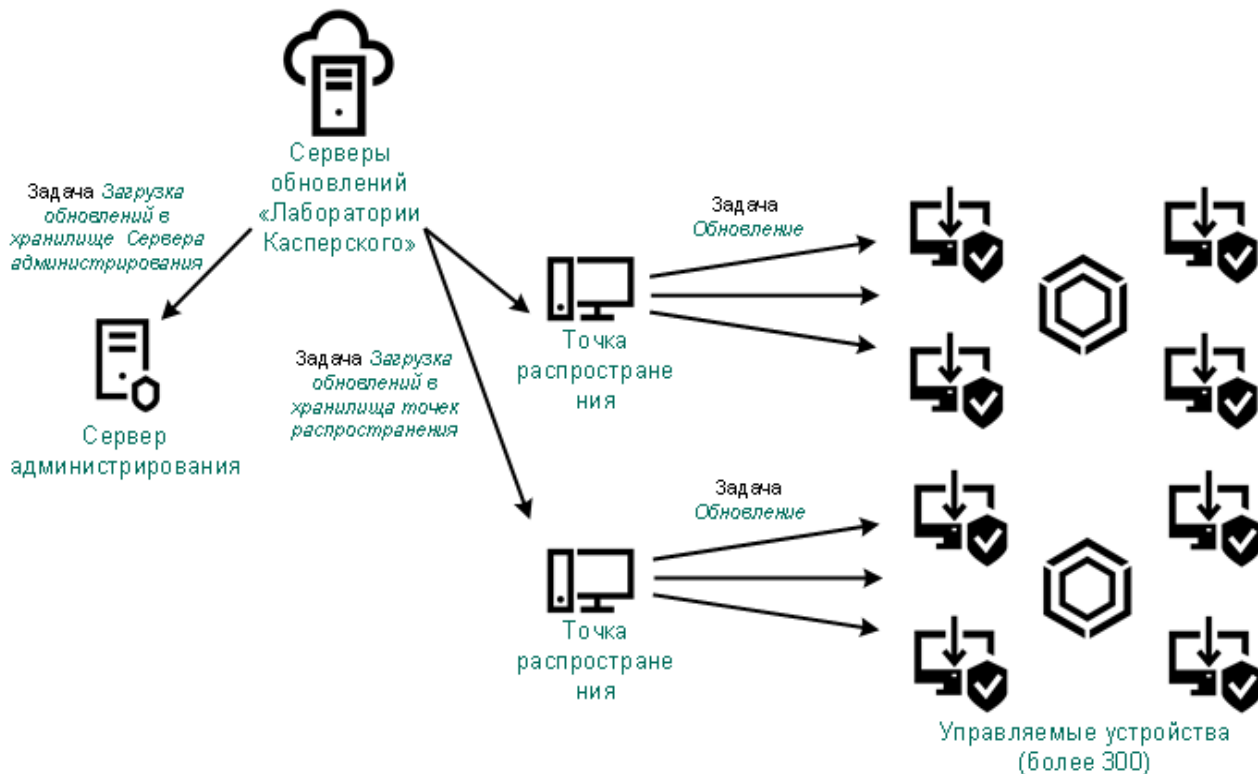
- идентификатор и версия приложения;
- идентификатор установки приложений;
- идентификатор активного ключа;
- идентификатор запуска задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

Использование двух задач: Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами

обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.



По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и/или точки распространения на использование протокола HTTP вместо HTTPS.

Для реализации этой схемы создайте задачу *Загрузка обновлений в хранилища точек распространения* в дополнение к задаче *Загрузка обновлений в хранилище Сервера администрирования*. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Для этой схемы также требуется задача *Загрузка обновлений в хранилище Сервера администрирования*, так как эта задача используется для загрузки баз и модулей приложений "Лаборатории Касперского" для Kaspersky Security Center.

Вручную через локальную папку, общую папку или FTP-сервер

Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать локальную папку или общий ресурс в качестве источника обновления баз, модулей приложений и приложений "Лаборатории Касперского" (см. раздел "Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах" см. стр. [1365](#)). В этой схеме вам нужно скопировать необходимые обновления из хранилища Сервера администрирования на съемный диск, а затем скопировать обновления в локальную папку или общий ресурс, указанный в качестве источника обновлений в параметрах Kaspersky Endpoint Security (см. рисунок ниже).

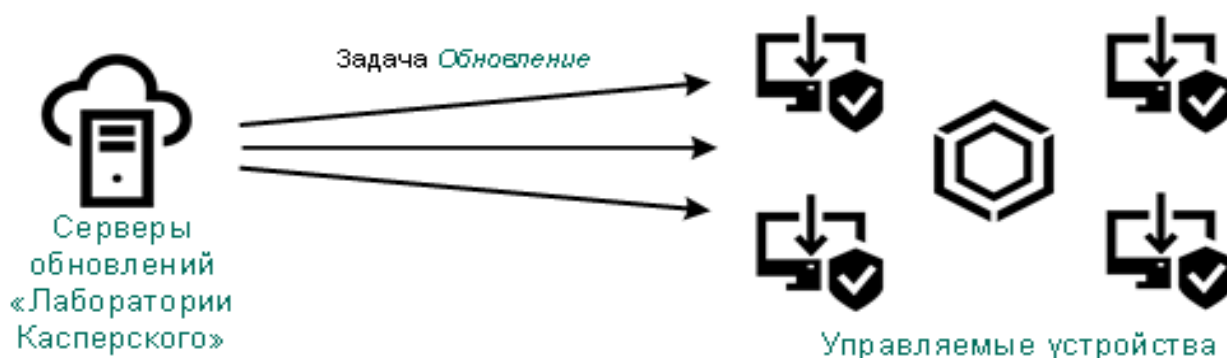


Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих справках:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



В этой схеме приложения безопасности не используют хранилища, предоставленные Kaspersky Security Center. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в интерфейсе приложения безопасности. Дополнительные сведения об этих параметрах см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

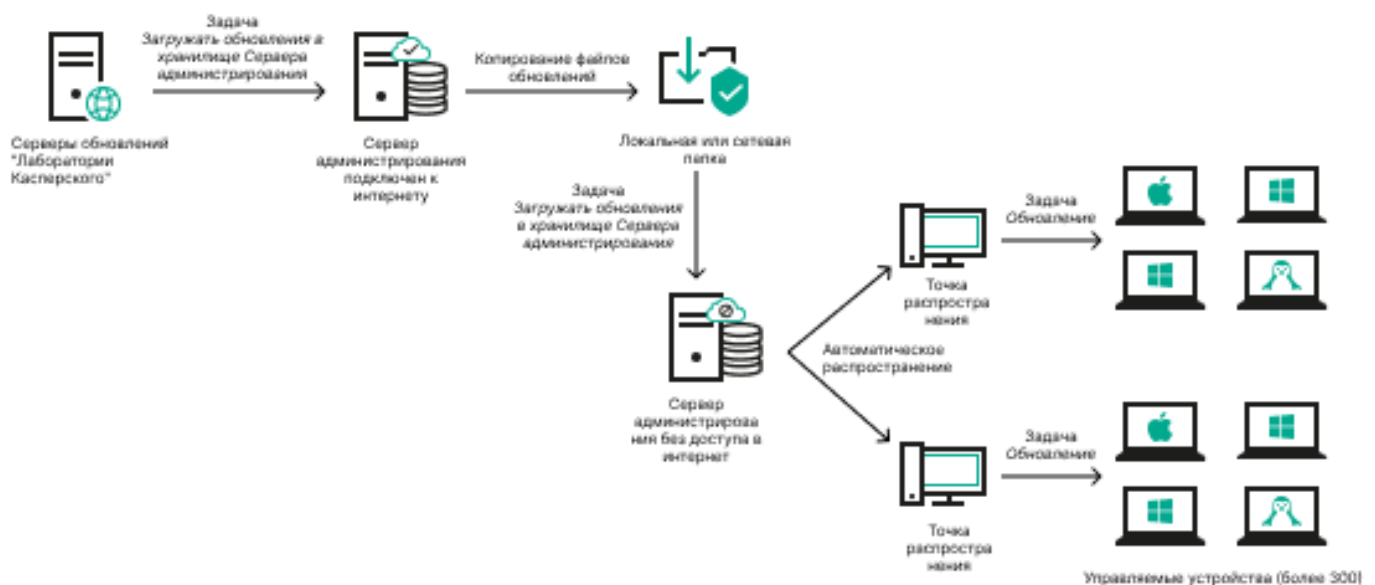
Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузка обновлений в хранилище Сервера администрирования* для загрузки обновлений из локальной или сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. Например, вы можете скопировать необходимые файлы обновления из одного из следующих источников:

- Сервер администрирования, имеющий выход в интернет (см. рис. ниже).

Так как Сервер администрирования загружает только те обновления, которые запрашиваются приложениями безопасности, наборы приложений безопасности, которыми управляют Серверы администрирования (подключенные и не подключенные к интернету) должны совпадать.

Если Сервер администрирования, который вы используете для загрузки обновлений, имеет версию 13.2 или более раннюю, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования* (см. раздел "Создание задачи *Загрузка обновлений в хранилище Сервера администрирования*" см. стр. [1347](#)), а затем включите параметр **Загружать обновления, используя старую схему**.



- Kaspersky Update Utility <https://support.kaspersky.com/updater4>

Так как утилита использует старую схему для загрузки обновлений, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования* (см. раздел "Создание задачи *Загрузка обновлений в хранилище Сервера администрирования*" см. стр. [1347](#)), а затем включите параметр **Загружать обновления, используя старую схему**.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Создание задачи Загрузка обновлений в хранилище Сервера администрирования

Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Задача *Загрузка обновлений в хранилище Сервера администрирования* может быть создана в одном экземпляре. Поэтому вы можете создать задачу *Загрузка обновлений в хранилище Сервера администрирования* только в случае, если она была удалена из списка задач Сервера администрирования.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования. Список обновлений включает:

- обновления баз и модулей приложений для Сервера администрирования;
- обновления баз и модулей приложений для приложений безопасности "Лаборатории Касперского";
- обновления компонентов Kaspersky Security Center;
- обновления приложений безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

Перед распространением обновлений на управляемые устройства вы можете выполнить задачу *Проверка обновлений* (см. раздел "*Проверка полученных обновлений*" см. стр. [1353](#)). Это позволяет убедиться, что Сервер администрирования правильно установит загруженные обновления и уровень безопасности не снизится из-за обновлений. Чтобы проверить обновления перед распространением, настройте параметр **Выполнить проверку обновлений** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

► Чтобы создать задачу *Загрузка обновлений в хранилище Сервера администрирования*:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите тип задачи **Загрузка обновлений в хранилище Сервера администрирования**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\\:|").
5. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

6. Нажмите на кнопку **Создать**.

Задача будет создана и отобразится в списке задач.

7. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
8. В окне свойств задачи на вкладке **Параметры приложения** укажите следующие параметры:
 - **Источники обновлений**

В качестве источника обновлений для Сервера администрирования могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского"
HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения. По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.
Выбрано по умолчанию.
- Главный Сервер администрирования
Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
- Локальная или сетевая папка
Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует проверки подлинности, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

Если общая папка с обновлениями защищена паролем, включите параметр **Задать учетную запись для доступа к общей папке источника обновлений (если используется)** и введите учетные данные, необходимые для доступа.

- **Папка для хранения обновлений**
- Прочие параметры:
 - **Принудительно обновить подчиненные Серверы**
Если параметр включен, после получения обновлений Сервер администрирования будет запускать задачи получения обновлений подчиненными Серверами администрирования. В противном случае задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.
По умолчанию параметр выключен.
 - **Копировать полученные обновления в дополнительные папки**

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

По умолчанию параметр выключен.

- **Не обновлять устройства и подчиненные Серверы администрирования принудительно до окончания копирования**

Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

По умолчанию параметр выключен.

- **Состав обновлений:**

- **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий.

По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**
- **Выполнить проверку обновлений**

Если флажок установлен, Сервер администрирования копирует обновления из источника, сохраняет их во временном хранилище и запускает задачу Проверка обновлений (см. раздел "Проверка полученных обновлений" см. стр. [1353](#)), указанную в поле **Задача проверки обновлений**. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования и распространяются на устройства, для которых Сервер администрирования является источником обновлений (запускаются задачи с типом расписания **При загрузке обновлений в хранилище**). Задача загрузки обновлений в хранилище считается завершенной только после завершения задачи *Проверка обновлений*.

По умолчанию параметр выключен.

1. В окне свойств задачи на вкладке **Расписание** создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск задачи:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Вручную**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Каждые N минут**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрываемым списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Каждый N час**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрываемым списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрываемым списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим

Ежемесячно, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрывающимся списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрывающимся списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрывающемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.
- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задач**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Остановить, если задача выполняется дольше**

По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

2. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и модули приложений копируются с источника обновлений и размещаются в папке общего доступа Сервера администрирования. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Из папки общего доступа обновления распространяются на клиентские устройства и подчиненные Серверы администрирования.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Проверка полученных обновлений

Перед установкой обновлений на управляемые устройства вы можете сначала проверить их на работоспособность и ошибки с помощью задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется автоматически в рамках задачи *Загрузка обновлений в хранилище Сервера администрирования*. Сервер администрирования загружает обновления с источника, сохраняет их во временном хранилище и запускает задачу *Проверка обновлений*. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования. Обновления распространяются на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи *Проверка обновлений* размещенные во временном хранилище обновления признаны некорректными или задача завершается с ошибкой, копирование обновлений в папку общего доступа не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции выполняются при следующем запуске задачи *Загрузка обновлений в хранилище Сервера администрирования*, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты приложения безопасности;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования приложения "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача *Проверка обновлений* считается успешно выполненной.

Прежде чем приступить к созданию задачи *Проверка обновлений*, выполните предварительные условия:

1. Создайте группу администрирования (см. раздел "Создание групп администрирования" на стр. [1194](#)) с несколькими тестовыми устройствами. Эта группа понадобится вам для проверки обновлений.

В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Такой подход повышает качество и вероятность обнаружения вирусов при проверке, а также минимизирует риск ложных срабатываний. При нахождении вирусов на тестовых устройствах задача *Проверка обновлений* считается завершившейся неудачно.

2. Создайте задачи обновления и поиска вредоносного ПО (см. раздел "Создание задачи" на стр. [1174](#)) для какого-нибудь приложения, которое поддерживает Kaspersky Security Center, например, Kaspersky Endpoint Security для Windows или Kaspersky Security для Windows Server. При создании задач обновления и поиска вредоносного ПО укажите группу администрирования с тестовыми устройствами.

Задача *Проверка обновлений* последовательно запускает задачи обновления и поиска вредоносного ПО на тестовых устройствах, чтобы убедиться, что все обновления актуальны. Также при создании задачи *Проверка обновлений* необходимо указать задачи обновления и поиска вредоносного ПО.

3. Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования* (см. раздел "Создание задачи *Загрузка обновлений в хранилище Сервера администрирования*" см. стр. [1347](#)).

► Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на имя задачи **Загрузка обновлений в хранилище Сервера администрирования**.
3. В открывшемся окне свойств задачи перейдите на вкладку **Параметры приложения** и включите параметр **Выполнить проверку обновлений**.
4. Если задача *Проверка обновлений* существует, нажмите на кнопку **Выберите задачу**. В открывшемся окне выберите задачу *Проверка обновлений* в группе администрирования с тестовыми устройствами.
5. Если вы не создавали задачу *Проверка обновлений* ранее, выполните следующие действия:
 - a. Нажмите на кнопку **Новая задача**.
 - b. В открывшемся мастере создания задачи укажите имя задачи, если вы хотите изменить предустановленное имя.
 - c. Выберите созданную ранее группу администрирования с тестовыми устройствами.
 - d. Выберите задачу обновления нужного приложения, поддерживаемого Kaspersky Security Center, а затем выберите задачу поиска вредоносного ПО.

После этого появляются следующие параметры. Рекомендуется оставить их включенными:

- **Перезагружать устройство после обновления баз**
- **Проверять статус постоянной защиты после обновления баз и перезапуска устройства**

- e. Укажите учетную запись, под которой будет запущена задача *Проверка обновлений*. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.

6. Закройте окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*, нажав на кнопку **Сохранить**.

Автоматическая проверка обновлений включена. Теперь вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования*, и она начнется с проверки обновлений.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....[455](#)

Создание задачи загрузки обновлений в хранилища точек распространения

Задача *Загрузка обновлений в хранилища точек распространения* работает только с точками распространения под управлением Windows. Точки распространения под управлением Linux или macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского". Если хотя бы одно устройство с операционной системой Linux или macOS находится в области действия задачи, задача будет иметь статус *Сбой*. Даже если задача успешно завершена на всех устройствах с операционной системой Windows, она вернет ошибку на остальных устройствах.

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилища точек распространения. Список обновлений включает:

- обновления баз и модулей приложений для приложений безопасности "Лаборатории Касперского";
- обновления компонентов Kaspersky Security Center;
- обновления приложений безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

► Чтобы создать задачу *Загрузка обновлений в хранилища точек распространения* для выбранной группы администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите в поле **Task type** выберите **Загрузка обновлений в хранилища точек распространения**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\\:|").
5. Нажмите на кнопку выбора, чтобы указать группу администрирования, выборку устройств или устройства, к которым применяется задача.

6. На шаге **Завершение создания задачи**, если вы хотите изменить параметры задачи по умолчанию, включите параметр **Открыть окно свойств задачи после ее создания**. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
7. Нажмите на кнопку **Создать**.
Задача будет создана и отобразится в списке задач.
8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
9. На вкладке **Параметры приложения** окна свойств задачи укажите следующие параметры:

- **Источники обновлений**

В качестве источника обновлений для точек распространения могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского"
HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.
По умолчанию этот вариант выбран.
- Главный Сервер администрирования
Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
- Локальная или сетевая папка
Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует проверки подлинности, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

- **Папка для хранения обновлений**

Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

- **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий.

По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

10. Создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск задачи**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Вручную**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Каждые N минут**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрываемым списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Каждый N час**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрываемым списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Ежедневно (не поддерживается переход на летнее время)**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрываемым списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрывающемся списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, приложение будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрывающимся списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрывающимся списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрывающемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

11. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи *Загрузка обновлений в хранилища точек распространения* обновления баз и модули приложений копируются с источника обновлений и размещаются в папке общего доступа. Загруженные обновления будут использоваться только теми точками распространения, которые входят в указанную группу администрирования и для которых нет явно заданной задачи получения обновлений.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center

Обновления и патчи для Сервера администрирования могут быть установлены только после получения явного одобрения администратором.

Автоматическая установка обновлений для компонентов Kaspersky Security Center включена по умолчанию при установке Агента администрирования на устройство. Вы можете выключить ее при установке Агента администрирования или же выключить позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center при локальной установке Агента администрирования на устройство:*

1. Запустите локальную установку Агента администрирования на устройство.
2. На шаге **Дополнительные параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**.
3. Следуйте далее указаниям мастера.

На устройстве будет установлен Агент администрирования с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center при установке Агента администрирования на устройство с помощью инсталляционного пакета:*

1. В главном окне программы перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.
2. Нажмите на пакет **Агент администрирования Kaspersky Security Center <номер версии>**.
3. В окне свойств откройте вкладку **Параметры**.
4. Выключите переключатель **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**.

Агент администрирования будет устанавливаться из этого пакета с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

Если при установке Агента администрирования на устройство флажок был установлен (снят), впоследствии вы можете выключить (включить) автоматическую установку с помощью политики Агента администрирования.

- Чтобы включить или выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center с помощью политики Агента администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Нажмите на политику Агента администрирования.
3. В окне свойств политики откройте вкладку **Параметры приложения**.
4. В разделе **Управление патчами и обновлениями** установите включите или выключите переключатель **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** чтобы включить или выключить автоматическую установку обновлений и патчей.
5. Установите замок (🔒) для этого переключателя.

Политика применится к выбранным устройствам, и автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center будет включена (выключена) на этих устройствах.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского" [455](#)

Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows

Вы можете настроить автоматическое обновление баз и модулей приложения Kaspersky Endpoint Security для Windows на клиентских устройствах.

- Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security для Windows на устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Endpoint Security для Windows выберите подтип задачи **Обновление**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\\:|).
5. Выберите область действия задачи.
6. Укажите группу администрирования, выборку устройств или устройства, к которым применяется задача.
7. На шаге **Завершение создания задачи**, если вы хотите изменить параметры задачи по умолчанию, включите параметр **Открыть окно свойств задачи после ее создания**. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
8. Нажмите на кнопку **Создать**.
Задача будет создана и отобразится в списке задач.

9. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
10. В окне свойств задачи обновления на вкладке **Параметры приложения** укажите локальный или мобильный режим:
 - **Локальный режим:** между устройством и Сервером администрирования установлена связь.
 - **Мобильный режим:** между устройством и Kaspersky Security Center не установлена связь (например, если устройство не подключено к интернету).
11. Включите источники обновлений, которые вы хотите использовать для обновления баз и модулей приложения для Kaspersky Endpoint Security для Windows. Если требуется изменить положение источников обновлений в списке, используйте кнопки **Вверх** и **Вниз**. Если включено несколько источников обновлений, Kaspersky Endpoint Security для Windows пытается подключиться к ним один за другим, начиная с верхней части списка, и выполняет задачу обновления, извлекая пакет обновления из первого доступного источника.
12. Включите параметр **Устанавливать одобренные обновления модулей приложений**, чтобы загружать и устанавливать обновления модулей приложений вместе с базами приложений.
 Если параметр включен, то Kaspersky Endpoint Security для Windows уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления включает обновления модулей приложения в пакет обновлений. Kaspersky Endpoint Security для Windows устанавливает только те обновления, для которых вы установили статус *Одобрено*; обновления будут установлены локально через интерфейс приложения или через Kaspersky Security Center.
 Вы также можете включить параметр **Автоматически устанавливать критические обновления модуля приложения**. При наличии обновлений модулей приложения Kaspersky Endpoint Security для Windows устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей приложения – после одобрения их установки администратором.
 Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то приложение устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.
13. Установите флажок **Копировать обновления в папку**, чтобы приложение сохраняло загруженные обновления в папку, а затем укажите путь к папке.
14. Задайте расписание запуска задачи. Чтобы обеспечить своевременное обновление, рекомендуется выбрать вариант **При загрузке обновлений в хранилище**.
15. Нажмите на кнопку **Сохранить**.

При выполнении задачи **Обновление** приложение отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых приложений.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Одобрение и отклонение обновлений программного обеспечения

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

► Чтобы подтвердить или отменить одно или несколько обновлений:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения "Лаборатории Касперского"** → **Обновления**.

Отобразится список доступных обновлений.

Для обновлений управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center. Если эта версия более поздняя, чем ваша текущая, эти обновления отображаются, но не могут быть одобрены. Также из таких обновлений невозможно создать инсталляционные пакеты, пока вы не обновите Kaspersky Security Center. Вам будет предложено обновить ваш экземпляр Kaspersky Security Center до необходимой минимальной версии.

2. Выберите обновления, которые требуется подтвердить или отклонить.
3. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или **Отклонить**, чтобы отклонить выбранное обновление.

По умолчанию установлено значение *Не определено*.

Обновления, для которых вы установили статус *Одобрено*, помещаются в очередь на установку.

Обновления, для которых вы установили статус *Отклонено*, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для приложений "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус *Отклонено*, Kaspersky Security Center не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем. Если вы устанавливаете статус *Отклонено* для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить обновления, вы можете сделать это вручную локально.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского" [455](#)

Обновление Сервера администрирования

Вы можете установить обновления Сервера администрирования с помощью Мастер обновления Сервера администрирования.

► Чтобы установить обновления Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения "Лаборатории Касперского"** → **Обновления**.
2. Запустите Мастер обновления Сервера администрирования одним из следующих способов:
 - Нажмите на имя обновления Сервера администрирования в списке обновлений и в открывшемся окне перейдите по ссылке **Запустить мастер обновления Сервера администрирования**.
 - Перейдите по ссылке **Запустить мастер обновления Сервера администрирования** в поле уведомления в верхней части окна приложения.
3. Чтобы указать, когда устанавливать обновление, в окне Мастер обновления Сервера администрирования выберите один из следующих вариантов:
 - **Установить сейчас**. Выберите этот вариант, если вы хотите установить обновления сейчас.
 - **Отложить установку**. Выберите этот вариант, если вы хотите установить обновления позже. В этом случае будет отображаться уведомление об этом обновлении.
 - **Игнорировать это обновление**. Выберите этот вариант, если вы не хотите устанавливать обновление и не хотите получать уведомления об этом обновлении.
4. Если вы хотите создать резервную копию Сервера администрирования перед установкой обновления, выберите параметр **Сделать резервную копию Сервера администрирования перед установкой обновления**.
5. Нажмите на кнопку **ОК**, чтобы закрыть окно мастера.

В процессе резервного копирования прерывается процесс установки обновлений.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Включение и выключение офлайн-модели получения обновлений

Не рекомендуется выключать офлайн-модель получения обновлений. Выключение может привести к сбоям в доставке обновлений на устройства. В некоторых случаях специалисты Службы технической поддержки "Лаборатории Касперского" могут рекомендовать вам выключить параметр **Загружать обновления и антивирусные базы с Сервера администрирования заранее**. Тогда вам нужно будет убедиться, что задача загрузки обновлений в хранилище для приложений "Лаборатории Касперского" настроена.

► **Чтобы включить или выключить офлайн-модель получения обновлений для группы администрирования:**

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Нажмите на кнопку **Группы**.
3. В списке групп администрирования выберите группу администрирования, для которой требуется включить офлайн-модель получения обновлений.
4. Нажмите на политику Агента администрирования.

Откроется окно свойств политики Агента администрирования.

По умолчанию параметры дочерней политики наследуют параметры родительской политики и не могут быть изменены. Если политика, которую вы хотите изменить, унаследована, то вам нужно создать политику для Агента администрирования в требуемой группе администрирования. В созданной политике вы можете изменить параметры, которые не заблокированы в родительской политике.

5. В окне **Параметры приложения** выберите раздел **Управление патчами и обновлениями**.
6. Включите или выключите параметр **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**, чтобы включить или выключить офлайн-модель получения обновлений соответственно.

По умолчанию офлайн-модель получения обновлений включена.

В результате офлайн-модель получения обновлений будет включена или выключена.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского" [455](#)

Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах

Обновление баз и модулей приложений "Лаборатории Касперского" на управляемых устройствах является важной задачей для обеспечения защиты устройств от вирусов и других угроз. Администратор обычно настраивает регулярное обновление (см. раздел "Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"" см. стр. [455](#)) с помощью хранилища Сервера администрирования или хранилищ точек распространения.

Когда вам необходимо обновить базы данных и модули приложений на устройстве (или группе устройств), которое не подключено к Серверу администрирования (главному или подчиненному), точке распространения или интернету, вам необходимо использовать альтернативные источники обновлений, такие как FTP-сервер или локальная папка. В этом случае вам нужно доставить файлы необходимых обновлений с помощью запоминающего устройства, такого как флеш-накопитель или внешний жесткий диск.

Вы можете скопировать требуемые обновления с:

- Сервера администрирования.

Чтобы хранилище Сервера администрирования содержало обновления, необходимые для приложения безопасности, установленного на автономном устройстве, по крайней мере на одном из управляемых сетевых устройств должно быть установлено это приложение безопасности. Это приложение должно быть настроено на получение обновлений из хранилища Сервера администрирования с помощью задачи Загрузка обновлений в хранилище Сервера администрирования.

- Любого устройства, на котором установлено такое же приложение безопасности и настроено получение обновлений из хранилища Сервера администрирования, хранилища точки распространения или напрямую с серверов обновлений "Лаборатории Касперского".

Ниже приведен пример настройки обновлений баз и модулей приложений путем копирования их из хранилища Сервера администрирования.

► *Чтобы обновить базы данных и модули приложений "Лаборатории Касперского" на автономных устройствах:*

1. Подключите съемный диск к устройству, на котором установлен Сервер администрирования.
2. Скопируйте файлы обновлений на съемный диск.

По умолчанию обновления расположены: \\<server name>\KLSHARE\Updates.

Также вы можете настроить в Kaspersky Security Center регулярное копирование обновлений в выбранную вами папку. Для этого используйте параметр **Копировать полученные обновления в дополнительные папки** в свойствах задачи Загрузка обновлений в хранилище Сервера администрирования. Если вы укажете папку, расположенную на запоминающем устройстве или внешнем жестком диске, в качестве папки назначения для этого параметра, это запоминающее устройство всегда будет содержать последнюю версию обновлений.

3. На автономных устройствах настройте программу безопасности (например, настройте Kaspersky Endpoint Security для Windows) на получение обновлений из локальной папки или общего ресурса, такого как FTP-сервер или общая папка.
4. Скопируйте файлы обновлений со съемного диска в локальную папку или общий ресурс, который вы хотите использовать в качестве источника обновлений.
5. На автономном устройстве, на которое требуется установить обновления, запустите задачу обновления Kaspersky Endpoint Security для Windows.

После завершения задачи обновления базы данных и модули приложений "Лаборатории Касперского" будут обновлены на устройстве.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"	455
Создание задачи Загрузка обновлений в хранилище Сервера администрирования	1347

Резервное копирование и восстановление веб-плагинов

Kaspersky Security Center Web Console позволяет создавать резервную копию данных текущего состояния веб-плагина, чтобы впоследствии можно было восстановить сохраненное состояние. Например, вы можете создать резервную копию данных веб-плагина перед его обновлением до более новой версии. После

обновления, если более новая версия не соответствует вашим требованиям или ожиданиям, вы можете восстановить предыдущую версию веб-плагинов из резервной копии данных.

► *Для резервного копирования данных веб-плагинов:*

1. В главном окне приложения перейдите в раздел **Параметры** → **Веб-плагины**.
2. В разделе **Веб-плагины** выберите веб-плагины, для которых требуется создать резервную копию данных и нажмите на кнопку **Создать резервную копию данных**.

Резервное копирование данных выбранных веб-плагинов. Вы можете просмотреть созданные резервные копии данных на вкладке **Резервные копии данных**.

► *Чтобы восстановить веб-плагин из резервной копии данных:*

1. В главном окне приложения перейдите в раздел **Параметры** → **Резервные копии данных**.
2. В разделе **Резервные копии данных** выберите резервную копию данных веб-плагинов, который вы хотите восстановить, а затем нажмите на кнопку **Восстановить из резервной копии данных**.

Веб-плагин восстанавливается из выбранной резервной копии данных.

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.
Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область действия политик задается с помощью тегов, местоположения устройств в подразделениях Active Directory, членства в группах безопасности Active Directory и прочего.
- Задание области действия групповых задач.
Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.
- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.
- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- Один офис.
- Множество небольших изолированных офисов.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

В этом разделе

Типовая конфигурация точек распространения: один офис.....[686](#)

Типовая конфигурация точек распространения: множество небольших удаленных офисов[687](#)

О назначении точек распространения[1369](#)

Автоматическое назначение точек распространения[1370](#)

Назначение точек распространения вручную[1370](#)

Изменение списка точек распространения для группы администрирования[1375](#)

Принудительная синхронизация[1376](#)

Включение push-сервера[1378](#)

Типовая конфигурация точек распространения: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных частей (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Можно использовать автоматическое назначение точек распространения, либо назначать точки распространения вручную.
- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение точек распространения и в каждой выделенной части сети назначить одно или несколько устройств точками распространения на корневую группу администрирования, например, на группу **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты `tracert`.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Типовая конфигурация точек распространения: множество небольших удаленных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).

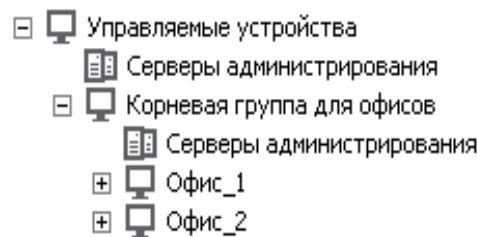


Рисунок 17. Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить одну или несколько точек распространения. Точками распространения нужно назначать устройства удаленного офиса, имеющие достаточно места на диске. Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Ноутбук, находившийся в группе администрирования **Офис 1**, но физически перемещенный в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

О назначении точек распространения

Вы можете назначить управляемое устройство в качестве точки распространения вручную (см. раздел "Назначение точек распространения вручную" на стр. [1370](#)) или автоматически (см. раздел "Автоматическое назначение точек распространения" на стр. [1370](#)).

Если вы назначаете управляемое устройство в качестве точки распространения вручную, вы можете выбрать любое устройство в своей сети.

Если вы назначаете точки распространения автоматически, Kaspersky Security Center может выбрать только то управляемые устройства, которые соответствует следующим условиям:

- Устройство должно иметь не менее 50 ГБ свободного места на диске.

- Управляемое устройство подключается к Kaspersky Security Center напрямую (не через шлюз).
- Управляемое устройство не является ноутбуком.

Если в вашей сети нет устройств, соответствующих заданным условиям, Kaspersky Security Center не будет автоматически назначать какое-либо устройство точкой распространения.

Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать (см. раздел "О назначении точек распространения" на стр. [1369](#)), какие устройства назначать точками распространения.

► Чтобы назначить точки распространения автоматически:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.
3. Выберите параметр **Автоматически назначать точки распространения**.

Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

4. Нажмите на кнопку **Сохранить**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Назначение точек распространения вручную

Kaspersky Security Center позволяет вручную назначать устройства точками распространения.

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения. Однако если вы по какой-то причине хотите отказаться от автоматического назначения точек распространения (например, если вы хотите использовать специально выделенные серверы), вы можете назначать точки распространения вручную, предварительно рассчитав их количество и конфигурацию.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

► Чтобы вручную назначить устройство точкой распространения:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.
3. Выберите параметр **Вручную назначать точки распространения**.
4. Нажмите на кнопку **Назначить**.
5. Выберите устройство, которое вы хотите сделать точкой распространения.

При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения.

6. Выберите группу администрирования, которую вы хотите включить в область действия выбранной точки распространения.
7. Нажмите на кнопку **ОК**.

Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

8. Нажмите на добавленную точку распространения в списке, чтобы открыть окно ее свойств.
9. В окне свойств настройте параметры точки распространения:

- В разделе **Общие** укажите параметр взаимодействия точки распространения с клиентскими устройствами:

- **SSL-порт**

Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к агенту обновлений с использованием протокола SSL.

По умолчанию номер порта – 13000.

- **Использовать многоадресную IP-рассылку**

Если флажок установлен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

- **Адрес IP-рассылки**

IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

По умолчанию указан IP-адрес 225.6.7.8.

- **Номер порта IP-рассылки**

Номер порта многоадресной рассылки.

Номер порта по умолчанию – 15001. Если в качестве агента обновлений указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.

- **Адрес точки распространения для удаленных устройств**
- **Распространять обновления**

Если флажок установлен, обновления распространяются на клиентские устройства с помощью этого агента обновлений.

По умолчанию флажок установлен.

- **Распространять инсталляционные пакеты**

Если флажок установлен, инсталляционные пакеты обновления распространяются на клиентские устройства с помощью этого агента обновлений.

По умолчанию флажок установлен.

- **Запустить push-сервер**

- **Порт push-сервера**

- В разделе **Область действия** укажите область, на которую точка распространения распространяет обновления (группы администрирования и/или сетевое местоположение).

Только устройства под управлением операционной системы Windows могут определять свое сетевое местоположение. Определение сетевого местоположения недоступно для устройств под управлением других операционных систем.

- Если точка распространения работает на машине, отличной от Сервера администрирования, в разделе **Источник обновлений** можно выбрать источник обновлений для точки распространения:

- **Источник обновлений**

- **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий.

По умолчанию параметр включен.

- В разделе **Параметры подключения к интернету** можно настроить параметры доступа к сети интернет:

- **Использовать прокси-сервер**

Если флажок установлен, в полях ввода можно настроить параметры подключения к прокси-серверу.

По умолчанию флажок снят.

- **Адрес прокси-сервера**

Адрес прокси-сервера.

- **Номер порта**

Номер порта, по которому будет выполняться подключение.

- **Не использовать прокси-сервер для локальных адресов**

Если флажок установлен, то при подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

По умолчанию флажок снят.

- **Аутентификация на прокси-сервере**

Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

По умолчанию флажок снят.

- **Имя пользователя**

Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

- В разделе **Прокси-сервер KSN** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.

- **Включить прокси-сервер KSN на стороне точки распространения**

Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Пересылать KSN запрос Серверу администрирования**

Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

По умолчанию параметр включен.

- **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к KPSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения.

Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к KPSN.

- **Игнорировать параметры прокси-сервера для подключения к KPSN**

Установите этот флажок, если параметры прокси-сервера настроены в свойствах точки распространения или политики Агента администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

Это параметр доступен, если вы выбрали параметр **Доступ к облачной службе**

KSN/KPSN непосредственно через интернет.

- **Порт**

Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.
- **Использовать UDP-порт**
- **UDP-порт**
- Если точка распространения работает на машине, отличной от Сервера администрирования, в разделе **Шлюз соединения** можно настроить точку распространения как шлюз соединения для экземпляров Агента администрирования и Сервером администрирования:
 - **Шлюз соединения**
 - **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**
 - **Открыть локальный порт для Kaspersky Security Center Web Console**

При подключении мобильных устройств к Серверу администрирования через точку распространения, выполняющую роль шлюза соединения, вы можете включить следующие параметры:

- **Открыть порт для мобильных устройств (SSL-аутентификация только Сервера администрирования)**
- **Открыть порт для мобильных устройств (двусторонняя SSL-аутентификация)**

В обоих случаях сертификаты проверяются во время установки TLS-сеанса только на точке распространения. Сертификаты не пересылаются на проверку Сервером администрирования. После установки TLS-сеанса с мобильным устройством точка распространения использует сертификат Сервера администрирования для создания туннеля для синхронизации между мобильным устройством и Сервером администрирования. Если вы откроете порт для двусторонней SSL-аутентификации, единственный способ распространить сертификат мобильного устройства – это с помощью установочного пакета.
- Настройте опрос доменов Windows, Active Directory и IP-диапазонов точкой распространения:
 - **Windows-домены**

Вы можете включить обнаружение устройств для Windows-доменов и задать его расписание.
 - **Контроллеры домена**
 - **IP-диапазоны**

Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов.

Если включить параметр **Использовать Zeroconf для опроса IPv6-сетей**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией <http://www.zeroconf.org/> (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вам нужно установить утилиту avahi-browse на точке

распространения.

- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных:

- **Использовать папку по умолчанию**

При выборе этого варианта для сохранения данных будет использоваться папка, в которую на агенте обновлений установлен Агент администрирования.

- **Использовать указанную папку**

При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на агенте обновлений, так и удаленно, на любом из устройств, входящих в состав сети организации.

Учетная запись, под которой на агенте обновлений запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

10. Нажмите на кнопку **ОК**.

В результате выбранные устройства будут выполнять роль точек распространения.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Изменение списка точек распространения для группы администрирования

Вы можете просмотреть список точек распространения, назначенных для определенной группы администрирования, и изменить список, добавив или удалив точки распространения.

► *Чтобы просмотреть и изменить список точек распространения для группы администрирования:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
3. В открывшейся панели слева выберите группу администрирования, для которой вы хотите просмотреть назначенные точки распространения.

Для этого используйте пункт меню **Точки распространения**.

4. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Точки распространения**.
5. Чтобы добавить точки распространения для группы администрирования, нажмите на кнопку **Назначить** над списком управляемых устройств и выберите устройства в открывшейся панели.
6. Чтобы удалить назначенные точки распространения, выберите устройства из списка и нажмите на кнопку **Отменить назначение**.

В зависимости от изменений, точки распространения добавляются в список или существующие точки распространения удаляются из списка.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

Принудительная синхронизация

Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, но в некоторых случаях вам может потребоваться запустить синхронизацию для указанного устройства принудительно. Вы можете запустить принудительную синхронизацию для следующих устройств:

- Устройств с установленным Агентом администрирования.
- Устройств под управлением KasperskyOS.

Перед запуском принудительной синхронизации для устройства под управлением KasperskyOS убедитесь, что устройство включено в область действия точки распространения и что на точке распространения включен push-сервер (см. раздел "Включение push-сервера" см. стр. [1378](#)).

- iOS-устройств.
- Android-устройств.

Перед запуском принудительной синхронизации для Android-устройства необходимо настроить Firebase Cloud Messaging.

Синхронизация одного устройства

► *Чтобы осуществить принудительную синхронизацию между Сервером администрирования и управляемым устройством:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования. В открывшемся окне свойств выберите раздел **Общие**.
3. Нажмите на кнопку **Синхронизировать принудительно**.

Приложение выполняет синхронизацию выбранного устройства с Сервером администрирования.

Синхронизация нескольких устройств

► *Чтобы осуществить принудительную синхронизацию между Сервером администрирования и несколькими управляемыми устройствами:*

1. Откройте список устройств группы администрирования или выборку устройств:
 - В главном меню перейдите в раздел **Активы (Устройства) → Управляемые устройства**, перейдите по ссылке в поле **Текущий путь** над списком управляемых устройств и выберите группу администрирования, в которую входят устройства для синхронизации.
 - Запустите выборку устройств (см. раздел "Выборки устройств" на стр. [1218](#)), чтобы просмотреть список устройств.

2. Установите флажки рядом с устройствами, которые требуется синхронизировать с Сервером администрирования.
3. Над списком управляемых устройств нажмите на кнопку с многоточием (**...**) и нажмите на кнопку **Синхронизировать принудительно**.

Приложение выполняет синхронизацию выбранных устройств с Сервером администрирования.

4. В списке устройств проверьте, что время последнего подключения к Серверу администрирования для выбранных устройств изменилось на текущее время. Если время не изменилось, обновите содержимое страницы, нажав на кнопку **Обновить**.

Выбранные устройства синхронизированы с Сервером администрирования.

Просмотр времени доставки политики

После изменения политики для приложения "Лаборатории Касперского" на Сервере администрирования администратор может проверить, доставлена ли измененная политика на определенные управляемые устройства. Политика может быть доставлена во время регулярной или принудительной синхронизации.

► *Чтобы просмотреть дату и время доставки политики приложения на управляемые устройства:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования. В открывшемся окне свойств выберите раздел **Общие**.
3. Выберите вкладку **Приложения**.
4. Выберите приложение, для которого требуется посмотреть дату синхронизации политики.

Откроется окно политики приложения, с выбранным разделом **Общие**, и отобразится дата и время доставки политики.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства	405
Сценарий: настройка защиты сети.....	403
Включение push-сервера	1378

Включение push-сервера

В Kaspersky Security Center точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию (см. раздел "Принудительная синхронизация" см. стр. [1376](#)) устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой из них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Возможно, вы захотите использовать точки распространения в качестве push-серверов, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Постоянное соединение необходимо для некоторых операций, таких как запуск и остановка локальных задач, получение статистики для управляемого приложения или создание туннеля. Если вы используете точку распространения в качестве сервера push-сервера, вам не нужно использовать параметр **Не разрывать соединение с Сервером администрирования** на управляемых устройствах или отправлять пакеты на UDP-порт Агента администрирования.

Push-сервер поддерживает нагрузку до 50 000 одновременных подключений.

► Чтобы включить push-сервер на точке распространения:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
 2. На вкладке **Общие** выберите раздел **Точки распространения**.
 3. Нажмите на имя точки распространения, на которой вы хотите включить push-сервер.
Откроется окно свойств точки распространения.
 4. В разделе **Общие** включите параметр **Запустить push-сервер**.
 5. В поле **Порт push-сервера** укажите номер порта. Вы можете указать номер любого свободного порта.
 6. В поле **Адрес удаленного устройства** укажите IP-адрес или имя точки распространения.
 7. Нажмите на кнопку **ОК**.
- Push-сервер включен на выбранной точке распространения.

См. также:

Принудительная синхронизация [1376](#)

Управление приложениями сторонних производителей на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center связанные с управлением сторонними приложениями на клиентских устройствах.

В этом разделе

О приложениях сторонних производителей	1379
Установка обновлений приложений сторонних производителей	1383
Заккрытие уязвимостей в приложениях сторонних производителей	1416
Управление запуском приложений на клиентских устройствах	1441
Создание инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"	1459
Просмотр и изменение параметров инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"	1460
Параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"	1461
Теги приложений	1463

О приложениях сторонних производителей

Kaspersky Security Center может помочь вам обновить приложения сторонних производителей, установленное на клиентских устройствах, и закрыть уязвимости в приложениях сторонних производителей. Kaspersky Security Center может обновлять приложения сторонних производителей только с текущей версии до последней версии. В следующем списке представлены приложения сторонних производителей, которые вы можете обновить с помощью Kaspersky Security Center:

Список приложений сторонних производителей может обновляться и увеличиваться за счет новых приложений. Вы можете проверить, можете ли вы обновить приложение сторонних производителей (установленное на устройствах пользователей) с помощью Kaspersky Security Center, просмотрев список доступных обновлений в Kaspersky Security Center Web Console (см. раздел "Установка обновлений приложений сторонних производителей" на стр. [1389](#)).

- 7-Zip Developers: 7-Zip.
- Adobe Systems:
 - Adobe Acrobat DC;
 - Adobe Acrobat Reader DC;
 - Adobe Acrobat;
 - Adobe Reader;

- Adobe Shockwave Player.
- AIMPDevTeam: AIMP.
- ALTAP: Altap Salamander.
- Apache Software Foundation: Apache Tomcat.
- Apple:
 - Apple iTunes;
 - Apple QuickTime.
- Armory Technologies, Inc.: Armory.
- Cerulean Studios: Trillian Basic.
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber.
- Code Sector:
- Codec Guide:
 - K-Lite Codec Pack Basic;
 - K-Lite Codec Pack Full;
 - K-Lite Codec Pack Mega;
 - K-Lite Codec Pack Standard.
- DbVis Software AB:
- Decho Corp.:
 - Mozy Enterprise;
 - Mozy Home;
 - Mozy Pro.
- Dominik Reichl: KeePass Password Safe.
- Don HO don.h@free.fr: Notepad++.
- DoubleGIS: 2GIS.
- Dropbox, Inc.: Dropbox.
- aeUs: EaseUS Todo Backup Free.
- Electrum Technologies GmbH:
- Enter Srl: Iperius Backup.
- Eric Lawrence:
- EverNote: EverNote.
- Exodus Movement Inc: Exodus.
- EZB Systems:
- Famatech:
 - Radmin;

- Remote Administrator.
- Far Manager: FAR Manager.
- FastStone Soft: FastStone Image Viewer.
- FileZilla Project:
- Firebird Developers:
- Foxit Corporation:
 - Foxit Reader;
 - Foxit Reader Enterprise.
- Free Download Manager.ORG: Free Download Manager.
- GIMP project:
- GlavSoft LLC.: TightVNC.
- GNU Project: Gpg4win.
- Google:
 - Google Earth;
 - Google Chrome;
 - Google Chrome Enterprise;
 - Google Earth Pro.
- Inkscape Project:
- IrfanView: IrfanView.
- iterate GmbH:
- Logitech: SetPoint.
- LogMeIn, Inc.:
 - LogMeIn;
 - Hamachi;
 - LogMeIn Rescue Technician Console.
- Martin Prikryl:
- Microsoft: SQL Server Management Studio.
- Mozilla Foundation:
 - Mozilla Firefox;
 - Mozilla Firefox ESR;
 - Mozilla SeaMonkey;
 - Mozilla Thunderbird.
- New Cloud Technologies Ltd: Home Edition.
- OpenOffice.org: OpenOffice.

- Oracle Corporation:
 - Oracle Java JRE;
 - Oracle VirtualBox.
- PDF44: PDF24 MSI/EXE.
- Piriform:
 - CCleaner;
 - Defraggler;
 - Recuva;
 - Speccy.
- PostgreSQL: PostgreSQL.
- RealPlayer Cloud.
- RealVNC:
 - RealVNC Server;
 - RealVNC Viewer.
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (Complete/Minimum).
- Simon Tatham:
- Skype Technologies: Skype for Windows.
- Sober Lemur S.a.s.:
 - PDFsam Basic;
 - PDFsam Visual.
- Softland: FBackup.
- Splashtop Inc.: Splashtop Streamer.
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP.
- Sublime HQ Pty Ltd: Sublime Text.
- TeamViewer GmbH:
 - TeamViewer Host;
 - TeamViewer.
- Telegram Messenger LLP: Telegram Desktop.
- The Document Foundation:
 - LibreOffice;
 - LibreOffice HelpPack.
- The Git Development Community:
 - Git for Windows;
 - Git LFS.
- The Pidgin developer community:

- TortoiseSVN Developers:
- VLC media player.
- VMware:
 - VMware Player;
 - VMware Workstation.
- WinRAR Developers: WinRAR.
- WinZip: WinZip.
- Wireshark Foundation: Wireshark.
- Wrike: Wrike.
- Zimbra: Zimbra Desktop.

См. также:

Сценарий: обновление приложений сторонних производителей	499
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....	529
Установка обновлений приложений сторонних производителей	1383

Установка обновлений приложений сторонних производителей

Kaspersky Security Center позволяет управлять обновлениями программного обеспечения сторонних производителей, установленных на управляемых устройствах, и закрывать уязвимости в приложениях Microsoft и других производителей программного обеспечения с помощью установки необходимых обновлений.

Kaspersky Security Center выполняет поиск обновлений с помощью задачи *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Сервер администрирования получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах. После просмотра информации о доступных обновлениях вы можете выполнить установку обновлений на устройства.

Обновление некоторых приложений Kaspersky Security Center выполняется путем удаления предыдущей версии приложения и установки новой версии приложения.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются

для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Специалисты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также специалисты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Задачи для установки обновлений приложений сторонних производителей

Когда метаданные обновлений приложений сторонних производителей загружаются в хранилище, вы можете установить обновления на клиентские устройства, выполнив следующие задачи:

- *Задача Установка требуемых обновлений и закрытия уязвимостей* (см. раздел "Создание задачи Установка требуемых обновлений и закрытие уязвимостей" см. стр. [1399](#)).

Задача Установка требуемых обновлений и закрытие уязвимостей используется для установки обновлений для приложений Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления приложений других поставщиков. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование.

После завершения работы этой задачи обновления устанавливаются на управляемые устройства автоматически. При загрузке метаданных новых обновлений в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли обновления критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут загружены и установлены автоматически при следующем запуске задачи.

- *Задача Установка обновлений Центра обновления Windows* (см. раздел "Создание задачи Установка обновлений Центра обновления Windows" см. стр. [1407](#)).

Задача Установка обновлений Центра обновления Windows не требует лицензии, но ее можно использовать только для установки обновлений Центра обновления Windows.

После завершения работы этой задачи устанавливаются только те обновления, которые указаны в свойствах задачи. Позже, если вы захотите установить новые обновления, загруженные в хранилище Сервера администрирования, вам будет необходимо добавить требуемые обновления в список обновлений существующей задачи или создать задачу *Установка обновлений Центра обновления Windows*.

Использовать Сервер администрирования в роли WSUS-сервера

Информация о доступных обновлениях Microsoft Windows передается из центра обновлений Windows. Сервер администрирования может использоваться в роли сервера Windows Update (WSUS). Чтобы использовать Сервер администрирования в качестве WSUS-сервера, вам нужно создать задачу Синхронизация обновлений Windows Update и выберите параметр **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования. После настройки синхронизации данных с центром обновлений Windows Сервер администрирования с заданной периодичностью централизованно предоставляет обновления службам Windows Update на устройствах.

В этом разделе

Сценарий: обновление приложений сторонних производителей	499
Установка обновлений приложений сторонних производителей	1389
Создание задачи Поиск уязвимостей и требуемых обновлений	1393
Параметры задачи поиска уязвимостей и требуемых обновлений.	1396
Создание задачи Установка требуемых обновлений и закрытие уязвимостей	1399
Добавление правил для установки обновлений	1403
Создание задачи Установка обновлений Центра обновления Windows	1407
Просмотр информации о доступных обновлениях приложений сторонних производителей.	1410
Экспорт списка доступных обновлений в файл	1411
Одобрение и отклонение обновлений приложений сторонних производителей	1412
Создание задачи Синхронизация обновлений Windows Update	1413
Автоматическое обновление приложений сторонних производителей	1415

Сценарий: обновление приложений сторонних производителей

В этом разделе представлен сценарий обновления приложений сторонних производителей, установленных на клиентских устройствах. Приложения сторонних производителей включают в себя приложения от Microsoft и других поставщиков программного обеспечения (см. раздел "О приложениях сторонних производителей" на стр. [1379](#)). Обновления для приложений Microsoft предоставляются службой Центра обновления Windows.

Предварительные требования

Сервер администрирования должен иметь подключение к интернету для установки обновлений приложений сторонних производителей, отличных от приложений Microsoft.

По умолчанию Сервер администрирования не требует подключения к интернету для установки обновлений приложений Microsoft на управляемые устройства. Например, управляемые устройства могут загружать обновления приложений Microsoft непосредственно с серверов обновлений Microsoft или с Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации. Если вы используете Сервер администрирования в качестве сервера WSUS, Сервер администрирования должен быть подключен к интернету.

Этапы

Обновление производителей состоит из следующих этапов:

а. Поиск требуемых обновлений

Чтобы найти обновления приложений сторонних производителей, необходимые для управляемых устройств, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky Security Center Сервера администрирования. Если вы не запустили мастер, создайте задачу или запустите мастер первоначальной настройки.

Инструкции:

- Консоль администрирования: Поиск уязвимостей в приложениях, Задание расписания для задачи поиска уязвимостей и требуемых обновлений.
- Kaspersky Security Center Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений (на стр. [1393](#)), Параметры задачи поиска уязвимостей и требуемых обновлений (см. раздел "Параметры задачи поиска уязвимостей и требуемых обновлений." см. стр. [1396](#)).

b. Анализ списка найденных обновлений

Просмотрите список **Обновления программного обеспечения** и решите, какие обновления следует установить. Чтобы просмотреть подробную информацию о каждом обновлении, нажмите на имя обновления в списке. Для каждого обновления в списке также можно просмотреть статистику установки обновлений на клиентских устройствах.

Инструкции:

- Консоль администрирования: Просмотр информации о доступных обновлениях.
- Kaspersky Security Center Web Console: Просмотр информации о доступных обновлениях приложений сторонних производителей (см. раздел "Просмотр информации о доступных обновлениях приложений сторонних производителей." см. стр. [1410](#)).

c. Настройка установки обновлений

После того как Kaspersky Security Center получает список обновлений приложений сторонних производителей, вы можете установить их на клиентские устройства, используя задачу *Установка требуемых обновлений и закрытия уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Создайте одну из этих задач. Вы можете создать эти задачи на вкладке **Задачи** или с помощью списка **Обновления программного обеспечения**.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для установки обновлений для приложений Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления приложений других поставщиков. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование.

Задача *Установка обновлений Центра обновления Windows* не требует лицензии, но ее можно использовать только для установки обновлений Центра обновления Windows.

Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

Вы можете запустить задачу установки обновления по расписанию. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Инструкции:

- Консоль администрирования: Закрытие уязвимостей в приложениях, Просмотр информации о доступных обновлениях.
- Kaspersky Security Center Web Console: Создание задачи Установка требуемых обновлений и закрытие уязвимостей (см. стр. [1399](#)), Создание задачи Установка обновлений Центра обновления Windows (см. стр. [1407](#)), Просмотр информации о доступных обновлениях приложений сторонних производителей (см. раздел "Просмотр информации о доступных обновлениях приложений сторонних производителей." см. стр. [1410](#)).

d. Задание расписания задачи

Чтобы убедиться, что список обновлений всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. По умолчанию задача *Поиск уязвимостей и требуемых обновлений* запускается в 18:00:00 вручную.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. При планировании задачи *Установка обновлений Центра обновления Windows* обратите внимание, что для этой задачи вам нужно определять список обновлений каждый раз перед запуском этой задачи.

При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

e. Одобрение и отклонение обновлений программного обеспечения (если требуется)

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете указать правила установки обновлений в свойствах задачи. Если вы создали задачу *Установка обновлений Центра обновления Windows*, пропустите этот шаг.

Для каждого правила вы можете выбрать устанавливаемые обновления в зависимости от их статуса: *Не определено*, *Одобрено* или *Отклонено*. Например, вы можете создать определенную задачу для серверов и установить правило для этой задачи, чтобы разрешить установку только обновлений Центра обновления Windows и только тех, которые имеют статус *Одобрено*. После этого вы вручную устанавливаете статус *Одобрено* для тех обновлений, которые вы хотите установить. В этом случае обновления Центра обновления Windows со статусом *Не определено* или *Отклонено* не будут установлены на серверы, указанные в задаче.

При управлении установкой обновлений использовать статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. При ручном одобрении большого количества обновлений производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус на *Одобрено* или *Отклонено* в списке **Обновления программного обеспечения (Операции → Управление патчами → Обновления программного обеспечения)**.

Инструкции:

- Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения.
- Kaspersky Security Center Web Console: Одобрение и отклонение обновлений приложений сторонних производителей (см. раздел "Одобрение и отклонение обновлений приложений сторонних производителей." см. стр. [1412](#)).

f. Настройка Сервера администрирования для работы в качестве службы Windows Server Update Services (WSUS) (если требуется)

По умолчанию обновления Центра обновления Windows загружаются на управляемые устройства с серверов Microsoft. Вы можете изменить этот параметр, чтобы использовать Сервер администрирования в роли WSUS-сервера. В этом случае Сервер администрирования синхронизирует данные обновления с Центром обновления Windows с заданной периодичностью и предоставляет обновления централизованно службам Центра обновления Windows на сетевых устройствах.

Чтобы использовать Сервер администрирования в качестве сервера WSUS, создайте задачу Синхронизация обновлений Windows Update и установите флажок **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования.

Инструкции:

- Консоль администрирования: Синхронизация обновлений Windows Update с Сервером администрирования, Настройка обновлений Windows в политике Агента администрирования.
- Kaspersky Security Center Web Console: Создание задачи Синхронизация обновлений Windows Update (см. раздел "Создание задачи Синхронизация обновлений Windows Update." см. стр. [1413](#)).

г. Запуск задачи установки обновлений

Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. После запуска этих задач, обновления загружаются и устанавливаются на управляемые устройства. После завершения задачи убедитесь, что в списке задач она имеет статус *Завершена успешно*.

h. Создание отчета о результатах установки обновлений приложений сторонних производителей (если требуется)

Чтобы просмотреть статистику установки обновления, сформируйте **Отчет о результатах установки обновлений стороннего ПО**.

Инструкции:

- Консоль администрирования: Создание и просмотр отчета.
- Kaspersky Security Center Web Console: Генерация и просмотр отчета (см. стр. [1479](#)).

Результаты

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытия уязвимостей*, обновления будут автоматически установлены на управляемые устройства. При загрузке новых обновлений в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли они критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут установлены автоматически при следующем запуске задачи.

Если вы создали задачу *Установка обновлений Центра обновления Windows*, будут установлены только те обновления, которые указаны в свойствах задачи *Установка обновлений Центра обновления Windows*. Позже, если вы захотите установить новые обновления, загруженные в хранилище Сервера администрирования, вам будет необходимо добавить требуемые обновления в список обновлений существующей задачи или создать задачу *Установка обновлений Центра обновления Windows*.

См. также

Установка обновлений приложений сторонних производителей	1389
Создание задачи Поиск уязвимостей и требуемых обновлений	1393
Параметры задачи поиска уязвимостей и требуемых обновлений.	1396
Создание задачи Установка требуемых обновлений и закрытие уязвимостей	1399
Добавление правил для установки обновлений	1403
Создание задачи Установка обновлений Центра обновления Windows	1407
Просмотр информации о доступных обновлениях приложений сторонних производителей.	1410
Экспорт списка доступных обновлений в файл	1411
Одобрение и отклонение обновлений приложений сторонних производителей	1412
Создание задачи Синхронизация обновлений Windows Update	1413
Автоматическое обновление приложений сторонних производителей	1415
О приложениях сторонних производителей	1379

Установка обновлений приложений сторонних производителей

Вы можете установить обновления приложений сторонних производителей на управляемые устройства, создав и запустив одну из следующих задач:

- *Установка требуемых обновлений и закрытие уязвимостей* (см. раздел "Создание задачи Установка требуемых обновлений и закрытие уязвимостей" см. стр. [1399](#))

Задачу *Установка требуемых обновлений и закрытие уязвимостей* можно создать, только если у вас есть лицензия на Системное администрирование. Эту задачу можно использовать для установки обновлений Центра обновления Windows, предоставленных Microsoft, и обновлений приложений других поставщиков.

- *Установка обновлений Центра обновления Windows* (см. раздел "Создание задачи Установка обновлений Центра обновления Windows" см. стр. [1407](#))

Задачу *Установка обновлений Центра обновления Windows* можно использовать только для установки только обновлений Центра обновления Windows.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Также вы можете создать задачу для установки необходимых обновлений следующими способами:

- Открыть список обновлений и указать, какие обновления устанавливать.

В результате создается задача для установки выбранных обновлений. Также вы можете добавить выбранные обновления в существующую задачу.

- Запустить мастер установки обновлений.

Мастер установки обновления доступен при наличии лицензии на Системное администрирование.

Мастер упрощает создание и настройку задачи установки обновлений и позволяет исключить создание избыточных задач, содержащих те же самые обновления для установки.

Установка обновлений приложений сторонних производителей с помощью списка обновлений

► Чтобы установить обновления приложений сторонних производителей:

1. Откройте один из списков обновлений:

- Чтобы открыть список общих обновлений, перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.
- Чтобы открыть список обновлений для управляемого устройства, перейдите в раздел **Активы (Устройства)** → **Управляемые устройства** → <имя устройства> → **Дополнительно** → **Применимые обновления**.
- Чтобы открыть список обновлений для определенной программы, перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений** → <имя программы> → **Применимые обновления**.

Отобразится список доступных обновлений.

2. Установите флажки рядом с теми обновлениями, которые вы хотите установить.
3. Нажмите на кнопку **Установить обновления**.

Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не установятся.

4. Выберите один из следующих вариантов:

- **Новая задача**

Запустится мастер создания задачи (см. раздел "Создание задачи" на стр. [1174](#)). Если у вас есть лицензия на Системное администрирование, по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Если у вас нет лицензии, по умолчанию выбирается тип задачи *Установка обновлений Центра обновления Windows*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

- **Установить обновление (добавить правило в указанную задачу)**

Выберите задачу, в которую вы хотите добавить выбранные обновления. Если у вас есть лицензия на Системное администрирование, выберите задачу *Установка требуемых обновлений и закрытие уязвимостей*. Новое правило для установки выбранных обновлений будет автоматически добавлено в выбранную задачу. Если у вас нет лицензии, по умолчанию выбран тип задачи *Установка обновлений Центра обновления Windows*. Выбранные обновления добавлены в свойства задачи.

Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач, в разделе **Активы (Устройства)** → **Задачи**. Если вы выбрали добавление обновлений в существующую задачу, обновления сохраняются в свойствах задачи.

Чтобы установить обновления приложений сторонних производителей, запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Вы можете запустить эти задачи вручную (см. раздел "Запуск задачи вручную" см. стр. [1175](#)) или задать расписание в свойствах задачи, которую вы запускаете. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Установка обновлений приложений сторонних производителей с помощью мастера установки обновлений

Мастер установки обновления доступен при наличии лицензии на Системное администрирование.

► Чтобы создать задачу установки обновлений приложений сторонних производителей с помощью мастера установки обновления:

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

Отобразится список доступных обновлений.

2. Установите флажок рядом с обновлением, которое вы хотите установить.
3. Нажмите на кнопку **Запустить мастер установки обновления**.

Запустится мастер установки обновления. На странице **Выбор задачи установки обновления** отображается список всех существующих задач следующих типов:

- *Установка требуемых обновлений и закрытие уязвимостей*
- *Установка обновлений Центра обновления Windows*
- *Закрытие уязвимостей*

Вы не можете изменить задачи двух последних типов для установки новых обновлений. Для установки новых обновлений можно использовать только задачи *Установка требуемых обновлений и закрытие уязвимостей*.

4. Если вы хотите, чтобы мастер отображал только те задачи, которые устанавливаются выбранным вами обновлением, включите параметр **Показать только задачи, которые устанавливаются обновлением**.
5. Выберите действие, которое хотите выполнить:
 - Чтобы запустить задачу, установите флажок рядом с именем задачи и нажмите на кнопку **Запустить**.
 - Чтобы добавить новое правило в существующую задачу:
 - a. Установите флажок рядом с именем задачи и нажмите на кнопку **Добавить правило**.
 - b. На открывшейся странице настройте новое правило:
 - **Правило установки обновлений данного уровня важности**
 - **Правило установки обновлений данного уровня важности по MSRC**
 - **Правило установки обновлений данного поставщика**
 - **Правило установки обновлений типа**

- **Правило установки выбранного обновления**
- **Одобрить выбранные обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

По умолчанию параметр включен.

- c. Нажмите на кнопку **Добавить**.
- Чтобы создать задачу:
 - a. Нажмите на кнопку **Новая задача**.
 - b. На открывшейся странице настройте новое правило:
 - **Правило установки обновлений данного уровня важности**
 - **Правило установки обновлений данного уровня важности по MSRC**
 - **Правило установки обновлений данного поставщика**
 - **Правило установки обновлений типа**
 - **Правило установки выбранного обновления**
 - **Одобрить выбранные обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий

приложения, обновление приложения завершается с ошибкой.

Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

По умолчанию параметр включен.

с. Нажмите на кнопку **Добавить**.

Если вы решили запустить задачу, вы можете закрыть мастер. Задача выполняется в фоновом режиме. Никаких дальнейших действий не требуется.

Если вы выбрали добавление правила к существующей задаче, откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы решили создать задачу, создайте ее с помощью (см. раздел "Создание задачи Установка требуемых обновлений и закрытие уязвимостей" см. стр. [1399](#)) мастера создания задачи. Новое правило, добавленное вами в мастере установки обновлений, отображается в мастере создания задачи. После завершения работы мастера, задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

См. также:

Сценарий: обновление приложений сторонних производителей[499](#)

Создание задачи Поиск уязвимостей и требуемых обновлений

С помощью задачи Поиск уязвимостей и требуемых обновлений Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, установленных на управляемых устройствах.

Задача Поиск уязвимостей и требуемых обновлений создается автоматически во время работы мастера первоначальной настройки (см. раздел "Мастер первоначальной настройки (Kaspersky Security Center Web Console)" см. стр. [1047](#)). Если вы не запускали мастер первоначальной настройки, вы можете создать задачу вручную.

► Чтобы создать задачу Поиск уязвимостей и требуемых обновлений:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите тип задачи **Поиск уязвимостей и требуемых обновлений**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?:\|).
5. Выберите устройства, которым будет назначена задача.

6. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
7. Нажмите на кнопку **Создать**.
Задача будет создана и отобразится в списке задач.
8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
9. В окне свойств задачи укажите общие параметры задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)).
10. На вкладке **Параметры приложения** укажите следующие параметры:

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Соединяться с сервером обновлений для актуализации данных**

Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

- Сервер администрирования Kaspersky Security Center (см. параметры политики Агента администрирования).
- Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
- Серверы обновления Microsoft.

Если этот параметр включен, Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее и которая хранится в кеше устройства.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент Центра обновления Windows на управляемом устройстве подключается к серверу обновлений Microsoft, чтобы получить обновления, только если включен параметр **Соединиться с сервером обновлений для актуализации данных** и параметр **Активный** в группе параметров **Режим поиска Центра обновления Windows**.
- Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, полученную ранее от источника обновлений Microsoft и сохраненную в кеше устройства, если включен параметр **Соединиться с сервером обновлений для актуализации данных** и параметр **Пассивный** в группе параметров **Режим поиска Центра обновления Windows**, или если параметр **Соединиться с сервером обновлений для актуализации данных** выключен, а в группе параметров **Режим поиска Центра обновления Windows** выбран параметр **Активный**.
- Независимо от параметра **Соединиться с сервером обновлений для актуализации данных** (включен он или выключен), если в группе параметров **Выключен** выбран параметр **Режим поиска Центра обновления Windows**, Kaspersky Security Center не запрашивает информацию об обновлениях.
- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Укажите пути для дополнительного поиска приложений в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

11. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Сценарий: обновление приложений сторонних производителей[499](#)

Параметры задачи поиска уязвимостей и требуемых обновлений.

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически во время работы мастера первоначальной настройки. Если вы не запускали мастер первоначальной настройки, вы можете создать задачу вручную.

Помимо общих параметров задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)), вы можете указать следующие параметры при создании задачи *Поиск уязвимостей и требуемых обновлений* или позже, при настройке свойств созданной задачи:

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Соединяться с сервером обновлений для актуализации данных**

Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

- Сервер администрирования Kaspersky Security Center (см. параметры политики Агента администрирования).
- Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
- Серверы обновления Microsoft.

Если этот параметр включен, Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее и которая хранится в кеше устройства.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент Центра обновления Windows на управляемом устройстве подключается к серверу обновлений Microsoft, чтобы получить обновления, только если включен параметр **Соединиться с сервером обновлений для актуализации данных** и параметр **Активный** в группе параметров **Режим поиска Центра обновления Windows**.
 - Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, полученную ранее от источника обновлений Microsoft и сохраненную в кеше устройства, если включен параметр **Соединиться с сервером обновлений для актуализации данных** и параметр **Пассивный** в группе параметров **Режим поиска Центра обновления Windows**, или если параметр **Соединиться с сервером обновлений для актуализации данных** выключен, а в группе параметров **Режим поиска Центра обновления Windows** выбран параметр **Активный**.
 - Независимо от параметра **Соединиться с сервером обновлений для актуализации данных** (включен он или выключен), если в группе параметров **Выключен** выбран параметр **Режим поиска Центра обновления Windows**, Kaspersky Security Center не запрашивает информацию об обновлениях.
- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если

имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Укажите пути для дополнительного поиска приложений в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Рекомендации по настройке расписания запуска задачи

При планировании расписания запуска задачи *Поиск уязвимостей и требуемых обновлений* убедитесь, что включены два параметра **Запускать пропущенные задачи** и **Использовать автоматическое определение случайного интервала между запусками задачи**.

По умолчанию задача *Поиск уязвимостей и требуемых обновлений* запускается в 18:00:00 вручную. Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (утром следующего дня). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

См. также:

Сценарий: настройка защиты сети.....	403
Сценарий: обновление приложений сторонних производителей	499

Создание задачи Установка требуемых обновлений и закрытие уязвимостей

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, в том числе в приложениях Microsoft, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами.

Чтобы установить обновления или исправить уязвимости с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете выполнить одно из следующих действий:

- Запустите мастер установки обновлений (см. раздел "Установка обновлений приложений сторонних производителей" см. стр. [1389](#)) или мастер закрытия уязвимостей (см. раздел "Закрытие уязвимостей в приложениях сторонних производителей" на стр. [1421](#)).
- Создайте задачу *Установка требуемых обновлений и закрытие уязвимостей*.
- Добавьте правило для установки обновления (см. раздел "Добавление правил для установки обновлений" см. стр. [1403](#)) в существующую задачу *Установка требуемых обновлений и закрытие уязвимостей*.

► Чтобы создать задачу *Установка требуемых обновлений и закрытие уязвимостей*:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.

Если задача не отображается, проверьте, есть ли у вашей учетной записи права (см. раздел "Права доступа к функциям приложения" на стр. [1276](#)) **Чтение, Изменение и Выполнение** в функциональной области **Управление системой: Системное администрирование**. Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.

4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*>?\\:|).
5. Выберите устройства, которым будет назначена задача.

6. Укажите правила для установки обновления (см. раздел "Добавление правил для установки обновлений" см. стр. [1403](#)), а затем следующие параметры:

- **Начинать установку в момент перезагрузки или выключения устройства**

Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

По умолчанию параметр выключен.

- **Устанавливать требуемые общесистемные компоненты**

Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (прerequisites), необходимые для установки этого обновления. Например, такими prerequisites могут являться обновления операционной системы.

Если этот параметр выключен, необходимо установить prerequisites вручную.

По умолчанию параметр выключен.

- **Разрешать установку новой версии приложения при обновлении**

Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии приложения.

Если этот параметр выключен, приложение не обновляется. Можно позднее установить новые версии приложений вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию приложения или если требуется проверить обновление в тестовой инфраструктуре.

По умолчанию параметр включен.

После установки новой версии приложения может быть нарушена работа других приложений, установленных на клиентских устройствах и зависящих от работы обновляемой приложения.

- **Загружать обновления на устройство, не устанавливая их**

Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Загрузить обновления для**.

Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

По умолчанию параметр выключен.

- **Загрузить обновления для**

Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

7. Укажите параметры перезагрузки операционной системы:

- **Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами).

Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать

наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Время ожидания перед принудительным закрытием приложения в заблокированных сессиях через (мин)**

Принудительное завершение работы приложений, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

Если флажок установлен, работа приложений на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

Если флажок снят, работа приложений на заблокированном устройстве не прекращается.

По умолчанию флажок снят.

8. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
9. Нажмите на кнопку **Готово**.
Задача будет создана и отобразится в списке задач.
10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
11. В окне свойств задачи укажите общие параметры задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)) в соответствии с вашими требованиями.
12. Нажмите на кнопку **Сохранить**.
Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

См. также:

Сценарий: обновление приложений сторонних производителей	499
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей	529
Установка обновлений приложений сторонних производителей	1383

Добавление правил для установки обновлений

Эта функциональность доступна при наличии лицензии на Системное администрирование.

При установке обновлений программного обеспечения или закрытии уязвимостей в приложениях с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, добавляете ли вы правило для всех обновлений Центра обновления Windows или для обновлений приложений сторонних производителей (то есть приложений производства не "Лаборатории Касперского" и не Microsoft). При добавлении правила для обновления Центра обновления Windows или обновления приложений сторонних производителей вы можете выбрать приложения и версии приложений, для которых вы хотите установить обновления. При добавлении правила для всех обновлений вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые необходимо закрыть с помощью установки обновлений.

Вы можете добавить правило для установки обновлений следующими способами:

- Добавить правило при создании задачи *Установка требуемых обновлений и закрытие уязвимостей* (см. раздел "Создание задачи *Установка требуемых обновлений и закрытие уязвимостей*" см. стр. [1399](#)).
- Добавить правило на вкладке **Параметры приложения** в окне свойств существующей задачи *Установка требуемых обновлений и закрытие уязвимостей*.
- С помощью мастера установки обновлений (см. раздел "Установка обновлений приложений сторонних производителей" см. стр. [1389](#)) или мастера закрытия уязвимостей (см. раздел "Закрытие уязвимостей в приложениях сторонних производителей" на стр. [1421](#)).

► Чтобы добавить правило для всех обновлений:

1. Нажмите на кнопку **Добавить**.

Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для всех обновлений**.

3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:

- Набор обновлений для установки

Выберите обновления, которые должны быть установлены на клиентские

устройства:

- **Устанавливать только утвержденные обновления.** В этом случае устанавливаются только одобренные обновления.
- **Устанавливать все обновления, кроме отклоненных.** В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
- **Устанавливать все обновления, включая отклоненные.** В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осммотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

4. В окне **Обновления** выберите обновления для установки:

- **Устанавливать все подходящие обновления**

В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

- **Устанавливать только обновления из списка**

В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные приложения или чтобы обновить только требуемые приложения.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх

версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

По умолчанию параметр включен.

5. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

- **Закрывать все уязвимости, соответствующие остальным критериям**

В этом случае будут закрыты все уязвимости программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

- **Закрыть только уязвимости из списка**

Закрывать только уязвимости, которые выбраны вручную в списке. Этот список содержит все обнаруженные уязвимости.

Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных приложениях или чтобы закрыть уязвимости только в требуемых приложениях.

6. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

► Чтобы добавить правило для обновлений Центра обновления Windows:

1. Нажмите на кнопку **Добавить**.

Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для обновлений Windows Update**.

3. В окне **Общие условия** настройте следующие параметры:

- **Набор обновлений для установки**

Выберите обновления, которые должны быть установлены на клиентские устройства:

- **Устанавливать только утвержденные обновления.** В этом случае устанавливаются только одобренные обновления.
- **Устанавливать все обновления, кроме отклоненных.** В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
- **Устанавливать все обновления, включая отклоненные.** В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.
5. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.
6. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

► Чтобы добавить правило для обновления приложений сторонних производителей:

1. Нажмите на кнопку **Добавить**.

Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для сторонних обновлений**.
3. В окне **Общие условия** настройте следующие параметры:

- **Набор обновлений для установки**

Выберите обновления, которые должны быть установлены на клиентские устройства:

- **Устанавливать только утвержденные обновления.** В этом случае устанавливаются только одобренные обновления.
- **Устанавливать все обновления, кроме отклоненных.** В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
- **Устанавливать все обновления, включая отклоненные.** В этом случае

устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмоторительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.
5. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе Параметры, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

См. также:

Сценарий: обновление приложений сторонних производителей	499
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....	529

Создание задачи Установка обновлений Центра обновления Windows

Задача *Установка обновлений Центра обновления Windows* позволяет устанавливать обновления программного обеспечения, предоставляемые службой Центра обновления Windows, на управляемые устройства.

Если у вас нет лицензии на Системное администрирование, вы не можете создавать задачи с типом *Установка обновлений Центра обновления Windows*. Чтобы установить новые обновления, вы можете добавить их в существующую задачу *Установка обновлений Центра обновления Windows*. Рекомендуется использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. раздел "Создание задачи Установка требуемых обновлений и закрытие уязвимостей" см. стр. [1399](#)) вместо задачи *Установка обновлений Центра обновления Windows*. Задача *Установка требуемых обновлений и закрытие уязвимостей* позволяет автоматически устанавливать несколько обновлений и закрывать несколько уязвимостей в соответствии с заданными правилами (см. раздел "Добавление правил для установки обновлений" см. стр. [1403](#)). Также эта задача позволяет устанавливать обновления для приложений сторонних производителей, то есть приложений производства не Microsoft.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

► Чтобы создать задачу Установка обновлений Центра обновления Windows:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center выберите тип задачи **Установка обновлений Центра обновления Windows**.
4. Укажите имя задачи, которую вы создаете.
Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\":|).
Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\":|).
5. Выберите устройства, которым будет назначена задача.
6. Нажмите на кнопку **Добавить**.
Откроется список обновлений.
7. Выберите обновления Центра обновлений Windows, которые вы хотите установить и нажмите на кнопку **ОК**.
8. Укажите параметры перезагрузки операционной системы:
 - **Не перезагружать устройство**
Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами).
Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.
 - **Перезагрузить устройство**
В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).
 - **Запрашивать у пользователя**
На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

9. Задайте параметры учетной записи:

- **Учетная запись по умолчанию**

Задача будет запускаться под той же учетной записью, под которой была установлено и запущено приложение, выполняющее эту задачу.

По умолчанию выбран этот вариант.

- **Задать учетную запись**

Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

- **Учетная запись**

Учетная запись, от имени которой будет запускаться задача.

- **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

10. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными

по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

11. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

13. В окне свойств задачи укажите общие параметры задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)) в соответствии с вашими требованиями.

14. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Просмотр информации о доступных обновлениях приложений сторонних производителей.

Вы можете просмотреть список доступных обновлений для приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на клиентских устройствах.

- *Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на клиентских устройствах,*

в главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

Отобразится список доступных обновлений.

Вы можете указать фильтр для просмотра списка обновлений приложений. Нажмите на значок **Фильтр** () в верхнем правом углу списка обновлений приложений для управления фильтром. Вы также можете выбрать один из предустановленных фильтров в раскрывающемся списке **Предустановленные фильтры** над списком уязвимостей в приложениях.

- *Чтобы просмотреть свойства обновления:*

1. Нажмите на имя требуемого обновления программного обеспечения.
2. Откроется окно свойств обновления, в котором отображается следующая информация, сгруппированная по вкладкам:
 - **Общие**
 - **Атрибуты**
 - **Устройства**
 - **Закрываемые уязвимости**
 - **Пересечения обновлений**
 - **Задачи для установки обновления**

- *Чтобы просмотреть статистику установки обновления:*

1. Установите флажок рядом с требуемым обновлением.
2. Нажмите на кнопку **Статистика состояния установки обновлений**.

На диаграмме отобразится информация о статусах обновлений. Нажав на статус, откроется список устройств, на которых обновление имеет выбранный статус.

Вы можете просмотреть информацию о доступных обновлениях для приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на выбранном управляемом устройстве под управлением Windows.

► *Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на выбранном управляемом устройстве:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Управляемые устройства**.
Отобразится список управляемых устройств.
2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обновления приложений сторонних производителей.
Откроется окно свойств выбранного устройства.
3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.
4. На левой панели выберите раздел **Применимые обновления**. Если вы хотите просматривать только установленные обновления, включите параметр **Показывать установленные обновления**.

Отобразится список доступных обновлений приложений сторонних производителей для выбранного устройства.

См. также:

Сценарий: обновление приложений сторонних производителей[499](#)

Экспорт списка доступных обновлений в файл

Вы можете экспортировать отображаемый список обновлений для приложений сторонних производителей, включая программное обеспечение Microsoft, в файл формата CSV или TXT. Вы можете использовать эти файлы, например, чтобы отправить их вашему начальнику по информационной безопасности или сохранить их в целях статистики.

► *Чтобы экспортировать список доступных обновлений для приложений сторонних производителей в текстовый файл, установленных на всех управляемых устройствах:*

1. В главном окне приложения перейдите в раздел **Операции → Управление патчами → Обновления программного обеспечения**.
На странице отображается список доступных обновлений для приложений сторонних производителей, установленных на всех управляемых устройствах.
2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список доступных обновлений для приложений сторонних производителей, включая программное обеспечение Microsoft, загружается на устройство, которое вы используете в данный момент.

► Чтобы экспортировать список доступных обновлений для приложений сторонних производителей в текстовый файл, установленных на выбранном управляемом устройстве:

1. Откройте список доступных обновлений приложений сторонних производителей на выбранном управляемом устройстве (см. раздел "Просмотр информации о доступных обновлениях приложений сторонних производителей." см. стр. [1410](#)).

2. Выберите обновления программного обеспечения, которые вы хотите экспортировать.

Пропустите этот шаг, если вы хотите экспортировать полный список обновлений приложений.

При экспорте полного списка обновлений приложений, будут экспортированы только те обновления, которые отображаются на текущей странице.

Если вы хотите экспортировать только установленные обновления, установите флажок **Показывать установленные обновления**.

3. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список обновления приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на выбранных управляемых устройствах, загружается на устройство, которое вы используете в данный момент.

См. также:

Сценарий: обновление приложений сторонних производителей[499](#)

Одобрение и отклонение обновлений приложений сторонних производителей.

При настройке задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете создать правило, для выполнения которого устанавливаемые обновления должны иметь определенный статус. Например, правило обновления может разрешить установку следующего:

- только одобренных обновлений;
- только одобренных обновлений и неопределенных обновлений;
- всех обновлений, независимо от статусов обновлений.

Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

При управлении установкой обновлений использовать статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. При ручном одобрении большого количества обновлений производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

► Чтобы подтвердить или отменить одно или несколько обновлений:

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

Отобразится список доступных обновлений.

2. Выберите обновления, которые требуется подтвердить или отклонить.
3. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или **Отклонить**, чтобы отклонить выбранное обновление.

По умолчанию установлено значение *Не определено*.

Выбранные обновления имеют статусы, которые вы указали.

Также вы можете изменить статус в свойствах требуемого обновления.

► *Чтобы одобрить или отклонить обновление:*

1. В главном окне программы перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

Отобразится список доступных обновлений.

2. Выберите обновление, которое требуется одобрить или отклонить.

Откроется окно свойств обновления.

3. В разделе **Общие** выберите статус обновления, изменив параметр **Статус одобрения обновления**. Вы можете выбрать статус *Одобрено*, *Отклонено* или *Не определено*.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Выбранное обновление имеет статус, который вы указали.

Если вы устанавливаете статус **Отклонено** для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить их, вы можете сделать это вручную локально.

См. также:

Сценарий: обновление приложений сторонних производителей	499
Создание задачи Установка требуемых обновлений и закрытие уязвимостей	1399

Создание задачи Синхронизация обновлений Windows Update.

Задача *Синхронизация обновлений Windows Update* доступна при наличии лицензии на Системное администрирование.

Задача *Синхронизация обновлений Windows Update* требуется, если вы хотите использовать Сервер администрирования в роли WSUS-сервера. В этом случае Сервер администрирования загружает обновления Windows в базу данных и предоставляет обновления Центра обновления Windows на

клиентских устройствах в централизованном режиме с помощью Агентов администрирования. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

Задача *Синхронизация обновлений Windows Update* загружает с серверов Microsoft только метаданные. Во время выполнения задачи установки обновлений, Kaspersky Security Center загружает только те обновления, которые вы выбрали для установки.

Во время выполнения задачи **Синхронизация обновлений Windows Update**, приложение получает список актуальных обновлений с сервера обновлений Microsoft. После чего Kaspersky Security Center определяет список устаревших обновлений. При следующем запуске задачи **Поиск уязвимостей и требуемых обновлений** Kaspersky Security Center отмечает устаревшие обновления и устанавливает время на удаление. При следующем запуске задачи **Синхронизация обновлений Windows Update** удаляются обновления, которые были отмечены на удаление 30 дней назад. Kaspersky Security Center также выполняет дополнительную проверку для удаления устаревших обновлений, которые были отмечены на удаление более 180 дней назад.

После завершения работы задачи **Синхронизация обновлений Windows Update** и удаления устаревших обновлений в базе данных могут оставаться хеш-коды файлов удаленных обновлений, а также соответствующие им файлы в папке %AllUsersProfile%\Application Data\KasperskyLab\admindkit\1093\working\wusfiles, в случае если они были загружены ранее. С помощью задачи **Обслуживание Сервера администрирования** можно удалить такие устаревшие записи из базы данных и соответствующие им файлы.

► *Чтобы создать задачу Синхронизация обновлений Windows Update:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите тип задачи **Синхронизация обновлений Windows Update**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*>?\":|).
5. Включите параметр **Загрузить файлы экспресс-установки**, если вы хотите, чтобы файлы экспресс-обновления загружались при выполнении задачи.

Когда Kaspersky Security Center синхронизирует обновления с серверами Microsoft Windows Update Servers, информация обо всех файлах сохраняется в базе данных Сервера администрирования. Также на диск загружаются все файлы, необходимые для обновления, при взаимодействии с Агентом обновления Windows. В частности, Kaspersky Security Center сохраняет информацию о файлах экспресс-установки в базу данных и загружает их по мере необходимости. Загрузка файлов экспресс-установки приводит к сокращению свободного места на диске.

Чтобы уменьшить сокращение объема дискового пространства и снизить трафик, выключите параметр **Загрузить файлы экспресс-установки**.

6. Выберите приложения, для которых требуется загрузить обновления.
Если установлен флажок **Все приложения**, то обновления будут загружаться для всех имеющихся приложений, а также для тех приложений, которые могут быть выпущены в будущем.
7. Выберите категории обновлений, которые вы хотите загрузить на Сервер администрирования.

Если установлен флажок **Все категории**, то обновления будут загружаться для всех имеющихся категорий обновлений, а также для тех категорий, которые могут появиться в будущем.

8. Выберите языки локализации обновлений, которые вы хотите загрузить на Сервер администрирования. Выберите один из следующих вариантов:

- **Загружать все языки, включая новые**

Если выбран этот вариант, на Сервер администрирования будут загружаться все доступные языки локализации обновлений. По умолчанию выбран этот вариант.

- **Загружать выбранные языки**

Если выбран этот вариант, в списке можно выбрать языки локализации обновлений, которые должны загружаться на Сервер администрирования.

9. Укажите, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **Учетная запись по умолчанию**

Задача будет запускаться под той же учетной записью, под которой была установлено и запущено приложение, выполняющее эту задачу.

По умолчанию выбран этот вариант.

- **Задать учетную запись**

Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

10. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

11. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

13. В окне свойств задачи укажите общие параметры задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)) в соответствии с вашими требованиями.

14. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Сценарий: обновление приложений сторонних производителей[499](#)

Автоматическое обновление приложений сторонних производителей

Некоторые приложения сторонних производителей могут обновляться автоматически. Поставщик приложения определяет, поддерживает ли приложение функцию автоматического обновления. Если приложение стороннего производителя, установленное на управляемом устройстве, поддерживает

автоматическое обновление, вы можете указать параметр автоматического обновления в свойствах приложения. После изменения параметра автоматического обновления Агенты администрирования применяют новый параметр на каждом управляемом устройстве, на котором установлено приложение.

Параметр автоматического обновления не зависит от других объектов и возможностей Системного администрирования. Например, этот параметр не зависит от статуса одобрения обновления или задач установки обновления, таких как *Установка требуемых обновлений и закрытие уязвимостей*, *Установка обновлений Центра обновления Windows* и *Закрытие уязвимостей*.

► *Чтобы настроить параметр автоматического обновления для приложения стороннего производителя:*

1. В главном окне программы перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений**.
2. Нажмите на имя приложения, для которого вы хотите изменить параметр автоматического обновления.

Чтобы упростить поиск, вы можете отфильтровать список по столбцу **Статус автоматических обновлений**.

Откроется окно свойств приложения.

3. В разделе **Общие** выберите значение для следующего параметра:

Статус автоматических обновлений

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка автоматического обновления применяется к выбранному приложению.

См. также:

Сценарий: обновление приложений сторонних производителей[499](#)

Закрытие уязвимостей в приложениях сторонних производителей

В этом разделе описаны возможности Kaspersky Security Center связанные с закрытием уязвимостей в приложениях, установленных на управляемых устройствах.

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей

В этом разделе представлен сценарий обнаружения и закрытия уязвимостей на управляемых устройствах под управлением Windows. Вы можете найти и закрыть уязвимости в приложениях в операционных системах и в приложениях сторонних производителей, включая программное обеспечение Microsoft (см. раздел "О приложениях сторонних производителей" на стр. [1379](#)).

Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- В сети вашей организации есть управляемые устройства под управлением Windows.

- Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:
 - Составление списка рекомендуемых исправлений уязвимостей в приложениях Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
 - Заккрытие уязвимостей в приложениях сторонних производителей, отличных от приложений Microsoft.

Этапы

Обнаружение и закрытие уязвимостей состоит из следующих этапов:

a. Поиск уязвимостей в программном обеспечении, установленном на управляемых устройствах

Чтобы найти уязвимости в приложениях, установленных на управляемых устройствах, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, запустите его сейчас или создайте задачу вручную.

Инструкции:

- Консоль администрирования: Поиск уязвимостей в приложениях, Задание расписания для задачи поиска уязвимостей и требуемых обновлений.
- Kaspersky Security Center Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений (на стр. [1393](#)), Параметры задачи поиска уязвимостей и требуемых обновлений (см. раздел "Параметры задачи поиска уязвимостей и требуемых обновлений." см. стр. [1396](#)).

b. Анализ списка обнаруженных уязвимостей в приложениях

Просмотрите список **Уязвимости в приложениях** и решите, какие уязвимости требуется закрыть. Чтобы просмотреть подробную информацию о каждой уязвимости, нажмите на имя уязвимости в списке. Для каждой уязвимости в списке вы также можете просмотреть статистику уязвимости на управляемых устройствах.

Инструкции:

- Консоль администрирования: Просмотр информации об уязвимостях в приложениях, Просмотр статистики уязвимостей на управляемых устройствах.
- Kaspersky Security Center Web Console: Просмотр информации об уязвимостях в приложениях (см. раздел "Просмотр информации об уязвимостях в приложениях, обнаруженных на всех управляемых устройствах" на стр. [1436](#)), Просмотр статистики уязвимостей на управляемых устройствах (см. раздел "Просмотр статистики уязвимостей на управляемых устройствах." на стр. [1438](#)).

c. Настройка закрытия уязвимостей

Обнаружив уязвимости в приложениях, вы можете закрыть уязвимости в приложениях на управляемых устройствах, используя задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. раздел "Создание задачи Установка требуемых обновлений и закрытие уязвимостей" см. стр. [1399](#)) или задачу *Заккрытие уязвимостей* (см. раздел "Создание задачи Заккрытие уязвимостей" см. стр. [1424](#)).

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, в том числе в приложениях Microsoft, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование. Чтобы устранить уязвимости в приложениях, задача *Установка требуемых обновлений и закрытие уязвимостей* использует рекомендованные обновления приложений.

Задача *Закрытие уязвимостей* не требует лицензии для Системного администрирования. Чтобы использовать эту задачу, требуется вручную указать пользовательские исправления для закрытия уязвимостей в приложениях сторонних производителей, которые указаны в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для приложений сторонних производителей.

Вы можете запустить мастер закрытия уязвимостей, который автоматически создаст одну из этих задач, или вы можете создать одну из этих задач вручную.

Инструкции:

- Консоль администрирования: Пользовательские исправления для уязвимостей в приложениях сторонних производителей, Закрытие уязвимостей в приложениях.
- Kaspersky Security Center Web Console: Пользовательские исправления для уязвимостей в приложениях сторонних производителей (на стр. [1435](#)), Закрытие уязвимостей в приложениях сторонних производителей (на стр. [1421](#)), Создание задачи Установка требуемых обновлений и закрытие уязвимостей (см. стр. [1399](#)).

d. Задание расписания задачи

Чтобы убедиться, что список уязвимостей всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. Рекомендуемый средний период – один раз в неделю.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. При задании расписания задачи *Закрытие уязвимостей*, вам нужно выбрать исправления приложений Microsoft или указать пользовательские исправления для приложений сторонних производителей каждый раз перед запуском задачи.

При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

e. Игнорирование уязвимостей в приложениях (если требуется)

Вы можете игнорировать уязвимости в приложениях, которые должны быть закрыты на всех управляемых устройствах или только на выбранных управляемых устройствах.

Инструкции:

- Консоль администрирования: Игнорирование уязвимостей в приложениях.
- Kaspersky Security Center Web Console: Игнорирование уязвимостей в приложениях (на стр. [1439](#)).

f. Запуск задачи закрытия уязвимости

Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или *Закрытие уязвимостей*. Когда задача будет завершена, убедитесь, что в списке задач она имеет статус *Завершена успешно*.

g. Создание отчета о результатах закрытия уязвимостей в приложениях (если требуется)

Чтобы просмотреть статистику о закрытых уязвимостях, сформируйте отчет об уязвимостях. В отчете отображается информация об уязвимостях в приложениях, которые не закрыты. Таким образом, вы можете иметь представление об обнаружении и закрытии уязвимостей в приложениях сторонних производителей в вашей организации, включая программное обеспечение Microsoft.

Инструкции:

- Консоль администрирования: Создание и просмотр отчета.
- Kaspersky Security Center Web Console: Генерация и просмотр отчета (см. стр. [1479](#)).

h. Проверка настройки обнаружения и закрытия уязвимостей в приложениях сторонних производителей

Убедитесь, что вы выполнили следующее:

- обнаружили и просмотрели список уязвимостей в приложениях на управляемых устройствах;
- игнорировали уязвимости в приложениях, если хотели;
- настроили задачу закрытия уязвимости;
- запланировали запуск задач для поиска и закрытия уязвимостей в приложениях так, чтобы они запускались последовательно;
- проверили, что задача закрытия уязвимостей была запущена.

Результаты

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытие уязвимостей*, уязвимости будут автоматически закрыты на управляемых устройствах. При запуске задачи, задача выполняет сопоставление списка доступных обновлений программного обеспечения с правилами, указанными в параметрах задачи. Все обновления программного обеспечения, которые соответствуют критериям в правилах, будут загружены в хранилище Сервера администрирования и будут установлены для закрытия уязвимостей в приложениях.

Если вы создали задачу *Закрытие уязвимостей*, закрываются только уязвимости в приложениях Microsoft.

См. также:

О приложениях сторонних производителей.....[1379](#)

Об обнаружении и закрытии уязвимостей в приложениях

Kaspersky Security Center обнаруживает и закрывает уязвимости в приложениях на управляемых устройствах под управлением операционных систем семейства Microsoft Windows. Уязвимости обнаружены в операционных системах и в приложениях сторонних производителей, включая программное обеспечение Microsoft (см. раздел "О приложениях сторонних производителей" на стр. [1379](#)).

Обнаружение уязвимостей в приложениях

Для обнаружения уязвимостей Kaspersky Security Center выполняет поиск известных уязвимостей программного обеспечения на основе признаков из баз данных об известных уязвимостях. Эта база формируются специалистами "Лаборатории Касперского". Она содержит информацию об уязвимостях, такую как описание уязвимостей, дата обнаружения уязвимостей, уровень критичности уязвимостей. Вы можете получить сведения об уязвимостях в программах на сайте "Лаборатории Касперского" (<https://threats.kaspersky.com/ru/>).

В Kaspersky Security Center для поиска уязвимостей приложений используется задача *Поиск уязвимостей и требуемых обновлений*.

Заккрытие уязвимостей в приложениях

Для закрытия уязвимостей в приложениях, Kaspersky Security Center использует обновления программного обеспечения выпущенные поставщиками программного обеспечения. Метаданные обновлений программного обеспечения загружаются в хранилище Сервера администрирования в результате выполнения следующих задач:

- *Загрузка обновлений в хранилище Сервера администрирования*. Эта задача предназначена для загрузки метаданных обновлений для приложений "Лаборатории Касперского" и приложений сторонних производителей. Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Задача загрузки обновлений в хранилище Сервера администрирования может быть создана вручную (см. раздел "Создание задачи Загрузка обновлений в хранилище Сервера администрирования" см. стр. [1347](#)).
- *Синхронизация обновлений Windows Update*. Эта задача предназначена для загрузки метаданных обновлений программного обеспечения Microsoft.

Обновления программного обеспечения для закрытия уязвимостей могут быть представлены в виде полных дистрибутивов или патчей. Обновления программного обеспечения, которые закрывают уязвимости в приложениях, называются *исправлениями*. *Рекомендуемые исправления* это исправления, которые рекомендуются к установке специалистами "Лаборатории Касперского". *Пользовательские исправления* это исправления, которые вручную указываются для установки пользователями. Чтобы установить пользовательское исправление, необходимо создать инсталляционный пакет, содержащий это исправление.

Если лицензия Kaspersky Security Center предусматривает возможности Системного администрирования, для закрытия уязвимостей используйте задачу *Установка требуемых обновлений и закрытие уязвимостей*. Эта задача автоматически закрывает несколько уязвимостей, устанавливая рекомендуемые исправления. Для этой задачи вы можете вручную настроить определенные правила для закрытия нескольких уязвимостей.

Если лицензия Kaspersky Security Center не предусматривает возможности Системного администрирования, для закрытия уязвимостей используйте задачу *Заккрытие уязвимостей*. С помощью этой задачи можно закрыть уязвимости, установив рекомендуемые исправления для приложений Microsoft и пользовательских исправлений для приложений сторонних производителей.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Специалисты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также специалисты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Для закрытия некоторых уязвимостей в приложениях вам нужно принять Лицензионное соглашение для установки приложений, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в приложении не закрывается.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Закрытие уязвимостей в приложениях сторонних производителей

После получения списка уязвимостей в приложениях вы можете закрыть уязвимости в приложениях на управляемых устройствах с операционными системами Windows. Вы можете закрыть уязвимости в операционной системе и приложениях сторонних производителей, включая программное обеспечение Microsoft, создав и запустив задачу *Закрытие уязвимостей* (см. раздел "*Создание задачи Закрытие уязвимостей*" см. стр. [1424](#)) или задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. раздел "*Создание задачи Установка требуемых обновлений и закрытие уязвимостей*" см. стр. [1399](#)).

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Также вы можете создать задачу для закрытия уязвимостей в приложениях следующими способами:

- Откройте список уязвимостей и укажите, какие уязвимости необходимо закрыть.
В результате создается задача закрытия уязвимостей в приложениях. Также можно добавить выбранные уязвимости в существующую задачу.
- Запустите мастер закрытия уязвимостей.

Мастер закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

Мастер упрощает создание и настройку задачи закрытия уязвимостей, а также исключает создание избыточных задач, содержащих те же обновления для установки.

Закрытие уязвимостей в приложениях с помощью списка уязвимостей

► Чтобы закрыть уязвимости в приложениях:

- Откройте один из списков уязвимостей:
 - Чтобы открыть общий список уязвимостей, в главном меню перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

- Чтобы открыть список уязвимостей управляемого устройства, в главном меню перейдите в раздел **Активы (Устройства)** → **Управляемые устройства** → <имя устройства> → **Дополнительно** → **Уязвимости в приложениях**.
- Чтобы открыть список уязвимостей для требуемой программы, в главном меню перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений** → <имя программы> → **Уязвимости**.

Отобразится страница со списком уязвимостей в приложениях сторонних производителей.

2. Выберите одну или несколько уязвимостей в списке и нажмите на кнопку **Закрыть уязвимость**.

Если рекомендуемое обновление программного обеспечения для закрытия одной из выбранных уязвимостей отсутствует, отображается информационное сообщение.

Для закрытия некоторых уязвимостей в приложениях вам нужно принять Лицензионное соглашение для установки приложений, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в приложении не закроется.

3. Выберите один из следующих вариантов:

- **Новая задача**

Запустится мастер создания задачи (см. раздел "Создание задачи" на стр. [1174](#)). Если у вас есть лицензия на Системное администрирование, по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Если у вас нет лицензии, по умолчанию выбирается тип задачи *Закрытие уязвимостей*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

- **Закрыть уязвимость (добавить правило в указанную задачу)**

Выберите задачу, в которую вы хотите добавить выбранные уязвимости. Если у вас есть лицензия на Системное администрирование, выберите задачу *Установка требуемых обновлений и закрытие уязвимостей*. В выбранную задачу будет автоматически добавлено новое правило для закрытия выбранных уязвимостей. Если у вас нет лицензии, по умолчанию выбран тип задачи *Закрытие уязвимостей*. Выбранные уязвимости будут добавлены в свойства задачи.

Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач, в разделе **Активы (Устройства)** → **Задачи**. Если вы выбрали добавление уязвимостей в существующую задачу, уязвимости сохраняются в свойствах задачи.

Чтобы закрыть уязвимости в приложениях сторонних производителей, запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей*. Если вы создали задачу *Закрытие уязвимостей*, вам нужно вручную указать обновления программного обеспечения для закрытия уязвимостей, перечисленных в свойствах задачи.

Закрытие уязвимостей в приложениях с помощью мастера закрытия уязвимостей

Мастер закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

► Чтобы закрыть уязвимости в приложениях с помощью мастера закрытия уязвимостей:

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

Откроется страница со списком уязвимостей в приложениях сторонних производителей, установленных на управляемых устройствах.

2. Установите флажок напротив уязвимости, которую требуется закрыть.
3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

Откроется мастер закрытия уязвимости. На странице **Выбор задачи закрытия уязвимости** отображается список всех существующих задач следующих типов:

- *Установка требуемых обновлений и закрытие уязвимостей*
- *Установка обновлений Центра обновления Windows*
- *Закрытие уязвимостей*

Вы не можете изменить последние два типа задач для установки новых обновлений. Для установки новых обновлений можно использовать только задачу *Установка требуемых обновлений и закрытие уязвимостей*.

4. Если вы хотите, чтобы мастер отображал только те задачи, которые закрывают выбранную уязвимость, включите параметр **Показывать только задачи, которые закрывают выбранную уязвимость**.
5. Выберите действие, которое хотите выполнить:
 - Чтобы запустить задачу, установите флажок рядом с именем задачи и нажмите на кнопку **Запустить**.
 - Чтобы добавить новое правило в существующую задачу:
 - a. Установите флажок рядом с именем задачи и нажмите на кнопку **Добавить правило**.
 - b. На открывшейся странице настройте новое правило:
 - **Правило закрытия уязвимостей данного уровня критичности**
 - **Правило для закрытия уязвимостей с помощью обновлений того же типа, что и обновление, определенное в соответствии с рекомендациями для выбранной уязвимости** (доступно только для уязвимостей в приложениях Microsoft)
 - **Правило закрытия уязвимостей в приложениях выбранного поставщика** (доступно только для уязвимостей в приложениях сторонних производителей)
 - **Правило закрытия уязвимости во всех версиях выбранного приложения** (доступно только для уязвимостей в приложениях сторонних производителей)
 - **Правило закрытия выбранной уязвимости**
 - **Одобрить обновления, закрывающие выбранную уязвимость**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

- c. Нажмите на кнопку **Добавить**.
- Чтобы создать задачу:
 - d. Нажмите на кнопку **Новая задача**.
 - e. На открывшейся странице настройте новое правило:
 - **Правило закрытия уязвимостей данного уровня критичности**

- **Правило для закрытия уязвимостей с помощью обновлений того же типа, что и обновление, определенное в соответствии с рекомендациями для выбранной уязвимости** (доступно только для уязвимостей в приложениях Microsoft)
- **Правило закрытия уязвимостей в приложениях выбранного поставщика** (доступно только для уязвимостей в приложениях сторонних производителей)
- **Правило закрытия уязвимости во всех версиях выбранного приложения** (доступно только для уязвимостей в приложениях сторонних производителей)
- **Правило закрытия выбранной уязвимости**
- **Одобрить обновления, закрывающие выбранную уязвимость**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

f. Нажмите на кнопку **Добавить**.

Если вы решили запустить задачу, вы можете закрыть мастер. Задача выполняется в фоновом режиме. Никаких дальнейших действий не требуется.

Если вы выбрали добавление правила к существующей задаче, откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы решили создать задачу, создайте ее с помощью (см. раздел "Создание задачи Установка требуемых обновлений и закрытие уязвимостей" см. стр. [1399](#)) мастера создания задачи. Новое правило, добавленное вами в мастер закрытия уязвимостей, отображается в мастере создания задачи. После завершения работы мастера, задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Создание задачи **Закрытие уязвимостей**

Задача *Закрытие уязвимостей* позволяет закрыть уязвимости в приложениях на управляемых устройствах с операционными системами Windows. Вы можете закрыть уязвимости в приложениях сторонних производителей, включая приложения Microsoft.

Если у вас нет лицензии на Системное администрирование, вы не можете создавать задачи с типом *Закрытие уязвимостей*. Чтобы закрыть новые уязвимости, вы можете добавить их в существующую задачу *Закрытие уязвимостей*. Рекомендуется использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. раздел "Создание задачи Установка требуемых обновлений и закрытие уязвимостей" см. стр. [1399](#)) вместо задачи *Закрытие уязвимостей*. Задача *Установка требуемых обновлений и закрытие уязвимостей* позволяет автоматически устанавливать несколько обновлений и закрывать несколько уязвимостей в соответствии с заданными правилами (см. раздел "Добавление правил для установки обновлений" см. стр. [1403](#)).

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

► Чтобы создать задачу **Закрытие уязвимостей**, выполните следующие действия:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center выберите тип задачи **Закрытие уязвимостей**.
4. Укажите имя задачи, которую вы создаете.
Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\":|).
5. Выберите устройства, которым будет назначена задача.
6. Нажмите на кнопку **Добавить**.
Откроется список уязвимостей.
7. Выберите уязвимости, которые вы хотите закрыть и нажмите на кнопку **ОК**.
Для уязвимостей в приложениях Microsoft обычно существуют рекомендуемые исправления. Дополнительные действия для них не требуются. Для уязвимостей в приложениях сторонних производителей сначала необходимо указать исправление пользователя для каждой уязвимости (см. раздел "Пользовательские исправления для уязвимостей в приложениях сторонних производителей" на стр. [1435](#)), которую вы хотите закрыть. После этого вы сможете добавить эти уязвимости в задачу **Закрытие уязвимостей**.
8. Укажите параметры перезагрузки операционной системы:

- **Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами).
Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя,

периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

9. Задайте параметры учетной записи:

- **Учетная запись по умолчанию**

Задача будет запускаться под той же учетной записью, под которой была установлено и запущено приложение, выполняющее эту задачу.

По умолчанию выбран этот вариант.

- **Задать учетную запись**

Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

- **Учетная запись**

Учетная запись, от имени которой будет запускаться задача.

- **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

10. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
11. Нажмите на кнопку **Готово**.
Задача будет создана и отобразится в списке задач.
12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
13. В окне свойств задачи укажите общие параметры задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)) в соответствии с вашими требованиями.
14. Нажмите на кнопку **Сохранить**.
Задача создана и настроена.

Создание задачи Установка требуемых обновлений и закрытие уязвимостей

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, в том числе в приложениях Microsoft, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами.

Чтобы установить обновления или исправить уязвимости с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете выполнить одно из следующих действий:

- Запустите мастер установки обновлений (см. раздел "Установка обновлений приложений сторонних производителей" см. стр. [1389](#)) или мастер закрытия уязвимостей (см. раздел "Закрытие уязвимостей в приложениях сторонних производителей" на стр. [1421](#)).
- Создайте задачу *Установка требуемых обновлений и закрытие уязвимостей*.
- Добавьте правило для установки обновления (см. раздел "Добавление правил для установки обновлений" см. стр. [1403](#)) в существующую задачу *Установка требуемых обновлений и закрытие уязвимостей*.

► Чтобы создать задачу *Установка требуемых обновлений и закрытие уязвимостей*:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.

Если задача не отображается, проверьте, есть ли у вашей учетной записи права (см. раздел "Права доступа к функциям приложения" на стр. [1276](#)) **Чтение, Изменение и Выполнение** в функциональной области **Управление системой: Системное администрирование**. Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.

4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\\:|).
5. Выберите устройства, которым будет назначена задача.
6. Укажите правила для установки обновления (см. раздел "Добавление правил для установки обновлений" см. стр. [1403](#)), а затем следующие параметры:

- **Начинать установку в момент перезагрузки или выключения устройства**

Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

По умолчанию параметр выключен.

- **Устанавливать требуемые общесистемные компоненты**

Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

Если этот параметр выключен, необходимо установить пререквизиты вручную.

По умолчанию параметр выключен.

- **Разрешать установку новой версии приложения при обновлении**

Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии приложения.

Если этот параметр выключен, приложение не обновляется. Можно позднее установить новые версии приложений вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию приложения или если требуется проверить обновление в тестовой инфраструктуре.

По умолчанию параметр включен.

После установки новой версии приложения может быть нарушена работа других приложений, установленных на клиентских устройствах и зависящих от работы обновляемой приложения.

- **Загружать обновления на устройство, не устанавливая их**

Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от

"Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Загрузить обновления для**.

Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

По умолчанию параметр выключен.

- **Загрузить обновления для**

Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

7. Укажите параметры перезагрузки операционной системы:

- **Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами).

Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Время ожидания перед принудительным закрытием приложения в заблокированных сессиях через (мин)**

Принудительное завершение работы приложений, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

Если флажок установлен, работа приложений на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

Если флажок снят, работа приложений на заблокированном устройстве не прекращается.

По умолчанию флажок снят.

8. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
9. Нажмите на кнопку **Готово**.
Задача будет создана и отобразится в списке задач.
10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
11. В окне свойств задачи укажите общие параметры задачи (см. раздел "Общие параметры задач" см. стр. [1176](#)) в соответствии с вашими требованиями.
12. Нажмите на кнопку **Сохранить**.
Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

См. также:

Сценарий: обновление приложений сторонних производителей	499
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей	529
Установка обновлений приложений сторонних производителей	1383

Добавление правил для установки обновлений

Эта функциональность доступна при наличии лицензии на Системное администрирование.

При установке обновлений программного обеспечения или закрытии уязвимостей в приложениях с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, добавляете ли вы правило для всех обновлений Центра обновления Windows или для обновлений приложений сторонних производителей (то есть приложений производства не "Лаборатории Касперского" и не Microsoft). При добавлении правила для обновления Центра обновления Windows или обновления приложений сторонних производителей вы можете выбрать приложения и версии приложений, для которых вы хотите установить обновления. При добавлении правила для всех обновлений вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые необходимо закрыть с помощью установки обновлений.

Вы можете добавить правило для установки обновлений следующими способами:

- Добавить правило при создании задачи *Установка требуемых обновлений и закрытие уязвимостей* (см. раздел "Создание задачи *Установка требуемых обновлений и закрытие уязвимостей*" см. стр. [1399](#)).
- Добавить правило на вкладке **Параметры приложения** в окне свойств существующей задачи *Установка требуемых обновлений и закрытие уязвимостей*.
- С помощью мастера установки обновлений (см. раздел "Установка обновлений приложений сторонних производителей" см. стр. [1389](#)) или мастера закрытия уязвимостей (см. раздел "Закрытие уязвимостей в приложениях сторонних производителей" на стр. [1421](#)).

► Чтобы добавить правило для всех обновлений:

1. Нажмите на кнопку **Добавить**.

Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для всех обновлений**.
3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:

- **Набор обновлений для установки**

Выберите обновления, которые должны быть установлены на клиентские устройства:

- **Устанавливать только утвержденные обновления.** В этом случае устанавливаются только одобренные обновления.
- **Устанавливать все обновления, кроме отклоненных.** В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
- **Устанавливать все обновления, включая отклоненные.** В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

4. В окне **Обновления** выберите обновления для установки:

- **Устанавливать все подходящие обновления**

В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

- **Устанавливать только обновления из списка**

В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные приложения или чтобы обновить только требуемые приложения.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить

приложения, не пытайтесь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

По умолчанию параметр включен.

5. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

- **Закрывать все уязвимости, соответствующие остальным критериям**

В этом случае будут закрыты все уязвимости программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

- **Закрывать только уязвимости из списка**

Закрывать только уязвимости, которые выбраны вручную в списке. Этот список содержит все обнаруженные уязвимости.

Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных приложениях или чтобы закрыть уязвимости только в требуемых приложениях.

6. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

► Чтобы добавить правило для обновлений Центра обновления Windows:

1. Нажмите на кнопку **Добавить**.

Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для обновлений Windows Update**.

3. В окне **Общие условия** настройте следующие параметры:

- **Набор обновлений для установки**

Выберите обновления, которые должны быть установлены на клиентские устройства:

- **Устанавливать только утвержденные обновления.** В этом случае устанавливаются только одобренные обновления.
- **Устанавливать все обновления, кроме отклоненных.** В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
- **Устанавливать все обновления, включая отклоненные.** В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на

тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.
5. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.
6. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

► Чтобы добавить правило для обновления приложений сторонних производителей:

1. Нажмите на кнопку **Добавить**.

Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для сторонних обновлений**.
3. В окне **Общие условия** настройте следующие параметры:

- Набор обновлений для установки

Выберите обновления, которые должны быть установлены на клиентские устройства:

- **Устанавливать только утвержденные обновления.** В этом случае устанавливаются только одобренные обновления.
- **Устанавливать все обновления, кроме отклоненных.** В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
- **Устанавливать все обновления, включая отклоненные.** В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмоторительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.
5. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе Параметры, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

См. также:

Сценарий: обновление приложений сторонних производителей	499
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....	529

Пользовательские исправления для уязвимостей в приложениях сторонних производителей

Чтобы использовать задачу *Закрытие уязвимостей*, необходимо вручную указать обновления программного обеспечения, чтобы закрыть уязвимости в приложениях сторонних производителей, перечисленные в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для других приложений сторонних

производителей. *Пользовательские исправления* это обновления программного обеспечения для закрытия уязвимостей, которые администратор вручную указывает для установки.

► *Чтобы выбрать пользовательские исправления для уязвимостей в приложениях сторонних производителей:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

На странице отображается список уязвимостей в приложениях, обнаруженных на клиентских устройствах.

2. В списке уязвимостей в приложениях перейдите по ссылке с названием уязвимости, для которой вы хотите указать пользовательское исправление.

Откроется окно свойств уязвимости.

3. На левой панели выберите раздел **Пользовательские и другие исправления**.

Отобразится список пользовательских исправлений для выбранной уязвимости в приложениях.

4. Нажмите на кнопку **Добавить**.

Отобразится список доступных инсталляционных пакетов. Список отобразившихся инсталляционных пакетов соответствует списку в папке **Операции** → **Хранилища** → **Инсталляционные пакеты**. Если вы не создали инсталляционный пакет, содержащий пользовательское исправление для закрытия выбранной уязвимости, вы можете создать пакет сейчас, запустив мастер создания инсталляционного пакета.

5. Выберите инсталляционный пакет (или пакеты), содержащий пользовательское исправление (или пользовательские исправления) для уязвимости приложений сторонних производителей.

6. Нажмите на кнопку **Сохранить**.

Указаны инсталляционные пакеты, содержащие пользовательские исправления для уязвимости в приложениях. После запуска задачи *Закрытие уязвимостей* будет установлен инсталляционный пакет и закрыта уязвимость в приложениях.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Просмотр информации об уязвимостях в приложениях, обнаруженных на всех управляемых устройствах

После проверки программного обеспечения на управляемых устройствах на наличие уязвимостей (см. раздел "Создание задачи Поиск уязвимостей и требуемых обновлений" на стр. [1393](#)) вы можете просмотреть список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах. Если вы запустите задачу для иерархии Серверов администрирования, вы можете просмотреть список управляемых устройств с обнаруженными уязвимостями только для выбранного Сервера администрирования.

- Чтобы просмотреть список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах,

в главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

На странице отображается список уязвимостей в приложениях, обнаруженных на клиентских устройствах.

Вы также можете сформировать и просмотреть отчет об уязвимостях (см. раздел "Генерация и просмотр отчета" см. стр. [1479](#)).

Вы можете указать фильтр для просмотра списка уязвимостей в приложениях. Нажмите на значок **Фильтр** () в верхнем правом углу списка уязвимостей в приложениях для управления фильтром. Вы также можете выбрать один из предустановленных фильтров в раскрывающемся списке **Предустановленные фильтры** над списком уязвимостей в приложениях.

Вы можете получить подробную информацию о любой уязвимости из списка.

- Чтобы получить информацию об уязвимости в приложениях,

в списке уязвимостей в приложениях перейдите по ссылке с названием уязвимости.

Откроется окно свойств уязвимости в приложениях.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Просмотр информации об уязвимостях в приложениях, обнаруженных на выбранных управляемых устройствах

Вы можете просмотреть информацию об уязвимостях в приложениях, обнаруженных на выбранном управляемом устройстве под управлением Windows.

- Чтобы экспортировать список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обнаруженные уязвимости в приложениях.

Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

Отобразится список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве.

► *Чтобы просмотреть свойства выбранной уязвимости в приложениях,*

перейдите по ссылке с названием уязвимости в списке уязвимостей в приложениях.

Откроется окно свойств выбранной уязвимости в приложениях.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Просмотр статистики уязвимостей на управляемых устройствах.

Вы можете просмотреть статистическую информацию каждой уязвимости в приложениях на управляемых устройствах. Статистика представлена в виде диаграмм. На диаграмме отображается количество устройств со следующими статусами:

- *Игнорируется на:* <количество устройств>. Этот статус присваивается, если в свойствах уязвимости вы вручную установили параметр игнорировать уязвимость.
- *Закрыта на:* <количество устройств>. Этот статус присваивается, если задача закрытия уязвимости успешно завершена.
- *Запланирована к закрытию на:* <количество устройств>. Этот статус присваивается, если вы создали задачу закрытия уязвимостей, но задача пока еще не завершена.
- *Применено исправление на:* <количество устройств>. Этот статус присваивается, если вы вручную выбрали обновление программного обеспечения, чтобы закрыть уязвимость, но это обновление не закрыло уязвимость.
- *Требуется закрытия на:* <количество устройств>. Этот статус присваивается, если уязвимость была закрыта только на некоторых управляемых устройствах, а уязвимость требуется закрыть на других управляемых устройствах.

► *Чтобы просмотреть статистику уязвимости на управляемых устройствах:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

Отобразится страница со списком уязвимостей в приложениях, обнаруженных на управляемых устройствах.

2. Установите флажок рядом с требуемой уязвимостью.
3. Нажмите на кнопку **Статистика уязвимостей на устройствах**.

Отобразится диаграмма статусов уязвимости. Нажав на статус, откроется список устройств, на которых уязвимость имеет выбранный статус.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Экспорт списка уязвимостей в приложениях в текстовый файл

Вы можете экспортировать список отображаемых уязвимостей в файл формата CSV или TXT. Вы можете использовать эти файлы, например, чтобы отправить их вашему начальнику по информационной безопасности или сохранить их в целях статистики.

► *Чтобы экспортировать список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах, в текстовый файл:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

Отобразится страница со списком уязвимостей в приложениях, обнаруженных на управляемых устройствах.

2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список уязвимостей в приложениях, загружается на устройство, которое вы используете в данный момент.

► *Чтобы экспортировать список уязвимостей в приложениях, обнаруженных на выбранных управляемых устройствах, в текстовый файл:*

1. Откройте список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве (см. раздел "Просмотр информации об уязвимостях в приложениях, обнаруженных на выбранных управляемых устройствах" на стр. [1437](#)).

2. Выберите уязвимости в приложениях, которые вы хотите экспортировать.

Пропустите этот шаг, если вы хотите экспортировать полный список уязвимостей в приложениях, обнаруженных на управляемых устройствах.

При экспорте полного списка уязвимостей в приложениях, обнаруженных на управляемом устройстве, будут экспортированы только те уязвимости, которые отображаются на текущей странице.

3. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список уязвимостей в приложениях, экспортируется с выбранного управляемого устройства, которое вы используете в данный момент.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Игнорирование уязвимостей в приложениях

Вы можете игнорировать уязвимости в приложениях и не закрывать их. Причины для игнорирования уязвимостей в приложениях могут быть, например, следующими:

- Вы не считаете, что уязвимость в приложении является критической для вашей организации.
- Вы понимаете, что закрытие уязвимости в приложениях может повредить данные приложения, для которого требуется закрыть уязвимость.

- Вы уверены, что уязвимость в приложениях не представляет опасности для сети вашей организации, так как вы используете другие меры для защиты управляемых устройств.

Вы можете игнорировать уязвимость в приложениях на всех управляемых устройствах или только на выбранных управляемых устройствах.

► *Чтобы пропустить уязвимость в приложениях на всех управляемых устройствах:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

На странице отображается список уязвимостей в приложениях, обнаруженных на управляемых устройствах.

2. В списке уязвимостей в приложениях нажмите на имя уязвимости в приложениях, которую вы хотите пропустить.

Откроется окно свойств уязвимости в приложениях.

3. На вкладке **Общие** включите параметр **Игнорировать уязвимость**.

4. Нажмите на кнопку **Сохранить**.

Окно свойств уязвимости в приложениях закроется.

Уязвимость в приложениях пропускается на всех управляемых устройствах.

► *Чтобы пропустить уязвимость в приложениях на выбранных управляемых устройствах:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с именем устройства, на котором вы хотите пропустить уязвимость в приложениях.

Откроется окно свойств устройства.

3. В окне свойств устройства выберите раздел **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

Отобразится список уязвимостей в приложениях, обнаруженных на устройстве.

5. В списке уязвимостей в приложениях выберите уязвимость, которую вы хотите пропустить на выбранном устройстве.

Откроется окно свойств уязвимости в приложениях.

6. В окне свойств уязвимости в приложениях на вкладке **Общие** включите параметр **Игнорировать уязвимость**.

7. Нажмите на кнопку **Сохранить**.

Окно свойств уязвимости в приложениях закроется.

8. Закройте окно свойств устройства.

Уязвимость в приложениях пропускается на выбранном устройстве.

Пропущенные уязвимости в приложениях не будут закрыты после завершения работы задачи *Закрытие уязвимостей* и задачи *Установка требуемых обновлений и закрытие уязвимостей*. Вы можете исключить пропущенные уязвимости в приложениях из списка уязвимостей с помощью фильтра.

См. также:

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....[529](#)

Управление запуском приложений на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center связанные с управлением приложениями, запущенных на клиентских устройствах.

В этом разделе

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Получение и просмотр списка приложений, установленных на клиентских устройствах.....[1458](#)

Использование компонента Контроль приложений для управления исполняемыми файлами

Вы можете использовать компонент Контроль приложений, чтобы разрешить или запретить запуск исполняемых файлов на пользовательских устройствах. Компонент Контроль приложений поддерживает операционные системы Windows и Linux.

Для операционных систем Linux компонент Контроль приложений доступен, начиная с Kaspersky Endpoint Security 11.2 для Linux.

Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux создана и активна.

Этапы

Сценарий использования компонента Контроль приложений состоит из следующих этапов:

а. Формирование и просмотр списка исполняемых файлов на клиентских устройствах

Этот этап помогает вам определить, какие исполняемые файлы обнаружены на управляемых устройствах. Просмотрите список исполняемых файлов и сравните его со списками разрешенных и

запрещенных исполняемых файлов. Ограничения использования исполняемых файлов могут быть связаны с политиками информационной безопасности в вашей организации.

Инструкции:

- Консоль администрирования: Инвентаризация исполняемых файлов.
- Kaspersky Security Center Web Console: Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах (на стр. [1444](#)).

b. Создание категорий для исполняемых файлов, используемых в вашей организации

Проанализируйте списки исполняемых файлов, хранящихся на управляемых устройствах. На основе анализа сформируйте категории для исполняемых файлов. Рекомендуется создать категорию "Рабочие приложения", которая охватывает стандартный набор исполняемых файлов, используемых в вашей организации. Если разные группы безопасности используют свои наборы исполняемых файлов в своей работе, для каждой группы безопасности можно создать отдельную категорию.

Инструкции:

- Консоль администрирования: Создание пополняемой вручную категории приложений, Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств, Создание категории приложений, в которую входят исполняемые файлы из указанных папок.
- Kaspersky Security Center Web Console: Создание пополняемой вручную категории приложений (на стр. [1446](#)), Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств (на стр. [1449](#)), Создание категории приложений, в которую входят исполняемые файлы из указанных папок (см. раздел "Создание категории приложений, в которую входят исполняемые файлы из выбранных папок" на стр. [1451](#)).

c. Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security

Настройте компонент Контроль приложений в политике Kaspersky Endpoint Security с использованием категорий, которые вы создали на предыдущем этапе.

Инструкции:

- Консоль администрирования: Настройка управления запуском приложений на клиентских устройствах.
- Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows (на стр. [1456](#)).

d. Включение компонента Контроль приложений в тестовом режиме

Чтобы правила Контроля приложений не блокировали исполняемые файлы, необходимые для работы пользователей, рекомендуется включить тестирование правил Контроля приложений и проанализировать их работу после создания правил. Когда тестирование включено, Kaspersky Endpoint Security для Windows не будет блокировать исполняемые файлы, запуск которых запрещен правилами Контроля приложений, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

При тестировании правил Контроля приложений рекомендуется выполнить следующие действия:

- Определите период тестирования. Период тестирования может варьироваться от нескольких дней до двух месяцев.
- Изучите события, возникающие в результате тестирования работы компонента Контроль приложений.

Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows (на стр. [1456](#)). Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

е. Изменение параметров категорий компонента Контроль приложений

Если требуется, измените параметры компонента Контроль приложений. На основании результатов тестирования вы можете добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию пополняемую вручную.

Инструкции:

- Консоль администрирования: Добавление исполняемых файлов, связанных с событием, в категорию приложений.
- Kaspersky Security Center Web Console: Добавление исполняемых файлов, связанных с событием, в категорию приложений (на стр. [1454](#)).

ф. Применение правил Контроля приложений в рабочем режиме

После проверки правил Контроля приложений и завершения настройки категорий вы можете применить правила Контроль приложений в рабочем режиме.

Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows (на стр. [1456](#)). Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

г. Проверка конфигурации Контроля приложений

Убедитесь, что вы выполнили следующее:

- Создали категории для исполняемых файлов.
- Настроили Контроль приложений с использованием категорий.
- Применили правила Контроля приложений в рабочем режиме.

Результаты

После завершения сценария, запуск исполняемых файлов на управляемых устройствах контролируется. Пользователи могут запускать только те исполняемые файлы, которые разрешены в вашей организации, и не могут запускать исполняемые файлы, запрещенные в вашей организации.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>
- Справка Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/>
- Kaspersky Security для виртуальных сред Легкий агент <https://support.kaspersky.com/KSVLA/5.2/en-US/145134.htm>

Режимы и категории компонента Контроль приложений

Компонент Контроль приложений контролирует попытки пользователей запуска приложений. Вы можете использовать правила компонента Контроль приложений для контроля приложений.

Компонент Контроль приложений доступен для Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security 11.2 для Linux и выше, для Kaspersky Security для виртуальных сред Легкий агент. Все инструкции в этом разделе описывают настройку Контроля приложений для приложения Kaspersky Endpoint Security для Windows.

Запуск исполняемых файлов, параметры которых не соответствуют ни одному из правил Контроля приложений, регулируется выбранным режимом работы компонента:

- *Список запрещенных.* Режим используется, если вы хотите разрешить запуск всех исполняемых файлов, кроме тех, которые указаны в запрещающих правилах. По умолчанию выбран этот режим.
- *Список разрешенных.* Режим используется, если вы хотите запретить запуск всех исполняемых файлов, кроме тех, которые указаны в разрешающих правилах.

Правила Контроля приложений реализованы в категориях для исполняемых файлов. В Kaspersky Security Center существует три типа категорий:

- Пополняемая вручную категория (см. раздел "Создание пополняемой вручную категории приложений" на стр. [1446](#)). Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, KL-категория, путь к файлу, чтобы включить исполняемые файлы в категорию.
- Категория, в которую входят исполняемые файлы с выбранных устройств (см. раздел "Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств" на стр. [1449](#)). Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.
- Категория, в которую входят исполняемые файлы из выбранных папок (см. раздел "Создание категории приложений, в которую входят исполняемые файлы из выбранных папок" на стр. [1451](#)). Вы указываете папку, исполняемые файлы из которой автоматически попадают в категорию.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>
- Справка Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/>
- Kaspersky Security для виртуальных сред Легкий агент <https://support.kaspersky.com/KSVLA/5.2/en-US/145134.htm>

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах

Каждый раз, когда пользователь пытается запустить исполняемый файл, этот файл автоматически добавляется в список компонента Контроль приложений. Вы можете создать задачу инвентаризации и получить список исполняемых файлов, хранящихся на управляемых устройствах. Для инвентаризации исполняемых файлов вам нужно создать задачу инвентаризации.

Функция инвентаризации исполняемых файлов доступна для следующих приложений:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux версии 11.2 и выше
- Kaspersky Security для виртуальных сред 4.0 Легкий агент и выше

Вы можете снизить нагрузку на базу данных при получении информации об установленных приложениях. Для этого рекомендуется запускать задачу инвентаризации на нескольких эталонных устройствах, на которых установлен стандартный набор приложений.

► Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Задачи**.
Отобразится список задач.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи (см. раздел "Создание задачи" на стр. [1174](#)). Следуйте далее указаниям мастера.
3. На странице **Параметры новой задачи** в раскрывающемся списке **Приложение** выберите Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux в зависимости от типа операционной системы клиентских устройств.
4. В раскрывающемся списке **Тип задачи** выберите **Инвентаризация**.
5. На странице **Завершение создания задачи** нажмите на кнопку **Готово**.

После того как мастер создания задачи завершит свою работу, задача **Инвентаризация** создана и настроена. Вы можете изменить параметры созданной задачи. В результате созданная задача отобразится в списке задач.

Подробное описание задачи инвентаризации см. в следующих справках:

- Справка Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>
- Справка Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/index.htm>
- Kaspersky Security для виртуальных сред Легкий агент <https://support.kaspersky.com/KSVLA/5.2/en-US/145134.htm>

После выполнения задачи **Инвентаризация** формируется список исполняемых файлов, хранящихся на управляемых устройствах, и вы можете просмотреть этот список.

При выполнении инвентаризации приложение обнаруживает исполняемые файлы следующих форматов: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR и HTML-файлы.

► Чтобы просмотреть список исполняемых файлов, хранящихся на клиентских устройствах,

В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Исполняемые файлы**.

На странице отобразится список исполняемых файлов, хранящихся на клиентских устройствах.

► *Чтобы отправить исполняемый файл управляемого устройства в "Лабораторию Касперского":*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Исполняемые файлы**.
2. Перейдите по ссылке исполняемого файла, который вы хотите отправить в "Лабораторию Касперского".
3. В открывшемся окне перейдите в раздел **Устройства** и установите флажок рядом с управляемым устройством, с которого вы хотите отправить исполняемый файл.

Перед отправкой исполняемого файла убедитесь, что управляемое устройство имеет прямое подключение к Серверу администрирования, установив флажок **Не разрывать соединение с Сервером администрирования** (см. раздел "Параметры управляемого устройства" на стр. [1193](#)).

4. Нажмите на кнопку **Отправить в "Лабораторию Касперского"**.

Выбранный исполняемый файл загружается для дальнейшей отправки в "Лабораторию Касперского".

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Создание пополняемой вручную категории приложений

Вы можете указать набор критериев в качестве шаблона для исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов, соответствующих критериям, вы можете создать категорию приложений и использовать ее в настройке компонента Контроль приложений.

► *Чтобы создать пополняемую вручную категорию приложений:*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.
Откроется страница со списком категорий приложений.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На шаге **Выбор способа создания категории** выберите параметр **Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную**.
4. На шаге **Условия** нажмите на кнопку **Добавить**, чтобы добавить критерий условия для включения файлов в создаваемую категорию.
5. На шаге **Критерии условия** выберите тип правила для создания категории из списка:
 - **Из KL-категории**

Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". Приложения, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию приложений.

- **Выберите сертификат из хранилища сертификатов**

Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Задайте путь к приложению (поддерживаются маски)**

Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию приложений.

- **Съемный диск**

Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск приложения. Приложения, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию приложений.

- **Хеши файлов папки, метаданные файлов папки или сертификаты из папки:**

- **Выберите из списка исполняемых файлов**

Если выбран этот вариант, приложения для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

- **Выберите из реестра приложений**

Если выбран этот параметр, отображается реестр приложений. Вы можете выбрать приложения из реестра и указать следующие метаданные файла:

- Имя файла.
- Версия файла. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
- Название приложения.
- Версия приложения. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
- Производитель.

- **Задайте вручную**

Если выбран этот вариант, вам нужно указать хеш файла, метаданные или сертификат в качестве условия добавления приложений в пользовательскую категорию.

- **Хеш файла**

В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено

уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center для файлов категории:

- Если все экземпляры приложений безопасности, установленных в вашей сети, являются версиями приложения Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **SHA256**. Не рекомендуется добавлять категорию, созданную по критерию SHA256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою приложения безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.
- Если в вашей сети установлены более ранние версии, чем Kaspersky Endpoint Security 10 Service Pack 2 для Windows, выберите **MD5-хеш**. Добавить категорию, созданную по критерию контрольной суммы MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, невозможно. В этом случае вы можете использовать криптографическую хеш-функцию SHA256 для файлов категории.
- Если разные устройства в вашей сети используют как более ранние, так и более поздние версии Kaspersky Endpoint Security 10, установите флажок **SHA256** и флажок **MD5-хеш**.

Метаданные

Если этот параметр выбран, вы можете указать метаданные файла такие как имя файла, версию файла и поставщика. Метаданные будут передаваться на Сервер администрирования. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в категорию приложений.

Сертификат

Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Из файла MSI-пакета/архивной папки**

Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика приложения будут передаваться на Сервер администрирования. Приложения, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию приложений.

Выбранный критерий добавлен в список условий.

Вы можете добавить столько критериев для создания категории приложений, сколько вам нужно.

6. На шаге **Исключения** нажмите на кнопку **Добавить**, чтобы добавить критерий в область исключений и исключить файлы из создаваемой категории.
7. На шаге **Критерии условия**, выберите тип правила из списка, так же, как вы выбрали тип правила для создания категории.

После завершения мастера создается категория приложений. Оно появится в списке категорий приложений. Вы можете создать категорию приложений при настройке компонента Контроль приложений.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>
- Справка Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/>
- Kaspersky Security для виртуальных сред Легкий агент <https://support.kaspersky.com/KSVLA/5.2/en-US/145134.htm>

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств

Вы можете использовать исполняемые файлы с устройства как шаблон исполняемых файлов, запуск которых вы хотите разрешить или запретить. На основе исполняемых файлов с выбранных устройств вы можете создать категорию и использовать ее для настройки компонента Контроль приложений.

► Чтобы создать категорию, в которую входят исполняемые файлы с выбранных устройств:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.
Откроется страница со списком категорий.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На шаге **Выбор способа создания категории**, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы с выбранных устройств. Исполняемые файлы обрабатываются автоматически, их метрики заносятся в категорию**.
4. Нажмите на кнопку **Добавить**.
5. В открывшемся окне выберите устройство или устройства, чьи исполняемые файлы будут использоваться для создания категории.
6. Задайте следующие параметры:
 - Алгоритм вычисления хеш-функции

В зависимости от версии приложения защиты, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center для файлов категории:

- Если в вашей сети установлены версии приложений защиты Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою приложения защиты. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.
- Если в вашей сети установлены версии приложений защиты ниже версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows, установите флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**. Добавить категорию, созданную по критерию MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.
- Если на разных устройствах в вашей сети используются новые и ранние версии приложений защиты Kaspersky Endpoint Security 10, установите оба флажка, и **Вычислять SHA-256 для файлов в категории**, и **Вычислять MD5 для файлов в категории**.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Синхронизировать данные с хранилищем Сервера администрирования**

Выберите этот параметр, если вы хотите, чтобы Сервер администрирования периодически выполнял проверку изменений в указанной папке (или папках).

По умолчанию параметр выключен.

Если вы включите этот параметр, укажите период (в часах), чтобы проверять изменения в указанной папке (папках). По умолчанию период проверки равен 24 часам.

- **Тип файла**

В этом разделе вы можете указать тип файла, который используется для создания категории приложений.

Все файлы. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.

Только файлы вне категорий приложений. Для создаваемой категории

учитываются только файлы вне категорий приложений.

- **Папки**

В этом разделе вы можете указать папки выбранных устройств, содержащие файлы, которые используются для создания категории приложений.

Все папки. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.

Указанная папка. Для создаваемой категории учитывается только указанная папка. Если вы выбирали этот параметр, вам нужно указать путь к папке.

По завершении работы мастера создается категория исполняемых файлов. Она появится в списке категорий. Вы можете создать категорию при настройке компонента Контроль приложений.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Создание категории приложений, в которую входят исполняемые файлы из выбранных папок

Вы можете использовать исполняемые файлы выбранных папок как эталонный набор исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов из выбранных папок вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

► *Чтобы создать категорию, в которую входят исполняемые файлы из выбранных папок:*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.
Откроется страница со списком категорий.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На шаге **Выбор способа создания категории**, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы из указанной папки. Исполняемые файлы приложений, копируемых в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию**.
4. Укажите папку, исполняемые файлы которой будут использоваться для создания категории.
5. Настройте следующие параметры:
 - **Включать в категорию динамически подключаемые библиотеки (DLL)**

В категорию приложений включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль приложений регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center.

По умолчанию флажок снят.

- **Включать в категорию данные о скриптах**

В категорию приложений включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center.

По умолчанию флажок снят.

- **Алгоритм вычисления хеш-функции: Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше) / Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**

В зависимости от версии приложения защиты, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center для файлов категории:

- Если в вашей сети установлены версии приложений защиты Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою приложения защиты. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.
- Если в вашей сети установлены версии приложений защиты ниже версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows, установите флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**. Добавить категорию, созданную по критерию MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.
- Если на разных устройствах в вашей сети используются новые и ранние версии приложений защиты Kaspersky Endpoint Security 10, установите оба флажка, и **Вычислять SHA-256 для файлов в категории**, и **Вычислять MD5 для файлов в категории**.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Принудительно проверять папку на наличие изменений**

Если этот параметр включен, приложение периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

По умолчанию параметр выключен.

По завершении работы мастера создается категория исполняемых файлов. Она появится в списке категорий. Вы можете использовать категорию для настройки компонента Контроль приложений.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>
- Справка Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/>
- Kaspersky Security для виртуальных сред Легкий агент <https://support.kaspersky.com/KSVLA/5.2/en-US/145134.htm>

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Просмотр списка категорий приложений

Вы можете просмотреть список настроенных категорий исполняемых файлов и параметры каждой категории.

► *Чтобы просмотреть список категорий приложений,*

в главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.

Откроется страница со списком категорий.

► *Чтобы просмотреть свойства категории приложений,*

нажмите на имя категории.

Откроется окно свойств выбранной категории. Параметры сгруппированы на нескольких вкладках.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Добавление исполняемых файлов, связанных с событием, в категорию приложений

После настройки компонента Контроль приложений в политиках Kaspersky Endpoint Security для Windows в списке событий могут отображаться следующие события:

- **Запуск приложения запрещен** (*Критическое событие*). Это событие отображается, если вы настроили Контроль приложений для применения правил.
- **Запуск приложения запрещен в тестовом режиме** (*Информационное событие*). Это событие отображается, если вы настроили Контроль приложений для применения правил в тестовом режиме.
- **Сообщение администратору о запрете запуска приложения** (сообщение с уровнем важности *Предупреждение*). Это событие отображается, если вы настроили Контроль приложений для применения правил, а пользователь запросил доступ к приложению, которое заблокировано для запуска.

Рекомендуется создавать выборки событий (см. раздел "Создание выборки событий" см. стр. [1485](#)) для просмотра событий, связанных с компонентом Контроль приложений.

Вы можете добавить исполняемые файлы, связанные с событиями Контроля приложений, в существующую категорию приложений или в новую категорию приложений. Вы можете добавлять исполняемые файлы только в категорию приложений пополняемую вручную.

► Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
Отобразится список выборок событий.
2. Выберите выборку событий, чтобы просмотреть события, связанные с Контролем приложений, и запустите формирование этой выборки событий (см. раздел "Просмотр списка выборки событий" см. стр. [1486](#)).

Если вы не создали выборку событий, связанную с Контролем приложений, вы можете выбрать и запустить предопределенную выборку, например, **Последние события**.
Отобразится список событий.
3. Выберите события, связанные исполняемые файлы которых, вы хотите добавить в категорию приложений, и нажмите на кнопку **Назначить категорию**.
Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. На странице мастера укажите необходимые параметры:
 - В разделе **Действие с исполняемым файлом, связанным с событием** выберите один из следующих вариантов:
 - **Добавить в новую категорию приложений**
Выберите этот параметр, если вы хотите создать категорию приложений на основе исполняемых файлов, связанных с событиями.
По умолчанию выбран этот вариант.
Если вы выбрали этот параметр, укажите имя новой категории.
 - **Добавить в существующую категорию**

Выберите этот параметр, если вы хотите добавить исполняемые файлы, связанные с событиями, в существующую категорию приложений.

По умолчанию вариант не выбран.

Если вы выбрали этот параметр, выберите категорию приложений, пополняемую вручную, в которую вы хотите добавить исполняемые файлы.

- В разделе **Тип правила** выберите следующие параметры:
 - **Правила для добавления в область действия**
 - **Правила для добавления в исключения**
- В разделе **Параметр, используемый в качестве условия** выберите один из следующих вариантов:

- **Данные сертификата (или SHA256 для файлов без сертификата)**

Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложений или несколько приложений одного производителя.

Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA-256 для файлов без сертификата.

По умолчанию этот вариант выбран.

- **Данные сертификата (файлы без сертификата пропускаются)**

Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложений или несколько приложений одного производителя.

Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

- **Только SHA256 (файлы без хеша пропускаются)**

Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA-256 исполняемого файла.

- **Только MD5 (для совместимости с Kaspersky Endpoint Security 10 Service Pack 1)**

Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например,

заданная версия приложения.

Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции MD5 исполняемого файла. Вычисление хеш-функции MD5 поддерживается для версий Kaspersky Endpoint Security 10 Service Pack 1 для Windows и ниже.

5. Нажмите на кнопку **ОК**.

После завершения работы мастера исполняемые файлы, связанные с событиями Контроля приложений, добавляются в существующую категорию приложений или в новую категорию приложений. Вы можете просмотреть параметры категории приложений, которую вы изменили или создали.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>
- Справка Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/>
- Kaspersky Security для виртуальных сред Легкий агент <https://support.kaspersky.com/KSVLA/5.2/en-US/145134.htm>

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows

После создания категорий для Контроля приложений, вы можете использовать их для настройки Контроля приложений в политиках Kaspersky Endpoint Security для Windows.

► Чтобы настроить компонент Контроль приложений в политике Kaspersky Endpoint Security для Windows:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
Отобразится страница со списком политик.
2. Нажмите на политику **Kaspersky Endpoint Security для Windows**.
Откроется окно свойств политики.
3. Перейдите в раздел **Параметры приложения → Контроль безопасности → Контроль приложений**.
Отобразится окно **Контроль приложений** с параметрами компонента Контроль приложений.
4. Параметр **Контроль приложений** включен по умолчанию. Убедитесь, что переключатель **Контроль приложений Выключен** переведен в неактивное положение.
5. В блоке **Параметры Контроля приложений** включите режим работы с применением правил Контроля приложений и разрешите Kaspersky Endpoint Security для Windows блокировку запуска приложений.

Если вы хотите протестировать правила Контроля приложений, в разделе **Параметры Контроля приложений**, включите тестовый режим. В тестовом режиме Kaspersky Endpoint Security для Windows не блокирует запуск приложений, но фиксирует информацию о сработавших правилах в отчете. Перейдите по ссылке **Просмотреть отчет** для просмотра этой информации.

6. Включите параметр **Управление загрузкой модулей DLL**, если вы хотите, чтобы приложение Kaspersky Endpoint Security для Windows контролировало загрузку модулей DLL при запуске приложений пользователями.

Информация о модуле и приложении, которое загрузило модуль, будет сохранена в отчете.

Kaspersky Endpoint Security для Windows контролирует только DLL модули и драйверы, которые были загружены после того, как параметр **Управление загрузкой модулей DLL** был включен. Перезагрузите устройство после выбора параметра **Управление загрузкой модулей DLL**, если вы хотите, чтобы приложение Kaspersky Endpoint Security для Windows контролировало все модули и драйверы DLL, включая те, которые были загружены до запуска Kaspersky Endpoint Security для Windows.

7. (Если требуется.) В блоке **Шаблоны сообщений** измените шаблон сообщения, которое отображается, когда приложение заблокировано для запуска, и шаблон сообщения электронной почты, которое отправляется вам.
8. В блоке параметров **Режим Контроля приложений** выберите режим **Список запрещенных** или **Список разрешенных**.

По умолчанию выбран режим **Список запрещенных**.

9. Перейдите по ссылке **Параметры списков правил**.

Откроется окно **Списки запрещенных и разрешенных**, в котором можно добавить категорию приложений. По умолчанию отображается вкладка **Список запрещенных**, если выбран режим **Список запрещенных** или отображается вкладка **Список разрешенных**, если выбран режим **Список разрешенных**.

10. В окне **Списки запрещенных и разрешенных** нажмите на кнопку **Добавить**.

Откроется окно **Правило Контроля приложений**.

11. Перейдите по ссылке **Пожалуйста, выберите категорию**.

Откроется окно **Категории приложений**.

12. Добавьте категорию приложений (или категории), которые вы создали ранее.

Вы можете изменить параметры категории, нажав на кнопку **Изменить**.

Вы можете создать категорию, нажав на кнопку **Добавить**.

Вы можете удалить категорию, нажав на кнопку **Удалить**.

13. После того как формирование списка категорий приложений завершено, нажмите на кнопку **ОК**.

Окно **Категории приложений** закрывается.

14. В окне правил **Контроль приложений** в разделе **Субъекты и их права** создайте список пользователей и групп пользователей, чтобы применить к ним правила Контроля приложений.

15. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Правило Контроля приложений**.

16. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Списки запрещенных и разрешенных**.

17. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Контроль приложений**.

18. Закройте окно с параметрами политики Kaspersky Endpoint Security для Windows.

Компонент Контроль приложений настроен. После распространения политики на клиентские устройства запуск исполняемых файлов контролируется.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>
- Справка Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/>
- Kaspersky Security для виртуальных сред Легкий агент <https://support.kaspersky.com/KSVLA/5.2/en-US/145134.htm>

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....572

Получение и просмотр списка приложений, установленных на клиентских устройствах

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Linux и Windows.

Агент администрирования составляет список приложений, установленных на устройстве, и передает список Серверу администрирования. Агенту администрирования требуется около 10–15 минут для обновления списка приложений.

Для клиентских устройств с операционной системой Windows Агент администрирования получает большую часть информации об установленных приложениях из реестра Windows. Для клиентских устройств с операционной системой Linux информацию об установленных приложениях Агент администрирования получает от диспетчеров пакетов.

► Чтобы просмотреть список приложений, установленных на управляемых устройствах,

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений**.

На странице отображается таблица с приложениями, установленными на управляемых устройствах. Выберите приложение, чтобы просмотреть свойства этого приложения, например: имя производителя, номер версии, список исполняемых файлов, список устройств, на которых установлена программа, список доступных обновлений программного обеспечения или список обнаруженных уязвимостей программного обеспечения.

2. Вы можете группировать и фильтровать данные таблицы с установленными приложениями следующим образом:

- Нажмите на значок параметров () в правом верхнем углу таблицы.

В открывшемся меню **Параметры столбцов** выберите столбцы, которые будут отображаться в таблице. Чтобы просмотреть тип операционной системы клиентских устройств, на которых установлено приложение, выберите столбец **Тип операционной системы**.

- Нажмите на значок фильтрации () в правом верхнем углу таблицы, укажите и примените критерий фильтрации в открывшемся меню.

Отобразится отфильтрованная таблица установленных приложений.

Чтобы просмотреть список приложений, установленных на выбранном управляемом устройстве,

В главном окне приложения перейдите в раздел **Устройства** → **Управляемые устройства** → **Имя устройства** → **Дополнительно** → **Реестр приложений**. В этом меню можно экспортировать список приложений в файлы форматов CSV или TXT.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>
- Справка Kaspersky Endpoint Security для Linux <https://support.kaspersky.com/KES4Linux/12.0.0/en-US/>
- Kaspersky Security для виртуальных сред Легкий агент <https://support.kaspersky.com/KSVLA/5.2/en-US/145134.htm>

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Создание инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Kaspersky Security Center Web Console позволяет выполнять удаленную установку приложений сторонних производителей с помощью инсталляционных пакетов. Такие приложения сторонних производителей включены в соответствующую базу данных "Лаборатории Касперского". База данных создается автоматически при первом запуске задачи *Загрузка обновлений в хранилище Сервера администрирования* (см. раздел "Создание задачи *Загрузка обновлений в хранилище Сервера администрирования*" см. стр. [1347](#)).

► *Чтобы создать инсталляционный пакет для приложения стороннего производителя из базы "Лаборатории Касперского":*

- В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
- Нажмите на кнопку **Добавить**.
- На открывшейся странице мастера создания инсталляционного пакета выберите параметр **Выбрать приложение из базы "Лаборатории Касперского"** для создания инсталляционного пакета и нажмите на кнопку **Далее**.
- В открывшемся списке приложений выберите соответствующее приложение и нажмите на кнопку **Далее**.

5. Выберите нужный язык локализации в раскрывающемся списке и нажмите на кнопку **Далее**.

Этот шаг отображается только если приложение предоставляет несколько языков.

6. Если вам будет предложено принять Лицензионное соглашение для установки, на открывшейся странице **Лицензионное соглашение** перейдите по ссылке на веб-сайте производителя, чтобы прочитать Лицензионное соглашение, а затем установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения**.
7. На открывшейся странице **Имя нового инсталляционного пакета** в поле **Имя пакета** укажите имя инсталляционного пакета и нажмите на кнопку **Далее**.

Дождитесь загрузки созданного инсталляционного пакета на Сервер администрирования. После того как мастер создания инсталляционного пакета отобразит сообщение, информирующее вас, что процесс создания пакета успешно завершен, нажмите на кнопку **Готово**.

Созданный инсталляционный пакет появится в списке инсталляционных пакетов. Вы можете выбрать этот пакет при создании или перенастройке задачи *Удаленная установка приложения*.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Просмотр и изменение параметров инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Если вы ранее создавали какие-либо инсталляционные пакеты приложений сторонних производителей, перечисленные в базе "Лаборатории Касперского" (см. раздел "Создание инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"" см. стр. [1459](#)), вы можете просмотреть и изменить параметры (см. раздел "Параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"" см. стр. [1461](#)) этих пакетов.

Изменение параметров инсталляционного пакета приложения стороннего производителя из базы "Лаборатории Касперского" доступно только при наличии лицензии на Системное администрирование.

Чтобы просмотреть и изменить параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
2. В открывшемся списке инсталляционных пакетов нажмите на имя соответствующего пакета.
3. На открывшейся странице свойств измените параметры, если это требуется.
4. Нажмите на кнопку **Сохранить**.

Изменения сохранены.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Параметры инсталляционного пакета приложения стороннего производителя сгруппированы на следующих вкладках:

По умолчанию отображается только часть параметров, перечисленных ниже. Вы можете добавить соответствующие графы, нажав на кнопку **Фильтр** и выбрав соответствующие графы из списка.

- Вкладка **Общие**:
 - Поле ввода, содержащее название инсталляционного пакета, которое можно изменить вручную.
 - **Приложение**
 - **Версия**
 - **Размер**
 - **Создан**
 - **Путь**
- Вкладка **Последовательность установки**:
 - **Устанавливать требуемые общесистемные компоненты**
 - Таблица, в которой отображаются свойства обновления и которая содержит следующие графы:
 - **Имя**
 - **Описание**
 - **Источник**
 - **Тип**
 - **Категория**
 - **Уровень важности по MSRC**
 - **Уровень важности**
 - **Уровень важности патча**
 - **Статья**
 - **Бюллетень**
 - **Не назначено к установке (новая версия)**
 - **Назначено к установке**
 - **Устанавливается**

- Установлено
 - Сбой
 - Требуется перезагрузка
 - Зарегистрировано
 - Устанавливается интерактивно
 - Отозвано
 - Статус одобрения обновления
 - Ревизия
 - Идентификатор обновления
 - Версия приложения
 - Заменяемое
 - Заменяющее
 - Требуется принять условия Лицензионного соглашения
 - Описание веб-адреса
 - Семейство приложений
 - Приложение
 - Язык локализации
 - Не назначено к установке (новая версия)
 - Требуется установки пререквизитов
 - Режим загрузки
 - Является патчем
 - Не установлено
- Вкладка **Параметры**, на которой отображаются параметры инсталляционного пакета, их названия, описания и значения, которые используются в качестве параметров командной строки во время установки. Если в пакете таких нет параметров, отображается соответствующее сообщение. Вы можете изменить значения этих параметров.
 - Вкладка **История ревизий**, на которой отображаются версии инсталляционного пакета и которая содержит следующие графы:
 - **Ревизия** – номер ревизии инсталляционного пакета.
 - **Время** – дата и время изменения параметров инсталляционного пакета.
 - **Пользователь** – имя пользователя, изменившего параметры инсталляционного пакета.
 - **Действие** – действия, которые были выполнены с инсталляционным пакетом в этой ревизии.
 - **Описание** – описание ревизии изменения параметров инсталляционного пакета.
- По умолчанию описание ревизии не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

См. также:

Сценарий: настройка защиты сети.....[403](#)

Теги приложений

Kaspersky Security Center позволяет назначать теги приложениям из реестра приложений (см. раздел "Получение и просмотр списка приложений, установленных на клиентских устройствах" на стр. [1458](#)). Тег представляет собой метку приложения, которую можно использовать для группировки и поиска приложений. Назначенный приложению тег можно использовать в условиях для выборок устройств (см. раздел "Выборки устройств" на стр. [1218](#)).

Например, можно создать тег [\[Браузеры\]](#) и назначить его всем браузерам, таким как Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Сценарий: обнаружение сетевых устройств[1109](#)

Создание тегов приложений

► Чтобы создать тег приложения:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Теги приложений**.
2. Нажмите на кнопку **Добавить**.
Отобразится окно создания тега.
3. Укажите тег.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
Созданный тег появляется в списке тегов приложения.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Сценарий: обнаружение сетевых устройств[1109](#)

Изменение тегов приложений

► Чтобы переименовать тег приложения:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Теги приложений**.
2. Установите флажок рядом с тегом, который вы хотите переименовать, и нажмите на кнопку **Изменить**.

Откроется окно свойств тега.

3. Измените имя тега.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов приложений.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Сценарий: обнаружение сетевых устройств[1109](#)

Назначение тегов приложениям

► Чтобы назначить приложению теги:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений**.

2. Выберите приложение, для которого требуется назначить теги.

3. Выберите вкладку **Теги**.

На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в столбце **Назначенный тег**.

4. Установите флажки в столбце **Назначенный тег** для тегов, которые требуется назначить.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги назначены приложению.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....[572](#)

Сценарий: обнаружение сетевых устройств[1109](#)

Снятие назначенных тегов с приложений

► *Чтобы снять теги с приложения:*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений**.
2. Выберите приложение, с которого требуется снять теги.
3. Выберите вкладку **Теги**.

На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в столбце **Назначенный тег**.

4. Снимите флажки в столбце **Назначенный тег** для тегов, которые требуется снять.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги будут сняты с приложения.

Снятые с приложений теги не удаляются. При необходимости их можно удалить вручную (см. раздел "Удаление тегов приложений" см. стр. [1465](#)).

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....	572
Сценарий: обнаружение сетевых устройств	1109

Удаление тегов приложений

► *Чтобы удалить тег приложения:*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Теги приложений**.
2. В списке выберите теги приложения, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Выбранный тег приложения удален. Удаленный тег автоматически снимается со всех приложений, которым он был назначен.

См. также:

Использование компонента Контроль приложений для управления исполняемыми файлами.....	572
Сценарий: обнаружение сетевых устройств	1109

Мониторинг и отчеты

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky Security Center. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky Security Center можно настраивать функции мониторинга и параметры отчетов.

В этом разделе

Сценарий: мониторинг и отчеты	1466
О типах мониторинга и отчетах	1468
Панель мониторинга и веб-виджеты	1469
Отчеты	1474
События и выборки событий	1484
Уведомления и статусы устройств	1539
Объявления "Лаборатории Касперского"	1555
Просмотр информации об обнаруженных угрозах	1558
Cloud Discovery	1559

Сценарий: мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Kaspersky Security Center.

Предварительные требования

После развертывания Kaspersky Security Center в сети организации вы можете приступить к мониторингу состояния безопасности сети с помощью Kaspersky Security Center и к формированию отчетов.

Мониторинг и работа с отчетами в сети организации состоят из следующих этапов:

а. Настройка переключения статусов устройств

Ознакомьтесь с параметрами статусов устройства в зависимости от конкретных условий. Изменяя эти параметры (см. раздел "Настройка переключения статусов устройств" на стр. [1547](#)), вы можете изменить количество событий с уровнями важности *Критический* или *Предупреждение*. При настройке переключения состояний устройства убедитесь, что:

- новые параметры не противоречат политикам информационной безопасности вашей организации;
- вы можете своевременно реагировать на важные события безопасности в сети вашей организации.

б. Настройка параметров уведомлений о событиях на клиентских устройствах

Инструкции:

Настройка уведомлений (по электронной почте, по SMS или с помощью запуска исполняемого файла) о событиях на клиентских устройствах (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)).

с. Изменение ответа вашей сети безопасности на событие Вирусная атака

Вы можете изменить пороговые значения в свойствах Сервера администрирования. Вы также можете создать более строгую политику (см. раздел "Автоматическая активация политики по событию "Вирусная атака"" на стр. [1259](#)), которая будет активирована, или создать задачу (см. раздел "Создание задачи" на стр. [1174](#)), которая будет запускаться при возникновении этого события.

d. Выполнение рекомендуемых действий для критических и предупреждающих уведомлений

Инструкции:

Выполните рекомендуемые действия для сети вашей организации (см. раздел "Просмотр экранных уведомлений" на стр. [1540](#)).

e. Просмотр состояния безопасности сети вашей организации

Инструкции:

- Просмотр веб-виджета Состояние защиты (см. раздел "Использование панели мониторинга" на стр. [1469](#)).
- Генерация и просмотр отчета Отчет о состоянии защиты (см. раздел "Генерация и просмотр отчета" см. стр. [1479](#)).
- Генерация и просмотр отчета Отчет об ошибках (см. раздел "Генерация и просмотр отчета" см. стр. [1479](#)).

f. Нахождение незащищенных клиентских устройств

Инструкции:

- Просмотр веб-виджета Новые устройства (см. раздел "Использование панели мониторинга" на стр. [1469](#)).
- Генерация и просмотр отчета Отчет о развертывании защиты (см. раздел "Генерация и просмотр отчета" см. стр. [1479](#)).

g. Проверка защиты клиентских устройств

Инструкции:

- Генерация и просмотр отчета из категорий Состояние защиты и Статистика угроз (см. раздел "Генерация и просмотр отчета" см. стр. [1479](#)).
- Запуск и просмотр выборки событий Критическое (см. раздел "Просмотр списка выборки событий" см. стр. [1486](#)).

h. Оценка и ограничение загрузки событий в базу данных

Информация о событиях, которые возникают во время работы управляемых приложений, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

Инструкции:

- Расчет места в базе данных

- Ограничение максимального количества событий (см. раздел "Настройка количества событий в хранилище событий" на стр. [1018](#)).

i. Просмотр информации о лицензии

Инструкции:

- Добавление веб-виджета Используемые лицензионные ключи в панель мониторинга и его просмотр (см. раздел "Использование панели мониторинга" на стр. [1469](#)).
- Генерация и просмотр отчета Отчет об использовании лицензионных ключей (см. раздел "Генерация и просмотр отчета" см. стр. [1479](#)).

Результаты

После завершения сценария вы будете проинформированы о защите сети вашей организации и, таким образом, сможете планировать действия для дальнейшей защиты.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"[455](#)

О типах мониторинга и отчетах

Информация о событиях безопасности в сети организации хранится в базе данных Сервера администрирования. Kaspersky Security Center Web Console предоставляет следующие виды мониторинга и отчетов в сети вашей организации:

- Панель мониторинга
- Отчеты
- Выборки событий
- Уведомления

Панель мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Отчеты

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Выборки событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события, Отказы функционирования, Предупреждения и Информационные события.**
- Время: **Последние события.**
- Тип: **Запросы пользователей и События аудита.**

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center Web Console.

Уведомления

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

Панель мониторинга и веб-виджеты

В этом разделе содержится информация о панели мониторинга и веб-виджетах, представленных в панели мониторинга. Раздел содержит инструкции по управлению веб-виджетами и настройке веб-виджетов.

Использование панели мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Панель мониторинга доступна в Kaspersky Security Center Web Console в разделе **Мониторинг и отчеты** → **Панель мониторинга**.

В панели мониторинга представлены настраиваемые веб-виджеты. Вы можете выбрать большое количество различных веб-виджетов, представленных в виде круговых диаграмм, таблиц, графиков, гистограмм и списков. Информация, отображаемая в веб-виджетах, обновляется автоматически, период обновления составляет от одной до двух минут. Интервал времени между обновлениями зависит от типа веб-виджета. Вы можете обновить данные веб-виджета вручную с помощью меню, в любое время.

По умолчанию веб-виджеты включают информацию о событиях, хранящихся в базе данных Сервера администрирования.

Kaspersky Security Center Web Console имеет по умолчанию набор веб-виджетов для следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

Некоторые веб-виджеты имеют текст со ссылками. Чтобы просмотреть подробную информацию, перейдите по ссылке.

При настройке панели мониторинга можно добавлять (см. раздел "Добавление веб-виджета на информационную панель" см. стр. [1470](#)) необходимые веб-виджеты, скрывать веб-виджеты (см. раздел "Удаление веб-виджета с информационной панели" см. стр. [1470](#)), а также менять внешний вид или размер (см. раздел "Изменение размера или внешнего вида веб-виджета" см. стр. [1471](#)) веб-виджетов, перемещать (см. раздел "Перемещение веб-виджета на информационной панели" на стр. [1471](#)) веб-виджеты и изменять параметры (см. раздел "Изменение параметров веб-виджета" см. стр. [1472](#)) веб-виджетов.

См. также:

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985
Сценарий: мониторинг и отчеты	1466

Добавление веб-виджета на информационную панель

► Чтобы добавить веб-виджет на информационную панель:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
3. В списке доступных веб-виджетов выберите веб-виджет, который требуется добавить на информационную панель.

Веб-виджеты сгруппированы по категориям. Чтобы посмотреть, какие веб-виджеты входят в категорию, нажмите на значок шеврона (>) рядом с именем категории.

4. Нажмите на кнопку **Добавить**.

Выбранные веб-виджеты будут добавлены в конец информационной панели.

Можно изменить внешний вид (см. раздел "Изменение размера или внешнего вида веб-виджета" см. стр. [1471](#)) и параметры (см. раздел "Изменение параметров веб-виджета" см. стр. [1472](#)) добавленных веб-виджетов.

См. также:

Сценарий: мониторинг и отчеты	1466

Удаление веб-виджета с информационной панели

► Чтобы удалить веб-виджет с информационной панели:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется удалить.
3. Выберите **Скрыть веб-виджет**.
4. В появившемся окне **Предупреждение** нажмите на кнопку **ОК**.

Выбранный веб-виджет будет удален с информационной панели. В дальнейшем можно опять добавить веб-виджет на информационную панель (см. раздел "Добавление веб-виджета на информационную панель" см. стр. [1470](#)).

См. также:

Сценарий: мониторинг и отчеты	1466

Перемещение веб-виджета на информационной панели

► *Чтобы переместить веб-виджет на информационной панели:*

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙️) рядом с веб-виджетом, который требуется переместить.
3. Выберите **Переместить**.
4. Укажите место, куда требуется переместить веб-виджет. Можно выбрать только другой веб-виджет. Выбранные веб-виджеты поменяются местами.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Изменение размера или внешнего вида веб-виджета

Можно изменить внешний вид веб-виджетов: выбрать столбчатую или линейную диаграмму. Для некоторых веб-виджетов можно изменить размер: маленький, средний или крупный.

► *Чтобы изменить внешний вид веб-виджета:*

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙️) рядом с веб-виджетом, который требуется изменить.
3. Выполните одно из следующих действий:
 - Чтобы веб-виджет отображался как столбчатая диаграмма, выберите **Тип диаграммы: линейчатая диаграмма**.
 - Чтобы веб-виджет отображался как линейная диаграмма, выберите **Тип диаграммы: линейный график**.
 - Чтобы поменять размер области, занимаемой веб-виджетом, выберите одно из значений:
 - **Минимальный**
 - **Минимальный (только линейчатая диаграмма)**
 - **Средний (кольцевой график)**
 - **Средний (линейчатая диаграмма)**
 - **Максимальный**

Внешний вид выбранного веб-виджета будет изменен.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Изменение параметров веб-виджета

► Чтобы изменить параметры веб-виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙️) рядом с веб-виджетом, который требуется изменить.
3. Выберите **Показать параметры**.
4. В открывшемся окне параметров веб-виджета измените требуемые параметры веб-виджета.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Параметры выбранного веб-виджета будут изменены.

Набор параметров зависит от конкретного веб-виджета. Ниже приведены некоторые общие параметры:

- **Область веб-виджета** – набор объектов, для которых веб-виджет отображает информацию; например, группа администрирования или выборка устройств.
- **Выберите задачу** – задача, для которой веб-виджет отображает информацию.
- **Период** – период, за который отображается информация в веб-виджете; например, между двумя заданными датами, от заданной даты до настоящего времени или за указанное количество дней до настоящего времени.
- **Установить статус "Критический", если** и **Установить статус "Предупреждение", если** – правила, в соответствии с которыми назначаются цвета на графике статусов.

После изменения параметров веб-виджета вы можете обновить данные веб-виджета вручную.

► Чтобы обновить данные веб-виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙️) рядом с веб-виджетом, который требуется переместить.
3. Нажмите на кнопку **Обновить**.

Данные веб-виджета обновлены.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

О режиме Просмотра только панели мониторинга

Вы можете настраивать режим Просмотра только панели мониторинга (см. раздел "Настройка режима Просмотра только панели мониторинга" на стр. [1473](#)) для сотрудников, которые не управляют сетью, но хотят просматривать статистику защиты сети в Kaspersky Security Center (например, это может быть топ-менеджер). Когда у пользователя включен этот режим, у пользователя отображается только панель мониторинга с предопределенным набором веб-виджетов. Таким образом, пользователь может просматривать указанную в веб-виджетах статистику, например, состояние защиты всех управляемых устройств, количество недавно обнаруженных угроз или список наиболее частых угроз в сети.

При работе пользователя в режиме Просмотра только панели мониторинга применяются следующие ограничения:

- Главное меню не отображается, поэтому пользователь не может изменить параметры защиты сети.
- Пользователь не может выполнять действия с веб-виджетами, например, добавлять или скрывать их. Поэтому нужно разместить в панели мониторинга все необходимые пользователю веб-виджеты и настроить их, например, задать правило подсчета объектов или указать период.

Вы не можете назначить режим Просмотра только панели мониторинга себе. Если вы хотите работать в этом режиме, обратитесь к системному администратору, поставщику услуг (MSP) или пользователю с правами **Изменение списков управления доступом объектов** (см. раздел "**Настройка прав доступа к функциям приложения Управление доступом на основе ролей**" см. стр. [1275](#)) в функциональной области **Общие функции: Права пользователя**.

См. также:

Настройка режима Просмотра только панели мониторинга.....[1473](#)

Настройка режима Просмотра только панели мониторинга

Перед началом настройки режима Просмотра только панели мониторинга (см. раздел "О режиме Просмотра только панели мониторинга" на стр. [1472](#)) убедитесь, что выполнены следующие предварительные требования:

- У вас есть право **Modify object ACLs** (см. раздел "**Настройка прав доступа к функциям приложения Управление доступом на основе ролей**" см. стр. [1275](#)) в функциональной области **Общие функции: Права пользователя**. Если у вас нет этого права, вкладка для настройки режима будет отсутствовать.
- Пользователь с правом **Чтение** (см. раздел "**Настройка прав доступа к функциям приложения Управление доступом на основе ролей**" см. стр. [1275](#)) в области **Общие функции: Базовая функциональность**.

Если в вашей сети выстроена иерархия Серверов администрирования, для настройки режима Просмотра только панели мониторинга перейдите на тот Сервер, на котором учетная запись пользователя доступна на вкладке **Пользователи** в разделе **Пользователи и роли** → **Пользователи и группы**. Это может быть главный Сервер или физический подчиненный Сервер. На виртуальном Сервере администрирования настроить режим Просмотра только панели мониторинга невозможно.

► *Чтобы настроить режим Просмотра только панели мониторинга:*

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на имя учетной записи пользователя, для которой вы хотите настроить панель инструментов с веб-виджетами.
3. В открывшемся окне свойств учетной записи выберите вкладку **Панель мониторинга**.
На открывшейся вкладке отображается та же панель мониторинга, что и для пользователя.
4. Если параметр **Отображать режим Просмотра только панели мониторинга** включен, выключите его переключателем.

Когда этот параметр включен, также невозможно изменить панель мониторинга. После выключения параметра можно управлять веб-виджетами.

5. Настройте внешний вид панели мониторинга. Набор веб-виджетов, подготовленный на вкладке **Панель мониторинга**, доступен для пользователя с настраиваемой учетной записью. Пользователь с такой учетной записью не может изменять какие-либо параметры или размер веб-виджетов, добавлять или удалять веб-виджеты с панели мониторинга. Поэтому настройте их под пользователя, чтобы он мог просматривать статистику защиты сети. С этой целью на вкладке **Панель мониторинга** можно выполнять те же действия с веб-виджетами, что и в разделе **Мониторинг и отчеты** → **Панель мониторинга**:
 - Добавлять веб-виджеты (см. раздел "Добавление веб-виджета на информационную панель" см. стр. [1470](#)) в панель мониторинга.
 - Скрывать веб-виджеты (см. раздел "Удаление веб-виджета с информационной панели" см. стр. [1470](#)), которые не нужны пользователю.
 - Перемещать веб-виджеты (см. раздел "Перемещение веб-виджета на информационной панели" на стр. [1471](#)) в определенном порядке.
 - Изменять размер или внешний вид (см. раздел "Изменение размера или внешнего вида веб-виджета" см. стр. [1471](#)) веб-виджетов.
 - Изменять параметры веб-виджетов (см. раздел "Изменение параметров веб-виджета" см. стр. [1472](#)).
6. Переключите переключатель, чтобы включить параметр **Отображать режим Просмотра только панели мониторинга**.

После этого пользователю доступна только панель мониторинга. Пользователь может просматривать статистику, но не может изменять параметры защиты сети и внешний вид панели мониторинга. Так как вам отображается та же панель мониторинга, что и для пользователя, вы также не можете изменить панель мониторинга.

Если оставить этот параметр выключенным, у пользователя отображается главное меню, поэтому он может выполнять различные действия в Kaspersky Security Center, в том числе изменять параметры безопасности и веб-виджеты.
7. Нажмите на кнопку **Сохранить**, когда закончите настройку режима Просмотра только панели мониторинга. Только после этого подготовленная панель мониторинга будет отображаться у пользователя.
8. Если пользователь хочет просмотреть статистику поддерживаемых приложений "Лаборатории Касперского" и ему нужны для этого права доступа, настройте права (см. раздел "Настройка прав доступа к функциям приложения Управление доступом на основе ролей" см. стр. [1275](#)) для этого пользователя. После этого данные приложений "Лаборатории Касперского" отображаются у пользователя в веб-виджетах этих приложений.

Теперь пользователь может входить в Kaspersky Security Center под настраиваемой учетной записью и просматривать статистику защиты сети в режиме Просмотра только панели мониторинга.

Отчеты

В этом разделе описывается, как использовать отчеты, управлять шаблонами пользовательских отчетов, использовать шаблоны для создания отчетов и создавать задачи рассылки отчетов.

В этом разделе

Использование отчетов	1475
Создание шаблона отчета	1475
Просмотр и изменение свойств шаблона отчета.....	1476
Экспорт отчета в файл	1479
Генерация и просмотр отчета.....	1479
Создание задачи рассылки отчета.....	1480
Удаление шаблонов отчетов	1484

Использование отчетов

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Отчеты доступны в Kaspersky Security Center Web Console в разделе **Мониторинг и отчеты** → **Отчеты**.

По умолчанию отчеты включают информацию за последние 30 дней.

Kaspersky Security Center имеет по умолчанию набор отчетов для следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

Вы можете создавать пользовательские шаблоны отчетов (см. раздел "Создание шаблона отчета" см. стр. [1475](#)), редактировать шаблоны отчетов (см. раздел "Просмотр и изменение свойств шаблона отчета" см. стр. [1476](#)) и удалять их (см. раздел "Удаление шаблонов отчетов" см. стр. [1484](#)).

Можно создавать отчеты (см. раздел "Генерация и просмотр отчета" см. стр. [1479](#)) на основе существующих шаблонов, экспортировать отчеты в файл (см. раздел "Экспорт отчета в файл" см. стр. [1479](#)) и создавать задачи рассылки отчетов (см. раздел "Создание задачи рассылки отчета" см. стр. [1480](#)).

См. также:

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985
Сценарий: мониторинг и отчеты	1466

Создание шаблона отчета

► *Чтобы создать шаблон отчета:*

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.

2. Нажмите на кнопку **Добавить**.

В результате запустится мастер создания шаблона отчета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Введите название отчета и выберите тип отчета.
4. На шаге мастера **Область действия** выберите набор клиентских устройств (групп администрирования, выборки устройств или всех сетевых устройств), данные о которых будут отображаться в отчетах, сформированных на основе этого шаблона.
5. На шаге мастера **Период отчета** укажите период, за который будет формироваться отчет. Доступные значения:
 - между двумя указанными датами;
 - от указанной даты до даты создания отчета;
 - от даты создания отчета минус указанное количество дней до даты создания отчета.

В некоторых отчетах эта страница может не отображаться.

6. Нажмите на кнопку **ОК**, чтобы завершить работу мастера.
7. Выполните одно из следующих действий:
 - Нажмите на кнопку **Сохранить и запустить**, чтобы сохранить новый шаблон отчета и запустить формирование отчета на его основе.
Шаблон отчета будет сохранен. Отчет будет сформирован.
 - Нажмите на кнопку **Сохранить**, чтобы сохранить новый шаблон отчета.
Шаблон отчета будет сохранен.

Созданный шаблон можно использовать для формирования и просмотра отчетов.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Просмотр и изменение свойств шаблона отчета

Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

► Чтобы просмотреть и изменить свойства шаблона отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Установите флажок напротив шаблона отчета, свойства которого вы хотите просмотреть и изменить.
В качестве альтернативы можно сначала сформировать отчет (см. раздел "Генерация и просмотр отчета" см. стр. [1479](#)), а затем нажать на кнопку **Изменить**.
3. Нажмите на кнопку **Открыть свойства шаблона отчета**.
Откроется окно **Изменение отчета <имя отчета>** на вкладке **Общие**.
4. Измените свойства шаблона отчета:

- Вкладка **Общие**:

- Название шаблона отчета
- **Максимальное число отображаемых записей**

Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение.

Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Столбцы** → **Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

По умолчанию параметр включен. По умолчанию указано значение 1000.

- **Группа**

Нажмите на кнопку **Параметры**, чтобы изменить набор клиентских устройств, для которых создается отчет. Для некоторых типов отчетов кнопка может быть недоступна. Реальные данные зависят от значений параметров, указанных при создании шаблона отчета.

- **Период**

Нажмите на кнопку **Параметры**, чтобы изменить период, за который будет сформирован отчет. Для некоторых типов отчетов кнопка может быть недоступна. Доступные значения:

- между двумя указанными датами;
- от указанной даты до даты создания отчета;
- от даты создания отчета минус указанное количество дней до даты создания отчета.

- **Включать данные подчиненных и виртуальных Серверов администрирования**

Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

По умолчанию параметр включен.

- **До уровня вложенности**

Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию Серверов администрирования,

расположенных на более низких уровнях вложенности дерева.

- **Интервал ожидания данных (мин)**

Сервер администрирования, для которого создан шаблон отчета, ожидает данные от подчиненных Серверов администрирования в течение указанного времени для создания отчета. Если данные не получены от подчиненного Сервера администрирования в течение указанного интервала времени, отчет запускается в любом случае. Вместо фактических данных в отчете отображаются данные, полученные из кеша (если включен параметр **Кешировать данные с подчиненных Серверов администрирования**), или в противном случае **N/A** (Недоступно).

По умолчанию время ожидания составляет 5 минут.

- **Кешировать данные с подчиненных Серверов администрирования**

Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

Включение этого параметра позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

По умолчанию параметр выключен.

- **Период обновления данных в кеше (ч)**

Подчиненные Серверы администрирования через заданные интервалы времени (указанные в часах) передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Вы можете указать этот период в часах. Если установлено значение 0, данные передаются только во время генерации отчета.

По умолчанию указано значение 0.

- **Передавать подробную информацию с подчиненных Серверов администрирования**

В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все данные в одном отчете.

Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

По умолчанию параметр выключен.

- **Вкладка Столбцы**

Выберите поля, которые будут отображаться в отчете. С помощью кнопок **Вверх** и **Вниз** измените порядок отображения полей. С помощью кнопок **Добавить** и **Изменить** укажите, будет ли информация в отчете фильтроваться или сортироваться по выбранным полям.

В разделе **Фильтры детальных полей** вы также можете нажать на кнопку **Преобразовать фильтры**, чтобы начать использовать расширенный формат фильтрации. Этот формат позволяет комбинировать условия фильтрации, указанные в различных полях, с помощью логического ИЛИ. После нажатия на кнопку **Преобразовать фильтры**, справа открывается панель. Нажмите на кнопку **Преобразовать фильтры**, подтверждающую отзыв лицензии. Теперь вы можете определить преобразованный фильтр с условиями из раздела **Детальные данные**, которые применяются с помощью логического ИЛИ.

Преобразование отчета в формат, поддерживающий сложные условия фильтрации, сделает его несовместимым с предыдущими версиями Kaspersky Security Center (11 и ниже). Также в преобразованном отчете не будет данных с подчиненных Серверов администрирования с несовместимыми версиями.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

6. Закройте окно **Редактирование отчета <Название отчета>**.

Измененный шаблон отчета появится в списке шаблонов отчетов.

Экспорт отчета в файл

Вы можете экспортировать отчет в файл формата XML, HTML или PDF.

► *Чтобы экспортировать отчет в файл:*

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Установите флажок рядом с названием отчета, который требуется экспортировать в файл.
3. Нажмите на кнопку **Экспортировать отчет**.
4. В открывшемся окне измените имя файла отчета в поле **Имя**. По умолчанию имя файла совпадает с именем выбранного шаблона отчета.
5. Выберите тип файла отчета: XML, HTML или PDF.
6. Нажмите на кнопку **Экспортировать отчет**.

Отчет будет загружен, в выбранном формате, в папку по умолчанию, на ваше устройство, или откроется стандартное окно **Сохранить как** в вашем браузере, чтобы вы могли сохранить файл в нужном вам месте.

Отчет будет сохранен в файл.

См. также:

| Сценарий: мониторинг и отчеты [1466](#)

Генерация и просмотр отчета

► *Чтобы сформировать и просмотреть отчет:*

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.

2. Нажмите на имя шаблона отчета, который вы хотите использовать для создания отчета.
Отображается сгенерированный отчет с использованием выбранного шаблона.

Данные отчета отображаются в соответствии с языком локализации Сервера администрирования.

В отчете отображаются следующие данные:

- На вкладке **Сводная информация**:
 - тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
 - графическая диаграмма с наиболее характерными данными отчета;
 - сводная таблица с вычисляемыми показателями отчета.
- На вкладке **Подробнее** отобразится таблица с подробными данными отчета.

См. также:

Сценарий: обновление приложений сторонних производителей	499
Сценарий: мониторинг и отчеты	1466

Создание задачи рассылки отчета

Можно создать задачу рассылки выбранных отчетов.

► *Чтобы создать задачу рассылки отчета:*

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Установите флажки рядом с шаблонами отчетов, на основе которых вы хотите сформировать задачу рассылки отчетов.
3. Нажмите на кнопку **Создать задачу рассылки отчетов**.
Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. На шаге мастера **Параметры новой задачи** введите название задачи.
Название задачи по умолчанию – **Рассылка отчетов**. Если задача с таким названием уже существует, к названию задачи добавляется порядковый номер (<N>).
5. На шаге мастера **Конфигурация отчета** укажите следующие параметры:
 - a. Шаблоны отчетов, рассылаемых задачами.
 - b. Формат отчета: HTML, XLS или PDF.

Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на Сервер администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.

- c. Будут ли отчеты рассылаться по электронной почте, а также параметры почтовых уведомлений.
Вы можете указать до 20 адресов электронной почты. Чтобы разделить адреса электронной почты, нажмите на клавишу **Enter**. Вы также можете вставить список адресов электронной почты, разделенных запятыми, и нажать на клавишу **Enter**.
 - d. Будут ли отчеты сохраняться в папку, будут ли перезаписываться сохраненные ранее отчеты в этой папке и будет ли использоваться отдельная учетная запись для доступа к папке (для папки общего доступа).
6. На шаге мастера **Настройка расписания запуска задачи** выберите расписание запуска задачи.

Доступны следующие варианты расписания запуска задачи:

- **Вручную**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна приложения Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Каждые N минут**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N дней**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Ежемесячно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрывающимся списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** –

текущее системное время устройства.

- **В указанные дни**
- **При обнаружении вирусной атаки**

Если в раскрываемся списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемся списком можно выбрать приложения, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемся списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемся списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемся списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

7. На этом шаге мастера настройте другие параметры расписания запуска задачи:

- В разделе **Расписание задачи** проверьте или перенастройте ранее выбранное расписание и установите период, дни месяца или недели, задайте условие вирусной атаки или выполнение другой задачи в качестве запуска задачи. В этом разделе также можно указать время запуска, если выбрано подходящее расписание.
- В разделе **Дополнительные параметры** укажите следующие параметры:

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу

администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка приложения, Исправление уязвимостей).

- **Остановить, если задача выполняется дольше**

По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

8. На шаге мастера **Выбор учетной записи для запуска задачи** укажите учетные данные учетной записи, которая используется для запуска задачи.
9. Если требуется изменить другие параметры задачи после ее создания, на шаге мастера **Завершение создания задачи** включите параметр **Открыть окно свойств задачи после ее создания**. По умолчанию параметр включен.
10. Нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

Будет создана задача отправки отчета. Если параметр **Открыть окно свойств задачи после ее создания** включен, откроется окно параметров задачи.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Удаление шаблонов отчетов

► Чтобы удалить шаблоны отчетов:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Установите флажки напротив шаблонов отчетов, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**, чтобы подтвердить свой выбор.

Выбранные шаблоны отчетов будут удалены. Если эти шаблоны отчетов были включены в задачи рассылки отчетов, они также будут удалены из этих задач.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

События и выборки событий

В этом разделе содержится информация о событиях и выборках событий, о типах событий, возникших в компонентах Kaspersky Security Center, и об управлении блокировкой частых событий.

Использование выборок событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center Web Console.

Выборки событий доступны в Kaspersky Security Center Web Console в разделе **Мониторинг и отчеты** → **Выборки событий**.

По умолчанию выборки событий включают информацию за последние семь дней.

Kaspersky Security Center имеет набор выборок (предопределенных) по умолчанию:

- События с разным уровнем важности:

- **Критические события.**
- **Отказ функционирования.**
- **Предупреждения.**
- **Информационные сообщения.**
- **Запросы пользователей** (события управляемых приложений).
- **Последние события** (за последнюю неделю).
- **События аудита** (см. раздел "**Информационные события Сервера администрирования**" на стр. [1525](#)).

Вы можете также создавать и настраивать дополнительные пользовательские выборки событий (см. раздел "Создание выборки событий" см. стр. [1485](#)). В пользовательских выборках вы можете фильтровать события по свойствам устройств, в которых они возникли (по именам устройств, IP-диапазонам и группам администрирования), по типам событий и уровням важности, по названию приложения и компонента, а также по временному интервалу. Также можно включить результаты задачи в область поиска. Вы также можете использовать поле поиска, в котором можно ввести слово или несколько слов. Отображаются все события, содержащие любые введенные слова в любом месте их свойств (таких как имя события, описание, имя компонента).

Как для предопределенных выборок, так и для пользовательских выборок вы можете ограничить количество отображаемых событий или количество записей для поиска. Оба варианта влияют на время, за которое Kaspersky Security Center отображает события. Чем больше база данных, тем более трудоемким может быть процесс.

Вы можете выполнить следующее:

- Изменить параметры выборки событий (см. раздел "Изменение выборки событий" см. стр. [1486](#)).
- Сгенерировать выборки событий (см. раздел "Просмотр списка выборки событий" см. стр. [1486](#)).
- Просмотреть сведения о выбранных выборках событий (см. раздел "Просмотр информации о событии" см. стр. [1488](#)).
- Удалить выборки событий (см. раздел "Удаление выборок событий" см. стр. [1490](#)).
- Удалить события из базы данных Сервера администрирования (см. раздел "Удаление событий" см. стр. [1489](#)).

См. также:

Выборки устройств.....	1218
Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console	985

Создание выборки событий

► Чтобы создать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Новая выборка событий** укажите параметры новой выборки событий. Параметры можно указать в нескольких разделах этого окна.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Откроется окно подтверждения.

5. Чтобы просмотреть результат выборки событий, установите флажок **Перейти к результатам выборки**.

6. Нажмите на кнопку **Сохранить**, чтобы подтвердить создание выборки событий.

Если был установлен флажок **Перейти к результатам выборки**, результат выборки событий будет отображен на экране. В противном случае новая выборка событий появится в списке выборок событий.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Изменение выборки событий

► Чтобы изменить выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется изменить.
3. Нажмите на кнопку **Свойства**.
Откроется окно свойств выборки событий.
4. Отредактируйте свойства выборки событий.

Для стандартной выборки событий можно редактировать свойства только на следующих вкладках: **Общие** (за исключением имени выборки), **Время** и **Права доступа**.

Для пользовательских выборок можно изменять все свойства.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная выборка событий отображается в списке.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Просмотр списка выборки событий

► Просмотр выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется запустить.
3. Выполните одно из следующих действий:

- Чтобы настроить сортировку для результатов выборки событий:
 - a. Нажмите на кнопку **Изменить сортировку и запустить**.
 - b. В отобразившемся окне **Изменить сортировку для выборки событий** укажите параметры сортировки.
 - c. Нажмите на имя выборки.
- В противном случае, если вы хотите просмотреть список событий так, как они хранятся на Сервере администрирования, нажмите на название выборки.

Отобразится результат выборки событий.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Экспорт выборки событий

Kaspersky Security Center позволяет сохранить выборку событий и ее параметры в файл KLO. Вы можете использовать файл KLO для импорта сохраненной выборки событий (см. раздел "Импорт выборки событий" см. стр. 1487) как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Обратите внимание, что можно удалять только определенные пользователем выборки событий. Набор выборок событий, заданных по умолчанию в Kaspersky Security Center (предопределенные выборки), не может быть сохранен в файл.

► Чтобы экспортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется экспортировать.
Невозможно экспортировать несколько выборок событий одновременно. Если вы выберете более одной выборки, кнопка **Экспортировать** будет неактивна.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя и путь к файлу выборки событий, а затем нажмите на кнопку **Сохранить**.
Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл выборки событий автоматически сохраняется в папку **Загрузки**.

Импорт выборки событий

Kaspersky Security Center позволяет импортировать выборку событий из файла KLO. Файл KLO содержит экспортированную выборку событий (см. раздел "Экспорт выборки событий" см. стр. [1487](#)) и ее параметры.

► Чтобы импортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Нажмите на кнопку **Импортировать**, чтобы выбрать файл выборки событий, который вы хотите импортировать.
3. В открывшемся окне укажите путь к файлу KLO и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл выборки событий.

Начнется обработка выборки событий.

Появится уведомление с результатами импорта. Если выборка событий импортирована, вы можете перейти по ссылке **Просмотреть сведения об импорте**, чтобы просмотреть свойства выборки.

После успешного импорта выборка событий отображается в списке выборок. Также импортируются параметры выборки событий.

Если имя новой импортированной выборки событий идентично имени существующей выборки, имя импортированной выборки расширяется с помощью окончания вида (**<порядковый номер>**), например: **(1)**, **(2)**.

Просмотр информации о событии

► Чтобы просмотреть детальную информацию о событии:

1. Запустите выборку событий (см. раздел "Просмотр списка выборки событий" см. стр. [1486](#)).
2. Нажмите на требуемое событие.

Откроется окно **Свойства события**.

3. В открывшемся окне можно выполнить следующие действия:
 - Просмотреть информацию выбранного события.
 - Перейти к следующему или к предыдущему событию в списке – результате выборки событий.
 - Перейти к устройству, на котором возникло событие.
 - Перейти к группе администрирования, содержащей устройство, на котором возникло событие.
 - Для события, связанного с задачей, перейдите в свойства задачи.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Экспорт событий в файл

► Чтобы экспортировать события в файл:

1. Запустите выборку событий (см. раздел "Просмотр списка выборки событий" см. стр. [1486](#)).
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **Экспортировать в файл**.

Выбранные события экспортированы в файл.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Просмотр истории объекта из события

Из события создания или события изменения объекта, которое поддерживает управление ревизиями, вы можете перейти к истории ревизий объекта.

► Чтобы просмотреть историю объекта из события:

1. Запустите выборку событий (см. раздел "Просмотр списка выборки событий" см. стр. [1486](#)).
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **История ревизий**.

Откроется история ревизий объекта.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Удаление событий

► Чтобы удалить одно или несколько событий:

1. Запустите выборку событий (см. раздел "Просмотр списка выборки событий" см. стр. [1486](#)).
2. Установите флажки рядом с требуемыми событиями.
3. Нажмите на кнопку **Удалить**.

Выбранные события удалены и не могут быть восстановлены.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Удаление выборок событий

Можно удалять только пользовательские выборки событий. Предопределенные выборки событий невозможно удалить.

► Чтобы удалить выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Установите флажки напротив выборок событий, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Выборка событий будет удалена.

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Настройка срока хранения события

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Возможно, вам нужно хранить некоторые события в течение более длительного или более короткого периода, чем указано по умолчанию. Вы можете изменить срок хранения события по умолчанию.

Если вас не интересует сохранение каких-либо событий в базе данных Сервера администрирования, вы можете выключить соответствующий параметр в политике Сервера администрирования, политике приложения "Лаборатории Касперского" или в свойствах Сервера администрирования (только для событий Сервера администрирования). Это уменьшит количество типов событий в базе данных.

Чем больше срок хранения события, тем быстрее база данных достигает максимального размера. Однако более длительный срок хранения события позволяет выполнять задачи мониторинга и просматривать отчеты в течение более длительного интервала времени.

► Чтобы задать срок хранения события в базе данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Выполните одно из следующих действий:
 - Чтобы настроить срок хранения событий Агента администрирования или управляемого приложения "Лаборатории Касперского" нажмите на имя соответствующей политики.
Откроется страница свойств политики.

- Чтобы настроить события Сервера администрирования, в главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Если у вас есть политика для Сервера администрирования, вы можете нажать на название этой политики.

Откроется страница свойств Сервера администрирования (или страница свойств политики Сервера администрирования).

3. Выберите вкладку **Настройка событий**.

Отображается раздел **Критическое** со списком связанных событий.

4. Выберите раздел **Отказ функционирования**, **Предупреждение** или **Информационное сообщение**.
5. В списке типов событий на правой панели перейдите по ссылке с названием события, срок хранения которого вы хотите изменить.
В открывшемся окне в разделе **Регистрация событий** включите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.
6. В поле редактирования под переключателем укажите количество дней для сохранения события.
7. Если вы не хотите сохранять событие в базе данных Сервера администрирования, выключите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.

Если вы настраиваете события Сервера администрирования в окне свойств Сервера администрирования и если параметры событий заблокированы в политике Сервера администрирования Kaspersky Security Center, вы не сможете изменить значение срока хранения события.

8. Нажмите на кнопку **ОК**.

Окно свойств политики закроется.

Теперь, когда Сервер администрирования получает и сохраняет события выбранного типа, они будут иметь измененный срок хранения. Сервер администрирования не изменяет срок хранения ранее полученных событий.

События компонентов Kaspersky Security Center

Каждый компонент Kaspersky Security Center имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования Kaspersky Security Center, Агенте администрирования и Сервере iOS MDM. Типы событий, которые возникают в приложениях "Лаборатории Касперского", в этом разделе не перечислены.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)) в свойствах Сервера администрирования.

Структура данных описания типа события

Для каждого типа событий отображаются его имя, идентификатор, буквенный код, описание и время хранения по умолчанию.

- **Отображаемое имя типа события.** Этот текст отображается в Kaspersky Security Center, когда вы настраиваете события и при их возникновении.
- **Идентификатор типа события.** Этот цифровой код используется при обработке событий с использованием инструментов анализа событий сторонних производителей.
- **Тип события** (буквенный код). Этот код используется при просмотре и обработке событий с использованием публичных представлений базы данных Kaspersky Security Center и при экспорте событий в SIEM-системы.
- **Описание.** Этот текст содержит описание ситуации при возникновении события и описание того, что вы можете сделать в этом случае.
- **Срок хранения по умолчанию.** Это количество дней, в течение которых событие хранится в базе данных Сервера администрирования и отображается в списке событий Сервера администрирования. После окончания этого периода событие удаляется. Если значение времени хранения события указано 0, такие события регистрируются, но не отображаются в списке событий Сервера администрирования. Если вы настроили хранение таких событий в журнале событий операционной системы, вы можете найти их там.

Можно изменить время хранения событий:

- Консоль администрирования: Настройка срока хранения события.
- Kaspersky Security Center Web Console: Настройка срока хранения события (см. стр. [1490](#)).

Другие данные могут включать следующие поля:

- **event_id:** уникальный номер события в базе данных, генерируемый и присваиваемый автоматически. Его не нужно путать с **Идентификатором типа события**.
- **task_id:** идентификатор задачи, в результате выполнения которой возникло событие (если такая есть).
- **severity:** один из следующих уровней важности (в порядке возрастания важности):
 - 0) Недопустимый уровень важности.
 - 1) Информационное.
 - 2) Предупреждение.
 - 3) Ошибка.
 - 4) Критическое.

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

В этом разделе

Критические события Сервера администрирования	638
События отказа функционирования Сервера администрирования	646
События предупреждения Сервера администрирования	652
Информационные события Сервера администрирования	1525

Критические события Сервера администрирования

В таблице ниже приведены типы событий Сервера администрирования Kaspersky Security Center с уровнем важности **Критическое**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)) в свойствах Сервера администрирования.

Если вы указали порт в окне свойств Сервера администрирования в Консоли администрирования, Kaspersky Security Center публикует его метрики и критические события, которые будет получать Prometheus (система мониторинга и оповещения). Prometheus получает метрики и критические события, а затем генерирует алерты для каждого события.

Таблица 95. Критические события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионное ограничение превышено	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования). Kaspersky Security Center определяет правила генерации событий при превышении лицензионного ограничения.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Вирусная атака	26 (для компонента Защита от файловых угроз)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования. • Создайте более строгую политику, которая будет активирована, или создайте задачу, которая будет запускаться при возникновении этого события.	180 дней
Вирусная атака	27 (для компонента Защита от почтовых угроз)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования. • Создайте более строгую политику, которая будет активирована, или создайте задачу, которая будет запускаться при	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			возникновении этого события.	
Вирусная атака	28 (для сетевого экрана)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования. • Создайте более строгую политику, которая будет активирована, или создайте задачу, которая будет запускаться при возникновении этого события.	180 дней
Устройство стало неуправляемым	4111	KLSRV_HOST_OUT_CONTROL	События этого типа возникают, если управляемое устройство видимо в сети, но не подключено к Серверу администрирования в течение заданного периода. Определите, что мешает правильной работе Агента администрирования на устройстве. Возможные причины могут включать проблемы сети и удаление Агента администрирования с устройства.	180 дней
Статус устройства "Критический"	4113	KLSRV_HOST_STATUS_CRITICAL	События этого типа возникают, если управляемому устройству назначен статус	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			<i>Критический.</i> Вы можете настроить условия (см. раздел "Настройка переключения статусов устройств" на стр. 766) при выполнении которых, статус устройства изменяется на <i>Критический</i> .	
Файл ключа добавлен в список запрещенных	4124	KLSRV_LICENSE_BLACKLISTED	События этого типа возникают, если "Лаборатория Касперского" добавила код активации или лицензионный ключ, который вы используете, в запрещенный список. Обратитесь в Службу технической поддержки для получения подробной информации.	180 дней
Режим ограниченной функциональности	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	События этого типа возникают, если Kaspersky Security Center начинает работать в режиме базовой функциональности, без поддержки Управления мобильными устройствами и Системного администрирования. Ниже приведены причины и соответствующие ответы на событие: - Срок действия лицензии истек. Предоставьте лицензию на полную функциональность Kaspersky Security Center (добавьте действительный код активации или файл ключа на Сервер администрирования). - Сервер администрирования управляет большим количеством устройств, чем может	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			использоваться по предоставленной лицензии. Переместите устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера (если лицензионное ограничение другого Сервера не превышено).	
Срок действия лицензии скоро истекает	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	События этого типа возникают, если приближается дата окончания срока действия коммерческой лицензии. Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии. События этого типа публикуются за 30 дней, 15 дней, 5 дней и 1 день, до истечения срока действия лицензии. Вы не можете изменить количество дней. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня. После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности. Вы можете ответить на событие следующими способами: Убедитесь, что резервный	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			лицензионный ключ добавлен на Сервер администрирования. Если вы используете подписку, продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена.	
Срок действия сертификата истек	4132	KLSRV_CERTIFICATE_EXPIRED	События этого типа возникают, если истекает срок действия сертификата Сервера администрирования для Управления мобильными устройствами. Вам необходимо обновить сертификат, срок действия которого истекает.	180 дней
Обновления модулей приложений "Лаборатории Касперского" отозваны	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	События этого типа возникают, если обновления (см. раздел "Одобрение и отклонение обновлений программного обеспечения" см. стр. 1363) были отозваны техническими специалистами "Лаборатории Касперского", например, по причине их замены на более новые версии. Для таких обновлений отображается статус <i>Отозвано</i> . Событие не относится к патчам Kaspersky Security Center и не относится к модулям управляемых приложений "Лаборатории Касперского". Событие содержит причину, из-за которой обновления не установлены.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Аудит: Не удалось выполнить экспорт в SIEM-систему	5130	KLAUD_EV_SIEM_EXPORT_ERROR	События этого типа возникают при сбое экспорта событий в SIEM-систему из-за ошибки соединения с SIEM-системой.	180 дней

См. также:

События отказа функционирования Сервера администрирования	646
Информационные события Сервера администрирования	1525
События предупреждения Сервера администрирования	652
О событиях в Kaspersky Security Center	881

События отказа функционирования Сервера администрирования

В таблице ниже приведены типы событий Сервера администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)) в свойствах Сервера администрирования.

Таблица 96. События отказа функционирования Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Ошибка времени выполнения	4125	KLSRV_RUNTIME_ERROR	События этого типа возникают из-за неизвестных проблем. Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением. Подробную информацию о событии можно найти в его описании.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных приложений превышено ограничение числа установок	4126	KLSRV_INVLICPROD_EXCEDED	Сервер администрирования генерирует события такого типа периодически (каждый час). События этого типа возникают, если в Kaspersky Security Center вы управляете лицензионными ключами приложений сторонних производителей и если количество установок превысило заданное в лицензионном ключе приложения стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите приложение стороннего производителя с устройств, на которых оно не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений. В группу лицензионных приложений входят приложения сторонних производителей, отвечающие заданным вами критериям.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось выполнить опрос облачного сегмента	4143	KLSRV_KLCLOUD_SCAN_ERROR	События этого типа возникают, если Сервер администрирования не может опросить сегмент сети в облачном окружении. Прочтите информацию в описании события и отреагируйте соответствующим образом.	Не хранится
Не удалось выполнить копирование обновлений в заданную папку	4123	KLSRV_UPD_REPL_FAIL	События этого типа возникают, если обновления программного обеспечения копируются в общую папку (или папки). Вы можете ответить на событие следующими способами: • Проверьте, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись. • Проверьте, не были ли изменены имя пользователя и/или пароль к папке (к папкам). • Проверьте подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и модулей приложений.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Нет свободного места на диске	4107	KLSRV_DISK_FULL	События этого типа возникают, если на жестком диске устройства, на котором установлен Сервер администрирования, заканчивается дисковое пространство. Освободите дисковое пространство на устройстве.	180 дней
Общая папка недоступна	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	События этого типа возникают, если общая папка Сервера администрирования недоступна. Вы можете ответить на событие следующими способами: • Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен. • Проверьте, были ли изменены имя пользователя и/или пароль к папке. • Проверьте подключение к сети.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
База данных Сервера администрирования недоступна	4109	KLSRV_DATABASE_UNAVAILABLE	События этого типа возникают, если база Сервера администрирования становится недоступной. Вы можете ответить на событие следующими способами: • Проверьте, доступен ли удаленный сервер, на котором установлен SQL-сервер. • Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования. Например, из-за профилактических работ удаленный сервер с установленным SQL Server может быть недоступен.	180 дней

Недостаточно места в базе данных Сервера администрирования	4110	KLSRV_DATABASE_F ULL	События этого типа возникают, если нет свободного места в базе Сервера администрирования. Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие: • Вы используете SQL Server Express Edition: Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования превысила ограничение размера базы данных. Ограничьте количество событий, хранящихся в базе данных Сервера администрирования (см. раздел "Настройка количества событий в хранилище событий" на стр. 1018). В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль приложений в базе	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			данных Сервера администрирования. Вы используете СУБД, отличную от SQL Server Express Edition: Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования (см. раздел "Настройка количества событий в хранилище событий" на стр. 1018). Сократите список событий для хранения в базе данных Сервера администрирования (см. раздел "Настройка срока хранения события" см. стр. 1490). Просмотрите информацию о выборе СУБД.	

См. также:

Критические события Сервера администрирования	638
Информационные события Сервера администрирования	1525
События предупреждения Сервера администрирования	652
О событиях в Kaspersky Security Center	881

События предупреждения Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте

общие параметры уведомлений (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)) в свойствах Сервера администрирования.

Таблица 97. События предупреждения Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Обнаружено получение частого события		KLSRV_EVENT_SPAM_EVENTS_DETECTED	События этого типа возникают, если Сервер администрирования регистрирует частые события на управляемом устройстве. Дополнительную информацию см. в следующих разделах: Блокировка частых событий.	90 дней

Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHEC K_100_110	Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии составляет от 100% до 110% от общего количества единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования). Kaspersky Security Center определяет правила генерации событий при превышении лицензионного ограничения.	90 дней
Устройство долго не проявляет	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	События этого типа возникают, если управляемое устройство	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
активности в сети			неактивно в течение некоторого времени. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: - Удалите устройство из списка управляемых устройств вручную. - Укажите интервал, по истечении которого создается событие Устройство долго не проявляет активности в сети с помощью Консоли администрирования или с помощью Kaspersky Security Center Web Console (см. раздел "Просмотр и настройка действий, когда устройство неактивно" на стр. 1203). - Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Консоли администрирования или Kaspersky Security Center Web Console (см. раздел "Просмотр и настройка действий, когда устройство неактивно" на стр. 1203).	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Конфликт имен устройств	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания приложений на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве. Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска на эталонном устройстве.	90 дней
Статус устройства "Предупреждение"	4114	KLSRV_HOST_STATUS_WARNING	События этого типа возникают, если управляемому устройству назначен статус <i>Предупреждение</i>. Вы можете настроить условия (см. раздел "Настройка переключения статусов устройств" на стр. 766) при выполнении которых, статус устройства изменяется на <i>Предупреждение</i>.	90 дней

Для одной из групп лицензионных приложений скоро будет превышено ограничение числа установок	4127	KLSRV_INVLICPROD_FILLED	События этого типа возникают, если количество установок приложений сторонних производителей, включенных в группу лицензионных приложений, достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Сертификат запрошен	4133	KLSRV_CERTIFICATE_REQUESTED	События этого типа возникают, если не удастся автоматически перевыпустить сертификат для Управления мобильными устройствами. Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: - Автоматический перевыпуск был инициирован для сертификата, для которого параметр Автоматически перевыпускать сертификат, если это возможно. Это могло произойти из-за ошибки, которая возникла при создании сертификата. Может потребоваться перевыпуск сертификата вручную. - Если вы используете интеграцию с инфраструктурой открытых ключей, причиной может быть отсутствие атрибута SAM-Account-Name учетной записи, которая используется для интеграции с PKI и для выпуска сертификата. Просмотрите свойства учетной записи.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Сертификат удален	4134	KLSRV_CERTIFICATE_REMOVED	События этого типа возникают, если администратор удаляет сертификат любого типа (общий, почтовый, VPN) для Управления мобильными устройствами. После удаления сертификата мобильные устройства, подключенные по этому сертификату, не смогут подключиться к Серверу администрирования. Это событие может быть полезно при исследовании неисправностей, связанных с Управлением мобильными устройствами.	90 дней
Срок действия APNs-сертификата истек	4135	KLSRV_APN_CERTIFICATE_EXPIRED	События этого типа происходят, если истекает срок действия APNs-сертификата. Вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM.	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия APNs-сертификата истекает	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	События этого типа возникают, если до истечения срока действия APNs-сертификата остается менее 14 дней. При истечении срока действия APNs-сертификата, вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. Рекомендуется запланировать обновление APNs-сертификата до истечения срока его действия.	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-сообщение на мобильное устройство	4138	KLSRV_GCM_DEVICE_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Firebase Cloud Messaging (FCM) для подключения к управляемым мобильным устройствам с операционной системой Android, а FCM-сервер не может обработать некоторые запросы, полученные от Сервера администрирования. Это означает, что некоторые управляемые мобильные устройства не будут получать push-уведомление. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Firebase https://firebase.google.com/docs/cloud-messaging/http-server-ref (см. главу "Downstream message error response codes").	90 дней

HTTP-ошибка при отправке FCM-сообщения на FCM-сервер	4139	KLSRV_GCM_HTTP_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Firebase Cloud Messaging (FCM) для подключения управляемых мобильных устройств с операционной системой Android, а FCM-сервер возвращает запрос Серверу администрирования с кодом HTTP, отличным от 200 (OK). Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Проблемы на стороне FCM-сервера. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Firebase https://firebase.google.com/docs/cloud-messaging/http-server-ref (см. главу "Downstream message error response codes"). • Проблемы на стороне прокси-сервера (если вы используете прокси-сервер). Прочтите HTTP код в описании события и ответьте соответствующим образом.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-сообщение на FCM-сервер	4140	KLSRV_GCM_GENERAL_ERROR	События этого типа возникают из-за непредвиденных ошибок на стороне Сервера администрирования при работе с HTTP-протоколом Firebase Cloud Messaging. Прочтите информацию в описании события и отреагируйте соответствующим образом. Если вы не можете найти решение проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки "Лаборатории Касперского".	90 дней
Мало свободного места на жестком диске	4105	KLSRV_NO_SPACE_ON_VOLUMES	События этого типа возникают, если на устройстве, на котором установлен Сервер администрирования, почти закончилось дисковое пространство. Освободите дисковое пространство на устройстве.	90 дней

Мало свободного места в базе Сервера администрирования	4106	KLSRV_NO_SPACE_IN_DATABASE	События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие. Вы используете SQL Server Express Edition: • Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования достигла ограничения размера базы данных. • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования (см. раздел "Настройка количества событий в хранилище событий" на стр. 1018). • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
			Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. Вы используете СУБД, отличную от SQL Server Express Edition: • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования (см. раздел "Настройка количества событий в хранилище событий" на стр. 1018). • Сократите список событий для хранения в базе данных Сервера администрирования (см. раздел "Настройка срока хранения события" см. стр. 1490). Просмотрите информацию о выборе СУБД.	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Разорвано соединение с подчиненным Сервером администрирования	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с подчиненным Сервером администрирования. Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Разорвано соединение с главным Сервером администрирования	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с главным Сервером администрирования. Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен главный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Зарегистрированы новые обновления модулей приложений "Лаборатории Касперского"	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	События этого типа возникают, если Сервер администрирования регистрирует новые обновления приложений "Лаборатории Касперского", установленных на управляемых устройствах, для установки которых требуется одобрение. Одобрите или отклоните обновления с помощью Консоли администрирования или Kaspersky Security Center Web Console (см. раздел "Одобрение и отклонение обновлений программного обеспечения" на стр. 1363).	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Превышено ограничение числа событий, началось удаление событий из базы данных	4145	KLSRV_EVP_DB_TRUNCATING	События такого типа возникают, если удаление старых событий из базы данных Сервера администрирования началось после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. Вы можете ответить на событие следующими способами: • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования (см. раздел "Настройка количества событий в хранилище событий" на стр. 1018). • Сократите список событий для хранения в базе данных Сервера администрирования (см. раздел "Настройка срока хранения события" см. стр. 1490).	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Превышено ограничение числа событий, удалены события из базы данных	4146	KLSRV_EVP_DB_TRUNCATE D	События такого типа возникают, если старые события удалены из базы данных Сервера администрирования после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. Вы можете ответить на событие следующими способами: • Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования (см. раздел "Настройка количества событий в хранилище событий" на стр. 1018). • Сократите список событий для хранения в базе данных Сервера администрирования (см. раздел "Настройка срока хранения события" см. стр. 1490).	Не хранится

См. также:

Критические события Сервера администрирования	638
События отказа функционирования Сервера администрирования	646
Информационные события Сервера администрирования	1525
О событиях в Kaspersky Security Center	881

Информационные события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)) в свойствах Сервера администрирования.

Таблица 98. Информационные события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Лицензионный ключ использован более чем на 90%	4097	KLSRV_EV_LICENSE_CHECK_90	30 дней	
Обнаружено новое устройство	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 дней	
Устройство автоматически добавлено в группу	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 дней	
Устройство было автоматически перемещено с помощью правила	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 дней	
Устройство удалено из группы: долгое отсутствие активности в сети	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 дней	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Для одной из групп лицензионных приложений число разрешенных установок исчерпано более чем на 95%	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 дней	
Появились файлы для отправки на анализ в "Лабораторию Касперского"	4131	KLSRV_APS_FILE_APPEARED	30 дней	
Идентификатор экземпляра FCM мобильного устройства изменен	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 дней	
Обновления успешно скопированы в заданную папку	4122	KLSRV_UPD_REPL_OK	30 дней	
Установлено соединение с подчиненным Сервером администрирования	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 дней	
Установлено соединение с главным Сервером администрирования	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 дней	
Базы обновлены	4144	KLSRV_UPD_BASES_UPDATED	30 дней	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Аудит: Подключение к Серверу администрирования	4147	KLAUD_EV_SERVERCONNECT	30 дней	
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	30 дней	Это событие отслеживает изменения в следующих объектах: • группах администрирования; • группах безопасности; • пользователях; • установочных пакетах; • задачах; • политиках; • Серверах; • виртуальных Серверах.
Аудит: Изменение статуса объекта	4150	KLAUD_EV_TASK_STATE_CHANGED	30 дней	Например, это событие возникает, если задача завершилась ошибкой.
Аудит: Изменение параметров группы	4149	KLAUD_EV_ADMGROUP_CHANGED	30 дней	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Аудит: Подключение к Серверу администрирования было прервано	4151	KLAUD_EV_SERVERDISCONNECT	30 дней	
Аудит: Свойства объекта были изменены	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 дней	Это событие отслеживает изменения в следующих параметрах: • пользователь; • лицензия; • Сервер; • виртуальный Сервер.
Аудит: Права пользователя были изменены	4153	KLAUD_EV_OBJECTACLMODIFIED	30 дней	
Аудит: Импорт или экспорт ключей шифрования с Сервера администрирования	5100	KLAUD_EV_DPEKEYSEXPORT	30 дней	

События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

В этом разделе

События отказа функционирования Агента администрирования	670
События предупреждения Агента администрирования	674
Информационные события Агента администрирования	676

События отказа функционирования Агента администрирования

В таблице ниже приведены типы событий Агента администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)) в свойствах Сервера администрирования.

Таблица 99. События отказа функционирования Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Ошибка при установке обновления	7702	KLNAG_EV_PATCH_INSTALL_ERROR	События этого типа возникают, если автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center прошла неуспешно. Событие не относится к обновлениям управляемых приложений "Лаборатории Касперского". Прочтите описание события. Причиной этого события может быть проблема операционной системы Windows на Сервере администрирования. Если в описании упоминается какая-либо проблема конфигурации Windows, устраните эту проблему.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось установить обновление стороннего производителя	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	События этого типа возникают, если используются возможности Системного администрирования и Управления мобильными устройствами, и если обновление программного обеспечения сторонних производителей прошло неуспешно. Проверьте, корректна ли ссылка на приложение стороннего производителя. Прочтите описание события.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось установить обновления Центра обновления Windows	7717	KLNAG_EV_WUA_INSTALL_ERROR	События этого типа возникают, если обновления Центра обновления Windows были unsuccessful. Настройте обновления Microsoft Windows в политике Агента администрирования. Прочтите описание события. Поищите описание ошибки в базе знаний Microsoft. Обратитесь в службу технической поддержки Microsoft, если вы не можете решить проблему самостоятельно.	30 дней
Управление учетными записями: ошибки	7723	KLNAG_EV_USR_MNG_ERR	Общее событие предупреждения.	30 дней
Не удалось восстановить файл sudoers до референсного значения	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Событие содержит описание ошибки замены файла sudoers.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось установить корневые сертификаты	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Событие содержит описание ошибки установки сертификатов.	30 дней
Не удалось удалить корневые сертификаты	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Событие содержит описание ошибки удаления сертификатов.	30 дней

См. также:

События предупреждения Агента администрирования	674
Информационные события Агента администрирования	676

События предупреждения Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)) в свойствах Сервера администрирования.

Таблица 100. События предупреждения Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Возвращено предупреждение во время установки обновления модулей приложений	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 дней
Установка обновления стороннего ПО завершена с предупреждением	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 дней
Установка обновления стороннего программного обеспечения отложена	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 дней
Произошла проблема безопасности	549	GNRL_EV_APP_INCIDENT_OCCURRED	30 дней
Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN	7718	KSNPROXY_STARTED_CONNECTION_FAILED	30 дней
Управление учетными записями: предупреждения	7722	KLNAG_EV_USR_MNG_WARN	30 дней
Обнаружен файл sudoers, который не соответствует референсному значению	7724	KLNAG_EV_SUDOER_DIFFERENT	30 дней

См. также:

События отказа функционирования Агента администрирования[670](#)Информационные события Агента администрирования[676](#)

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)) в свойствах Сервера администрирования.

Таблица 101. Информационные события Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Обновление модулей приложений успешно установлено	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления модулей приложений	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 дней
Установлено приложение	7703	KLNAG_EV_INV_APP_INSTALLED	30 дней
Приложение удалено	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 дней
Установлено наблюдаемое приложение	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 дней
Удалено наблюдаемое приложение	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 дней
Установлено стороннее приложение	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 дней
Новое устройство добавлено	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Устройство удалено	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Обнаружено новое устройство	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство авторизовано	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней
Совместный доступ к рабочему столу Windows: файл был прочитан	7712	KLUSRLOG_EV_FILE_READ	30 дней
Совместный доступ к рабочему столу Windows: файл был изменен	7713	KLUSRLOG_EV_FILE_MODIFIED	30 дней
Совместный доступ к рабочему столу Windows: приложение было запущено	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 дней
Совместный доступ к рабочему столу Windows: предоставлен	7715	KLUSRLOG_EV_WDS_BEGIN	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Совместный доступ к рабочему столу Windows: завершен	7716	KLUSRLOG_EV_WDS_END	30 дней
Обновление для приложений стороннего производителя установлено успешно	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления стороннего ПО	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 дней
Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно	7719	KSNPROXY_STARTED_CON_CHK_OK	30 дней
Прокси-сервер KSN остановлен	7720	KSNPROXY_STOPPED	30 дней

См. также:

События отказа функционирования Агента администрирования	670
События предупреждения Агента администрирования	674

Блокировка частых событий

В этом разделе представлена информация об управлении блокировкой частых событий и об отмене блокировки частых событий.

В этом разделе

О блокировке частых событий	1536
Управление блокировкой частых событий	1537
Отмена блокировки частых событий	1538

О блокировке частых событий

Управляемое приложение, например Kaspersky Endpoint Security для Windows, установленное на одном или нескольких управляемых устройствах, может отправлять на Сервер администрирования множество однотипных событий. Прием частых событий может привести к перегрузке базы данных Сервера администрирования и перезаписи других событий. Сервер администрирования начинает блокировать наиболее частые события, когда количество всех полученных событий превышает установленное

ограничение для базы данных (см. раздел "Настройка количества событий в хранилище событий" на стр. [1018](#)).

Сервер администрирования автоматически блокирует получение частых событий. Вы не можете заблокировать частые события самостоятельно или выбрать, какие события заблокировать.

Чтобы узнать, заблокировано ли событие, вы можете просмотреть список уведомлений или просмотреть, присутствует ли это событие в свойствах Сервера администрирования в разделе **Блокировка частых событий**. Если событие заблокировано, можно выполнить следующие действия:

- Если вы хотите предотвратить перезапись базы данных, вы можете продолжать блокировать (см. раздел "Управление блокировкой частых событий" на стр. [1537](#)) получение событий такого типа.
- Если вы хотите, например, выяснить причину отправки частых событий на Сервер администрирования, вы можете разблокировать (см. раздел "Управление блокировкой частых событий" на стр. [1537](#)) частые события и в любом случае продолжить получение событий этого типа.
- Если вы хотите продолжать получать частые события до тех пор, пока они снова не будут заблокированы, вы можете отменить блокировку (см. раздел "Отмена блокировки частых событий" на стр. [1538](#)) частых событий.

Управление блокировкой частых событий

Сервер администрирования автоматически блокирует получение частых событий, но вы можете разблокировать и продолжать получать частые события. Также можно заблокировать получение частых событий, которые вы разблокировали ранее.

► *Чтобы управлять блокировкой частых событий:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Заблокированные частые события**.
3. В разделе **Заблокированные частые события**:
 - Если вы хотите разблокировать прием частых событий:
 - a. Выберите частые события, который нужно разблокировать, и нажмите на кнопку **Исключить**.
 - b. Нажмите на кнопку **Сохранить**.
 - Если вы хотите заблокировать прием частых событий:
 - a. Выберите частые события, которые вы хотите заблокировать и нажмите на кнопку **Заблокировано**.
 - b. Нажмите на кнопку **Сохранить**.

Сервер администрирования принимает разблокированные частые события и не принимает заблокированные частые события.

См. также:

О блокировке частых событий [1536](#)

Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует эти частые события.

► Чтобы отменить блокировку частых событий:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Заблокированные частые события**.
3. В разделе **Заблокированные частые события** нажмите строку частого события, для которого вы хотите отменить блокировку.
4. Нажмите на кнопку **Отменить блокировку**.

Частое событие удаляется из списка частых событий. Сервер администрирования будет получать события этого типа.

См. также:

О блокировке частых событий [1536](#)

Получение событий от Kaspersky Security для Microsoft Exchange Servers

Информация о событиях при работе управляемых приложений, таких как Kaspersky Endpoint Security для Windows, передается с управляемых устройств и регистрируется в базе данных Сервера администрирования. По умолчанию события от Kaspersky Security для Microsoft Exchange Servers версии 9.0 MR6 и ниже не регистрируются в базе данных Сервера администрирования. Если приложение Kaspersky Security для Microsoft Exchange Servers версии 9.0 MR6 и ниже установлено на управляемых устройствах в вашей организации и вы хотите получать события от этого приложения, включите регистрацию событий этого приложения с помощью утилиты klscflag.

► Чтобы включить регистрацию событий Kaspersky Security для Microsoft Exchange Servers:

1. На устройстве Сервера администрирования запустите командную строку Windows под учетной записью с правами администратора.
2. Измените текущую директорию на папку установки Kaspersky Security Center (обычно это C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).
3. Выполните одну из следующих команд:
 - Для установленного Сервера администрирования на отказоустойчивом кластере Windows Server:

```
klscflag.exe --stp cluster -fset -pv klserver -n
KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
```

- Для Сервера администрирования, установленного на узле отказоустойчивого кластера Kaspersky Security Center:

```
klscflag.exe --stp klloc -fset -pv klserver -n
KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
```

- Для Сервера администрирования, не работающего на кластере:

```
klscflag.exe -fset -pv klserver -n
KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
```

Регистрация событий для Kaspersky Security для Microsoft Exchange Servers включена.

Для Kaspersky Security для Microsoft Exchange Servers вы не можете задать срок хранения событий или выбрать, какие события должны сохраняться в хранилище Сервера администрирования. Вы можете установить максимальное количество событий, которые можно сохранить в хранилище (см. раздел "Настройка количества событий в хранилище событий" на стр. [1018](#)). Этот параметр применяется к событиям, полученным от всех приложений "Лаборатории Касперского".

Уведомления и статусы устройств

В этом разделе содержится информация о том, как просматривать уведомления, настраивать доставку уведомлений, использовать статусы устройств и включать изменение статусов устройств.

В этом разделе

Использование уведомлений	1539
Просмотр экранных уведомлений	1540
О статусах устройства	1542
Настройка переключения статусов устройств	1547
Настройка параметров доставки уведомлений	1549
Уведомление о событиях с помощью исполняемого файла	316

Использование уведомлений

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- экранные уведомления;
- уведомление по SMS;
- уведомление по электронной почте;
- уведомление запуском исполняемого файла или скрипта.

Экранные уведомления

Экранные уведомления предупреждают вас о событиях, сгруппированных по уровням важности (*Критическое уведомление*, *Предупреждающее уведомление*, и *Информационное уведомление*).

Экранные уведомления могут иметь один из двух статусов:

- *Просмотрено*. Это означает, что вы выполнили рекомендованное действие для уведомления или вы назначили этот статус для уведомления вручную.
- *Не просмотрено*. Это означает, что вы не выполнили рекомендуемое действие для уведомления или не назначили этот статус для уведомления вручную.

По умолчанию в список уведомлений входят уведомления со статусом *Не просмотрено*.

Вы можете контролировать сеть вашей организации, просматривая уведомления на экране (см. раздел "Просмотр экранных уведомлений" на стр. [1540](#)) и отвечая на них в режиме реального времени.

Уведомления по электронной почте, SMS и запуском исполняемого файла или скрипта

Kaspersky Security Center позволяет вам контролировать сеть вашей организации, отправляя уведомления о событиях, которые вы считаете важными. Для любого события вы можете настроить уведомления по электронной почте, SMS или запуском исполняемого файла или скрипта (см. раздел "Настройка параметров доставки уведомлений" на стр. [1549](#)).

Получив уведомление по SMS или по электронной почте, вы можете принять решение о своем ответе на событие. Этот ответ должен быть наиболее подходящим для сети вашей организации. Запустив исполняемый файл или скрипт, вы заранее определяете ответ на событие. Вы также можете рассмотреть запуск исполняемого файла или скрипта в качестве основного ответа на событие. После запуска исполняемого файла вы можете предпринять другие шаги для ответа на событие.

Просмотр экранных уведомлений

Вы можете просматривать экранные уведомления тремя способами:

- В разделе **Мониторинг и отчеты** → **Уведомления**. Здесь вы можете просмотреть уведомления, относящиеся к предопределенным категориям.
- В отдельном окне, которое можно открыть независимо от того, какой раздел вы используете в данный момент. В этом случае вы можете отметить уведомления как просмотренные.
- В веб-виджете **Уведомления, выбранные по уровню важности** в разделе **Мониторинг и отчеты** → **Панель мониторинга**. В этом веб-виджете вы можете просматривать только уведомления с уровнями важности *Критическое* и *Предупреждение*.

Вы можете выполнять действия, например, вы можете ответить на событие.

► Чтобы просмотреть уведомления предопределенной категории:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Уведомления**.
На левой панели выбрана категория **Все уведомления**, а справа отображаются все уведомления.
2. На левой панели выберите одну из следующих категорий:
 - **Развертывание**
 - **Устройства**
 - **Защита**

- **Обновления** (сюда входят уведомления о доступных для загрузки приложениях "Лаборатории Касперского" и уведомления о загруженных обновлениях антивирусных баз)
- **Защита от эксплойтов**
- **Сервер администрирования** (это уведомление включает в себя события, относящиеся только к Серверу администрирования)
- **Полезные ссылки** (сюда входят ссылки на ресурсы "Лаборатории Касперского", например, ссылка на Службу технической поддержки "Лаборатории Касперского", на форум "Лаборатории Касперского", на страницу продления лицензии или на Вирусную энциклопедию)
- **Корпоративные новости "Лаборатории Касперского"** (сюда входит информация о выпусках приложений "Лаборатории Касперского").

В списке уведомлений отобразится выбранная категория. Список содержит следующее:

- Значок, относящийся к теме уведомления: развертывание () , защита () , обновления () , управление устройствами () , Защита от эксплойтов () , Сервер администрирования () .
- Уровень важности уведомления. Отображаются уведомления со следующими уровнями важности: **Критические уведомления** () , **Предупреждающие уведомления** () , **Информационные уведомления** . Уведомления в списке сгруппированы по уровню важности.
- **Уведомление** . Здесь содержится описание уведомления.
- **Действие** . Здесь содержится ссылка на быстрое действие, которое рекомендуется выполнить. Например, по этой ссылке вы можете перейти к хранилищу (см. раздел "Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"" см. стр. [1087](#)) и установить приложение безопасности на устройства, просмотреть список устройств или список событий. После того, как вы выполнили рекомендуемое действие для уведомления, этому уведомлению присваивается статус *Просмотрено* .
- **Зарегистрированный статус** . Здесь содержится количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.

► Чтобы просмотреть экранные уведомления в отдельном окне по уровню важности:

1. Нажмите на значок флага () в правом верхнем углу Kaspersky Security Center Web Console.

Если около значка флажка есть красная точка, значит, есть непросмотренные уведомления.

Откроется окно со списком уведомлений. По умолчанию выбрана вкладка **Все уведомления** и отображаются уведомления, сгруппированные по уровням важности: *Критические уведомления* , *Предупреждающие уведомления* и *Информационные уведомления* .

2. Выберите вкладку **Система** .

Отображается список уведомлений с уровнями важности *Критические уведомления* () и *Предупреждающие уведомления* () . Список уведомление включает следующее:

- Цветной индикатор. Критические уведомления отмечены красным. Предупреждающие уведомления отмечены желтым.
- Значок, относящийся к теме уведомления: развертывание () , защита () , обновления () , управление устройствами () , Защита от эксплойтов () , Сервер администрирования () .
- Описание уведомления.

- Значок флажка. Серый флаг используется для уведомлений, которым присвоен статус *Не просмотрено*. Когда вы выбираете серый флаг и назначаете статус *Просмотрено* для уведомления, цвет флажка изменится на белый.
- Ссылка на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
- Количество дней, прошедших с даты регистрации уведомления на Сервере администрирования.

3. Выберите вкладку **Больше**.

Отображается список уведомлений с уровнем важности *Информационное уведомление*.

Структура списка такая же, как и для списка на вкладке **Система** (описание приведено выше). Отличается только отсутствием цветного индикатора.

Вы можете фильтровать уведомления по датам, когда они были зарегистрированы на Сервере администрирования. Используйте флажок **Показать фильтр**, чтобы настроить фильтр.

► Чтобы просмотреть экранные уведомления на веб-виджете:

1. В разделе **Панель мониторинга** выберите **Добавить или восстановить веб-виджет**.
2. В открывшемся окне нажмите на категорию **Другие**, выберите веб-виджет **Уведомления, выбранные по уровню важности** и нажмите на кнопку **Добавить** (см. раздел "Добавление веб-виджета на информационную панель" см. стр. [1470](#)).

Веб-виджет отображается на вкладке **Панель мониторинга**. По умолчанию на веб-виджете отображаются уведомления с уровнем важности *Критическое*.

Вы можете нажать на кнопку **Параметры** на веб-виджете и изменить параметры веб-виджета (см. раздел "Изменение параметров веб-виджета" см. стр. [1472](#)), чтобы просмотреть уведомления с уровнем важности *Предупреждающие уведомления*. Или вы можете добавить другой веб-виджет: **Уведомления, выбранные по уровню важности** с уровнем важности *Предупреждающие уведомления*.

Список уведомлений на веб-виджете ограничен размером и включает только два уведомления. Эти два уведомления относятся к последним событиям.

Список уведомлений веб-виджета включает следующее:

- Значок, относящийся к теме уведомления: развертывание () , защита () , обновления () , управление устройствами () , Защита от эксплойтов () , Сервер администрирования () .
- Описание уведомления со ссылкой на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
- Количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.
- Ссылка на другие уведомления. Перейдите по ссылке к просмотру уведомлений в разделе **Уведомления** в разделе **Мониторинг и отчеты**.

О статусах устройства

Kaspersky Security Center присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Kaspersky Security Center учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky Security Center не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический / Видим в сети*.
- *Предупреждение* или *Предупреждение / Видим в сети*.
- *ОК* или *ОК / Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

Таблица 102. Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи <i>Поиск вредоносного ПО</i> , на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача <i>Поиск вредоносного ПО</i> , ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.

Условие	Описание условия	Доступные значения
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
Обнаружены активные угрозы	Количество необработанных объектов в папке Активные угрозы превышает указанное значение.	Более чем 0 штук.
Требуется перезагрузка	Устройство видимо в сети, но приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.

Условие	Описание условия	Доступные значения
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	- Переключатель выключен. - Переключатель включен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи <i>Поиск уязвимостей и требуемых обновлений</i> на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	- Предельный. - Высокий. - Средний. - Игнорировать, если невозможно закрыть уязвимость. - Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	- Переключатель выключен. - Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней.
Давно не выполнялась проверка обновлений Центра обновления Windows	Не выполнялась задача <i>Синхронизация обновлений Windows Update</i> больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	- Не соответствует политике из-за отказа пользователя (только для внешних устройств). - Не соответствует политике из-за ошибки. - В процессе применения политики – требуется перезагрузка. - Не задана политика шифрования. - Не поддерживается. - В процессе применения политики.

Условие	Описание условия	Доступные значения
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	- Переключатель выключен. - Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	- Переключатель выключен. - Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	- Переключатель выключен. - Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы <i>Критический</i> или <i>Предупреждение</i> меняются на статус <i>ОК</i> , когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ.
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	- Переключатель выключен. - Переключатель включен.

Условие	Описание условия	Доступные значения
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности <i>Остановлено</i> или <i>Сбой</i> и отличается от следующих: <i>Запускается</i> , <i>Выполняется</i> или <i>Приостановлено</i> .	Более чем 0 минут.
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	- Переключатель выключен. - Переключатель включен.

Kaspersky Security Center позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *ОК*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3 дней** клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Если вы обновляете Kaspersky Security Center с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Когда Kaspersky Security Center присваивает устройству статус, для некоторых условий (см. графу "Описание условий") учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *ОК*.

См. также:

Настройка переключения статусов устройств[1547](#)

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

► Чтобы изменить статус устройства на *Критический*:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.

2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В отобразившемся окне свойств выберите вкладку **Статус устройства**.
4. Выберите раздел **Критический**.
5. В блоке **Установить статус "Критический"**, если включите условие, чтобы переключить устройство в состояние *Критическое*.

Вы можете изменить только параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.
7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.
8. Для выбранного условия установите необходимое вам значение.
Не для всех условий можно задать значения.
9. Нажмите на кнопку **ОК**.

При невыполнении заданных условий управляемому устройству присваивается статус *Критический*.

► *Чтобы изменить статус устройства на Предупреждение:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В отобразившемся окне свойств выберите вкладку **Статус устройства**.
4. Выберите раздел **Предупреждение**.
5. В блоке **Установить статус "Предупреждение"**, если включите условие, чтобы переключить устройство в состояние *Предупреждение*.

Вы можете изменить только параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.
7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.
8. Для выбранного условия установите необходимое вам значение.
Не для всех условий можно задать значения.
9. Нажмите на кнопку **ОК**.

При невыполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

См. также:

Уведомления и статусы устройств.....	1539
О статусах устройства.....	1205
Сценарий: мониторинг и отчеты.....	1466
Сценарий: настройка защиты сети.....	403

Настройка параметров доставки уведомлений

Вы можете настроить уведомления о событиях, возникающих в Kaspersky Security Center. В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- Электронная почта – при возникновении события приложение Kaspersky Security Center посылает уведомление на указанные адреса электронной почты.
- SMS – при возникновении события приложение Kaspersky Security Center посылает уведомления на указанные номера телефонов.
- Исполняемый файл – при возникновении события исполняемый файл запускается на Сервере администрирования.

► Чтобы настроить параметры доставки уведомлений о событиях, возникших в Kaspersky Security Center:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **Уведомление** и на правой панели выберите вкладку с требуемым способом уведомления:

- **Электронная почта**

На вкладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными

приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**
Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.
- **Использовать TLS, если поддерживается SMTP-сервером**
Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.
- **Всегда использовать TLS, для проверки срока действия сертификата сервера**
Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать сертификат для TLS подключения, перейдя по ссылке **Задать сертификаты**:

- Выберите файл сертификата SMTP-сервера:
Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

Вам нужно указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер с сертификатом в формате PKCS#12:

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

В поле **Тема** укажите тему электронной почты. Вы можете оставить поле пустым.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашего электронного письма. Переменная, в соответствии с выбранным шаблоном, автоматически отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив подстановочные параметры (см. раздел "Уведомление о событиях с помощью исполняемого файла" на стр. [316](#)) с подробными данными события.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить тестовое сообщение** можно проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения на указанные адреса электронной почты.

- **SMS**

На вкладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой.

Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**
Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.
- **Использовать TLS, если поддерживается SMTP-сервером**
Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.
- **Всегда использовать TLS, для проверки срока действия сертификата сервера**
Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать сертификат SMTP-сервера для TLS подключения, перейдя по ссылке **Задать сертификаты**:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **Тема** укажите тему электронной почты.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашего электронного письма. Переменная, в соответствии с выбранным шаблоном, отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя**. **Внимание: не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Номера телефонов получателей SMS-сообщений** укажите номера мобильных телефонов для получения SMS.

В поле **Текст уведомления** напишите текст уведомления о событии, отправляемый приложением при возникновении события. Текст может содержать подстановочные параметры (см. раздел "Уведомление о событиях с помощью исполняемого файла" на стр. [316](#)), такие как имя события, имя устройства и имя домена.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

Нажмите на кнопку **Отправить тестовое сообщение**, чтобы проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

Если выбран этот способ уведомления, в поле ввода можно указать, какое приложение будет запущено при возникновении события.

В поле **Исполняемый файл, который запустится на Сервере администрирования при возникновении события** укажите папку и имя файла, который запустится. Перед указанием файла подготовьте файл и укажите подстановочные параметры (см. раздел "Уведомление о событиях с помощью исполняемого файла" на стр. [316](#)), которые определяют сведения о событии, которые будут отправлены в сообщении. Указанные папка и файл должны находиться на Сервере администрирования.

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

3. На вкладке настройте параметры уведомлений.

4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Сохраненные параметры доставки уведомлений применяются ко всем событиям, которые возникают в Kaspersky Security Center.

Можно изменить значения параметров доставки уведомлений для определенных событий (см. раздел "Изменение политики" на стр. [1253](#)) в разделе **Настройка событий** в параметрах Сервера администрирования, параметрах политики или параметрах приложения.

См. также:

Сценарий: мониторинг и отчеты[1466](#)

Уведомление о событиях с помощью исполняемого файла

Kaspersky Security Center позволяет с помощью запуска исполняемого файла уведомлять администратора о событиях на клиентских устройствах. Исполняемый файл должен содержать другой исполняемый файл с подстановочными параметрами события, которые нужно передать администратору.

Таблица 103. Подстановочные параметры для описания события

Подстановочный параметр	Описание подстановочного параметра
%SEVERITY%	Уровень важности события
%COMPUTER%	Имя устройства, на котором произошло событие
%DOMAIN%	Домен.
%EVENT%	Событие
%DESCR%	Описание события
%RISE_TIME%	Время возникновения
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Имя задачи
%KL_PRODUCT%	Агент администрирования
%KL_VERSION%	Номер версии Агента администрирования
%HOST_IP%	IP-адрес
%HOST_CONN_IP%	IP-адрес соединения

Пример:

Для уведомления о событии используется исполняемый файл (например, script1.bat), внутри которого запускается другой исполняемый файл (например, script2.bat) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл script1.bat, который, в свою очередь, запустит файл script2.bat с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

Объявления "Лаборатории Касперского"

В этом разделе описано, как использовать, настраивать и отключать объявления "Лаборатории Касперского".

В этом разделе

Об объявлениях "Лаборатории Касперского"	1555
Настройка параметров объявлений "Лаборатории Касперского"	1556
Выключение объявлений "Лаборатории Касперского"	1557

Об объявлениях "Лаборатории Касперского"

Раздел Объявления "Лаборатории Касперского" (**Мониторинг и отчеты** → **Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center и управляемых приложениях, установленных на управляемых устройствах. Kaspersky Security Center периодически обновляет информацию в разделе, удаляет устаревшие объявления и добавляет новую информацию.

Kaspersky Security Center показывает только те объявления "Лаборатории Касперского", которые относятся к текущему подключенному Серверу администрирования и приложениям "Лаборатории Касперского", установленным на управляемых устройствах этого Сервера администрирования. Объявления отображаются индивидуально для любого типа Сервера администрирования – главного, подчиненного или виртуального.

Для получения объявлений "Лаборатории Касперского" Сервер администрирования должен иметь подключение к интернету.

Объявления включают информацию следующих типов:

- Объявления, связанные с безопасностью.

Объявления, связанные с безопасностью, предназначены для того, чтобы приложения "Лаборатории Касперского", установленные в вашей сети, были в актуальном состоянии и были полностью функциональными. В объявлениях может содержаться информация о критических обновлениях для приложений "Лаборатории Касперского", исправлениях для обнаруженных уязвимостей и способах устранения других проблем в приложениях "Лаборатории Касперского". Объявления, связанные с безопасностью, включены по умолчанию. Если вы не хотите получать объявления, вы можете отключить эту функцию.

Чтобы показать вам информацию, которая соответствует вашей конфигурации защиты сети, Kaspersky Security Center отправляет данные на облачные серверы "Лаборатории Касперского" и получает только те объявления, которые относятся к приложениям "Лаборатории Касперского", установленным в вашей сети. Данные, которые могут быть отправлены на серверы, описаны в Лицензионном соглашении, которое вы принимаете при установке Сервера администрирования Kaspersky Security Center.

- Рекламные объявления.

Рекламные объявления включают информацию о специальных предложениях для ваших приложений "Лаборатории Касперского", рекламу и новости "Лаборатории Касперского". Рекламные объявления по умолчанию выключены. Вы получаете этот тип объявлений только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить рекламные объявления, выключив KSN.

Чтобы показывать вам только актуальную информацию, которая может быть полезна для защиты ваших сетевых устройств и выполнения повседневных задач, Kaspersky Security Center отправляет данные на облачные серверы "Лаборатории Касперского" и получает соответствующие объявления. Данные, которые могут быть отправлены на серверы, описан в разделе "Обрабатываемые данные" Положения о KSN (см. раздел "О KSN и KPSN" на стр. [873](#)).

Информация разделена на следующие категории по важности:

5. Критическая информация.
6. Важная новость.
7. Предупреждение.
8. Информационное сообщение.

При появлении новой информации в разделе Объявления "Лаборатории Касперского" приложение Kaspersky Security Center Web Console отображает метку уведомления, соответствующую уровню важности объявлений. Вы можете нажать на метку, чтобы просмотреть это объявление в разделе Объявления "Лаборатории Касперского".

Вы можете указать параметры объявлений "Лаборатории Касперского" (см. раздел "Настройка параметров объявлений "Лаборатории Касперского"" см. стр. [1556](#)), включая категории объявлений, которые вы хотите просматривать, и место отображения метки уведомления.

См. также:

Настройка параметров объявлений "Лаборатории Касперского"	1556
Выключение объявлений "Лаборатории Касперского"	1557
О KSN и KPSN	873

Настройка параметров объявлений "Лаборатории Касперского"

В разделе Объявления "Лаборатории Касперского" вы можете указать параметры объявлений "Лаборатории Касперского", включая категории объявлений, которые вы хотите просматривать, и где отображать метку уведомления.

► Чтобы настроить объявления "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Объявления "Лаборатории Касперского"**.
2. Перейдите по ссылке **Параметры**.
Откроется окно объявлений "Лаборатории Касперского".
3. Задайте следующие параметры:
 - Выберите уровень важности объявлений, которые вы хотите просматривать. Объявления других категорий отображаться не будут.

- Выберите расположение, где вы хотите видеть метку уведомления. Метка может отображаться во всех разделах консоли или в разделе **Мониторинг и отчеты** и его подразделах.
4. Нажмите на кнопку **ОК**.

Параметры объявлений "Лаборатории Касперского" настроены.

См. также:

Об объявлениях "Лаборатории Касперского"	1555
Выключение объявлений "Лаборатории Касперского"	1557

Выключение объявлений "Лаборатории Касперского"

Раздел объявлений "Лаборатории Касперского" (**Мониторинг и отчеты** → **Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center и управляемых приложениях, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Объявления "Лаборатории Касперского" включают в себя информацию двух типов: объявления, связанные с безопасностью, и рекламные объявления. Вы можете выключить объявления каждого типа отдельно.

► Чтобы выключить объявления, связанные с безопасностью:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Объявления "Лаборатории Касперского"**.
3. Переведите переключатель в положение **Объявления безопасности Выключены**.
4. Нажмите на кнопку **Сохранить**.

Объявления "Лаборатории Касперского" выключены.

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN.

► Чтобы отключить объявления:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Выключите параметр **Использовать Kaspersky Security Network Включено**.
4. Нажмите на кнопку **Сохранить**.

Объявления выключены.

См. также:

Об объявлениях "Лаборатории Касперского"	1555
Настройка параметров объявлений "Лаборатории Касперского"	1556

Просмотр информации об обнаруженных угрозах

Вы можете включить или отключить отображение информации об алертах.

► Чтобы включить или выключить отображение раздела **Алерты** в главном меню:

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса**.
2. В появившемся окне **Параметры интерфейса** включите или выключите параметр **Показать EDR-алерты**.
3. Нажмите на кнопку **Сохранить**.

В консоли отображается раздел **Алерты** в разделе **Мониторинг и отчеты** главного меню. В разделе **Алерты** вы можете просматривать информацию об обнаруженных угрозах на устройствах. Если вы добавите лицензионный ключ для EDR Optimum https://support.kaspersky.com/KEDR_Optimum/2.3/en-US/220194.htm, Kaspersky Security Center Web Console автоматически отобразит подраздел **Алерты** в главном меню в разделе **Мониторинг и отчеты**. Также вы можете добавить веб-виджет (см. раздел "Добавление веб-виджета на информационную панель" см. стр. [1470](#)), в котором отображается информация об алертах.

Для корректного отображения подробной информации об обнаруженных угрозах в карточке алерта вам необходимо установить плагин Kaspersky Endpoint Agent <https://support.kaspersky.com/corporate/lifecycle#b2b.block8.kea> и совместимую версию плагина Kaspersky Endpoint Security (см. раздел "Загрузка плагинов для приложений "Лаборатории Касперского"" на стр. [1086](#)) (Kaspersky Endpoint Security для Linux 12.1 или выше, Kaspersky Endpoint Security для Mac 12.1 или выше, Kaspersky Endpoint Security для Windows 12.6 или выше).

Используйте меню **Фильтр**, чтобы отфильтровать алерты по дате и значениям поля.

Поле **Тип объекта** содержит одно из следующих значений:

- Неизвестно
- Фишинговая ссылка
- Вирус
- Троянское приложение
- Вредоносные утилиты
- Троянское приложение удаленного администрирования
- Червь
- Другое приложение
- Рекламное приложение
- Порнографическое приложение

- Опасно упакованное приложение
- Опасное поведение

Поле **Автоматический ответ** содержит одно из следующих значений:

- Обнаружен вредоносный объект
- Объект удален
- Объект вылечен
- Не удалось вылечить объект
- Объект помещен на карантин
- Обнаружен архив, защищенный паролем
- Обнаружен вирус

См. также:

Сценарий: мониторинг и отчеты [1466](#)

Cloud Discovery

Kaspersky Security Center позволяет отслеживать использование облачных сервисов на управляемых устройствах с операционной системой Windows и блокировать доступ к нежелательным облачным сервисам. Cloud Discovery отслеживает попытки пользователей получить доступ к этим службам через браузеры и настольные приложения. Также отслеживает попытки доступа пользователей к облачным сервисам через незашифрованные соединения (например, по протоколу HTTP). Эта функция позволяет выявлять и прекращать скрытое несанкционированное использование облачных сервисов.

Возможность блокировки доступна только в том случае, если вы активировали Kaspersky Security Center по лицензии Kaspersky Security Center EDR Optimum или XDR Expert.
Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Можно включить функцию Cloud Discovery и выбрать политики безопасности или профили, для которых ее требуется включить. Можно также включать и выключать функцию отдельно для каждой политики безопасности или профиля. Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей.

Чтобы заблокировать доступ к нежелательным облачным сервисам, убедитесь, что выполнены следующие условия:

- Вы используете версию Kaspersky Endpoint Security 11.2 для Windows или выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

- Вы приобрели лицензию на Kaspersky Next, которая дает возможность блокировать доступ к нежелательным облачным сервисам. Подробнее см. справку Kaspersky Next <https://support.kaspersky.com/help/NextPro/1.0/en-us/101540.htm>.

Информация об удачных и заблокированных попытках доступа к облачным сервисам отображается в веб-виджете Cloud Discovery и в отчетах Cloud Discovery. Веб-виджет также показывает уровень риска каждого облачного сервиса. Kaspersky Security Center получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности или профилями политик, в которых она включена.

В этом разделе

Включение функции Cloud Discovery с помощью веб-виджета	1560
Добавление веб-виджета Cloud Discovery в панель мониторинга	1561
Просмотр информации об использовании облачных сервисов	1561
Уровень риска облачного сервиса	1562
Блокировка доступа к нежелательным облачным сервисам	1563

Включение функции Cloud Discovery с помощью веб-виджета

Функция Cloud Discovery получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности, в которых она включена. Включить или выключить Cloud Discovery можно только для политики Kaspersky Endpoint Security для Windows.

Существуют два способа включить функцию Cloud Discovery:

- С помощью веб-виджета Cloud Discovery.
- В свойствах политики Kaspersky Endpoint Security для Windows.

Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows, см. в разделе Cloud Discovery <https://support.kaspersky.com/KESWin/12.4/en-US/187200.htm> справки Kaspersky Endpoint Security для Windows.

Обратите внимание, что вы можете выключить функцию Cloud Discovery только в параметрах политики Kaspersky Endpoint Security для Windows.

Чтобы включить Cloud Discovery, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

► Чтобы включить функцию Cloud Discovery с помощью веб-виджета Cloud Discovery:

1. Откройте Kaspersky Security Center.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.

3. В веб-виджете **Cloud Discovery** нажмите на кнопку **Включить**.

Если у вас установлен Kaspersky Endpoint Security для Windows версии 12.4, включите функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows. Подробнее см. раздел Cloud Discovery <https://support.kaspersky.com/KESWin/12.4/en-US/187200.htm> справки Kaspersky Endpoint Security для Windows.

Если у вас версия Kaspersky Endpoint Security для Windows ниже версии 12.4, обновите плагин Kaspersky Endpoint Security для Windows до версии 12.5.

4. В открывшемся окне **Включить Cloud Discovery** выберите политики безопасности, для которых вы хотите включить функцию и нажмите на кнопку **Включить**.

Следующие параметры политики будут включены автоматически: **Внедрение скрипта в веб-трафик для взаимодействия с веб-страницами**, **Мониторинг веб-сеансов** и **Проверка зашифрованных подключений**.

Функция Cloud Discovery включена, веб-виджет добавлен в панель мониторинга.

Добавление веб-виджета Cloud Discovery в панель мониторинга

Вы можете добавить веб-виджет **Cloud Discovery** в панель мониторинга, чтобы отслеживать использование облачных сервисов на управляемых устройствах.

Чтобы добавить веб-виджет Cloud Discovery в панель инструментов, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

► Чтобы добавить веб-виджет Cloud Discovery в панель мониторинга:

1. Откройте Kaspersky Security Center.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
3. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
4. В списке доступных веб-виджетов нажмите на значок шеврона (➤) рядом с категорией **Другое**.
5. Выберите веб-виджет **Cloud Discovery** и нажмите на кнопку **Добавить**.

Если функция Cloud Discovery выключена, следуйте инструкциям в разделе Включение функции Cloud Discovery с помощью веб-виджета.

Выбранный веб-виджет будет добавлен в конец панели мониторинга.

Просмотр информации об использовании облачных сервисов

Веб-виджет **Cloud Discovery** показывает информацию о попытках доступа к облачным сервисам. Веб-виджет также показывает уровень риска каждого облачного сервиса. Kaspersky Security Center получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных профилями безопасности, в которых они включены.

Перед просмотром убедитесь, что:

- Веб-виджет Cloud Discovery добавлен в панель мониторинга (см. раздел "Добавление веб-виджета Cloud Discovery в панель мониторинга" на стр. [1561](#)).
- Функция Cloud Discovery включена.
- У вас есть право **Чтение** в функциональной области **Общие функции: Базовая функциональность**.

► *Чтобы посмотреть веб-виджет Cloud Discovery:*

1. Откройте Kaspersky Security Center.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**. Веб-виджет **Cloud Discovery** отображается в панели мониторинга.
3. В левой части веб-виджета **Cloud Discovery** выберите категорию облачных сервисов.
В таблице в правой части веб-виджета отображается до пяти сервисов из выбранной категории, к которым пользователи чаще всего пытаются получить доступ. Учитываются как успешные, так и заблокированные попытки доступа.
4. В правой части веб-виджета выберите требуемый сервис.
В таблице ниже отображается до десяти устройств, наиболее часто обращающихся к этому сервису.
В веб-виджете отображаются запрашиваемые данные.

В отображаемом веб-виджете можно выполнить следующие действия:

- Перейдите в раздел **Мониторинг и отчеты** → **Отчеты**, чтобы просмотреть отчеты Cloud Discovery.
- Заблокируйте или разрешите доступ к выбранному облачному сервису.

The blocking capability is available only if you activated Kaspersky Security Center under a Kaspersky Security Center EDR Optimum or XDR Expert license.
The blocking capability is available only if you use Kaspersky Endpoint Security 11.2 for Windows or later.
Earlier versions of the security application only allow you to monitor the use of cloud services.

Уровень риска облачного сервиса

Cloud Discovery определяет уровень риска для каждого облачного сервиса. Уровень риска помогает определить службы, не соответствующие требованиям безопасности вашей организации. Например, уровень риска можно учесть при принятии решения о блокировке доступа к определенному сервису.

Уровень риска является оценочным показателем и ничего не говорит о качестве облачного сервиса или о производителе. Уровень риска – это рекомендация экспертов "Лаборатории Касперского".

Уровни риска облачных сервисов отображаются в веб-виджете Cloud Discovery и в списке всех контролируемых облачных сервисов.

Блокировка доступа к нежелательным облачным сервисам

Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей. Вы также можете разрешить доступ к облачным сервисам, которые ранее были заблокированы.

Например, уровень риска можно учесть при принятии решения о блокировке доступа к определенному сервису.

Вы можете заблокировать или разрешить доступ к облачным сервисам для политики безопасности или профиля политики.

Существует два способа заблокировать доступ к нежелательным облачным сервисам:

- С помощью веб-виджета Cloud Discovery.
В этом случае вы можете заблокировать доступ к сервисам по очереди.
- В свойствах политики Kaspersky Endpoint Security для Windows.
В этом случае вы можете заблокировать доступ к сервисам по очереди или сразу всю категорию.
Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows, см. в разделе Cloud Discovery <https://support.kaspersky.com/KESWin/12.4/en-US/187200.htm> справки Kaspersky Endpoint Security для Windows.

► Чтобы заблокировать или разрешить доступ к облачному сервису с помощью веб-виджета:

1. Откройте веб-виджет Cloud Discovery и выберите требуемый облачный сервис.
2. В панели **Топ-10 устройств, использующих эту службу** найдите политику безопасности или профиль политики, для которых вы хотите заблокировать или разрешить службу.
3. В соответствующей строке в столбце **Статус доступа в политике или профиле политики** выполните одно из следующих действий:
 - Чтобы заблокировать службу, в раскрывающемся списке выберите **Заблокировано**.
 - Чтобы разрешить службу, в раскрывающемся списке выберите **Разрешено**.
4. Нажмите на кнопку **Сохранить**.

Доступ к выбранной службе заблокирован или разрешен для политики безопасности или профиля политики.

Журнал активности Kaspersky Security Center Web Console

Журнал активности Kaspersky Security Center Web Console может помочь выяснить причины сбоя программного обеспечения. Когда вы обращаетесь в Службу технической поддержки "Лаборатории Касперского" в случае сбоя Kaspersky Security Center Web Console, специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить от вас файлы журнала. Файлы журнала событий Kaspersky Security Center Web Console хранятся в папке <Папка установки Kaspersky Security Center Web Console>/logs все время использования приложения. Файлы журнала не отправляются автоматически специалистам Службы технической поддержки "Лаборатории Касперского".

► Чтобы включить журнал активности Kaspersky Security Center Web Console,

установите флажок **Включить запись в журнал Kaspersky Security Center Web Console** в окне **Параметры подключения Kaspersky Security Center Web Console** мастера установки Kaspersky Security Center Web Console (см. раздел "Установка Kaspersky Security Center Web Console" см. стр. [988](#)).

Файлы журнала записываются в текстовом формате.

Имена файлов журнала записываются в формате <имя компонента>.<имя устройства>.<номер ревизии файла>.ГГГГ-ММ-ДД, где

- <имя компонента> – имя компонента Kaspersky Security Center или имя плагина управления Kaspersky Security Center Web Console.
- <имя устройства> – имя устройства, на котором запущен компонент или плагин (<имя компонента>).
- <номер ревизии файла> – номер файла журнала, созданного для компонента или плагина <имя компонента>, который запущен на устройстве <имя устройства>. В течение одного дня можно создать несколько файлов журнала для одного и того же компонента или плагина (<имя компонента>) и устройства (<имя устройства>). Максимальный размер файла журнала составляет 50 МБ. При достижении максимального размера файла создается новый файл журнала. Новый файл журнала (<номер ревизии файла>) увеличивается на 1.
- ГГГГ, ММ, и ДД это год, месяц и день, когда была создана первая запись журнала. Новый файл журнала создается, когда начинается новый день.

Интеграция Kaspersky Security Center с другими решениями

В этом разделе описывается, как настроить доступ из Kaspersky Security Center Web Console к другому приложению "Лаборатории Касперского", например Kaspersky Managed Detection and Response. В этом разделе также описано как настроить экспорт в SIEM-системы.

В этом разделе

Установка фоновое соединения	1564
Экспорт событий в SIEM-системы	1565

Установка фоновое соединения

Чтобы приложение Kaspersky Security Center Web Console могло выполнять свои фоновые задачи, вам необходимо установить межсервисное соединение между Kaspersky Security Center Web Console и Сервером администрирования. Вы можете установить это соединение, только если в вашей учетной записи есть право **Изменение списков управления доступом объектов** в функциональной области **Общий функционал: Права пользователей**.

Если вы устанавливаете плагин Kaspersky Endpoint Security для Windows 12.6 или обновляете плагин Kaspersky Endpoint Security для Windows с версии ниже 11.7 и фоновое соединение еще не установлено, отображается уведомление о том, что необходимо установить фоновое соединение. Также вам нужно

будет предоставить учетной записи службы права **Общий функционал: Операции с Сервером администрирования**.

► *Чтобы установить фоновое соединение:*

1. В главном окне приложения перейдите в раздел **Параметры** → **Интеграция**.
2. В разделе **Интеграция** переключите переключатель установки фонового соединения в положение: **Фоновое соединение для интеграции Включено**.
3. В разделе **Включить фоновое соединение** нажмите на кнопку **ОК**.

Фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования установлено. Сервер администрирования создает учетную запись для фонового подключения, и эта учетная запись используется как служебная учетная запись для поддержания взаимодействия Kaspersky Security Center с другим приложением или решением "Лаборатории Касперского". Имя этой учетной записи службы содержит префикс NWCSvcUser.

Сервер администрирования автоматически меняет пароль учетной записи службы каждые 30 дней в целях безопасности. Вы не можете удалить учетную запись службы вручную. Сервер администрирования автоматически удаляет эту учетную запись при отключении межсервисного соединения. Сервер администрирования создает единую учетную запись службы для каждой Консоли администрирования и назначает все учетные записи службы группе безопасности с именем ServiceNwcGroup. Сервер администрирования создает эту группу безопасности автоматически в процессе установки Kaspersky Security Center. Вы не можете удалить эту группу безопасности вручную.

См. также:

Сценарий: обновление Kaspersky Security Center и управляемых приложений безопасности.....[1333](#)

Экспорт событий в SIEM-системы

В этом разделе описывается, как настроить экспорт событий в SIEM-системы.

Сценарий: настройка экспорта событий в SIEM-системы

Kaspersky Security Center позволяет выполнять настройку одним из способов: экспорт в любую SIEM-систему, использующую формат Syslog, экспорт в QRadar, Splunk, ArcSight SIEM-системы, использующие форматы LEEF и CEF, или экспорт событий в SIEM-системы прямо из базы Kaspersky Security Center. По завершении этого сценария Сервер администрирования автоматически отправляет события в SIEM-систему.

Предварительные требования

Перед началом настройки экспорта событий в Kaspersky Security Center:

- Узнайте больше о методах экспорта событий (см. раздел "Об экспорте событий" на стр. [883](#)).
- Убедитесь, что у вас есть значения системных параметров (см. раздел "Предварительные условия" на стр. [881](#)).

Вы можете выполнять шаги этого сценария в любом порядке.

Процесс экспорта событий в SIEM-систему состоит из следующих шагов:

- Настройка SIEM-системы для получения событий из Kaspersky Security Center

Инструкции: Настройка экспорта событий в SIEM-системе (см. раздел "О настройке экспорта событий в SIEM-системе" на стр. [884](#)).

- Выбор события, которые вы хотите экспортировать в SIEM-систему:

Инструкции:

- Консоль администрирования: Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog, Выбор общих событий для экспорта в формате Syslog.
- Kaspersky Security Center Web Console: Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog (на стр. [1572](#)), Выбор общих событий для экспорта в формате Syslog (на стр. [1574](#)).
- Настройка экспорта событий в SIEM-систему одним из следующих способов:

- Укажите протоколы TCP/IP, UDP или TLS over TCP.

Инструкции:

- Консоль администрирования: Настройка экспорта событий в SIEM-системы.
- Kaspersky Security Center Web Console: Настройка экспорта событий в SIEM-системы (см. раздел "Настройка Kaspersky Security Center для экспорта событий в SIEM-систему" на стр. [1576](#)).
- Использование экспорта событий напрямую из базы данных Kaspersky Security Center (см. раздел "Экспорт событий напрямую из базы данных" на стр. [894](#)). В базе данных Kaspersky Security Center представлен набор публичных представлений; вы можете найти описание этих общедоступных представлений в документе klakdb.chm.

Результаты

После настройки экспорта событий в SIEM-систему вы можете просматривать результаты экспорта (см. раздел "Просмотр результатов экспорта" на стр. [899](#)), если вы выбрали события, которые хотите экспортировать.

См. также:

Об экспорте событий	883
Предварительные условия	881
О событиях в Kaspersky Security Center	881
О настройке экспорта событий в SIEM-системе	884
Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog	1572
Выбор общих событий для экспорта в формате Syslog	1574
Настройка Kaspersky Security Center для экспорта событий в SIEM-систему	1576
Экспорт событий напрямую из базы данных	894
Просмотр результатов экспорта	899

Предварительные условия

При настройке автоматического экспорта событий в Kaspersky Security Center необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

- **Протокол**

Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы	879

О событиях в Kaspersky Security Center

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Вы можете экспортировать эту информацию во внешние SIEM-системы (см. раздел "Сценарий: настройка экспорта

событий в SIEM-системы" см. стр. [879](#)). Экспорт информации о событиях во внешние SIEM-системы позволяет администраторам SIEM-систем оперативно реагировать на события системы безопасности, произошедшие на управляемых устройствах или группах администрирования.

Типы событий

В Kaspersky Security Center существуют следующие типы уведомлений:

- **Общие события.** Эти события возникают во всех управляемых приложениях "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- **Специфические события управляемых приложений "Лаборатории Касперского".** Каждое управляемое приложение "Лаборатории Касперского" имеет собственный набор событий.

Источники событий

События могут генерироваться следующими приложениями:

- Компонентами приложения Kaspersky Security Center:
 - Сервер администрирования (см. раздел "События Сервера администрирования" см. стр. [638](#))
 - Агент администрирования (см. раздел "События Агента администрирования" см. стр. [669](#))
 - Сервер iOS MDM
 - Управляемые приложения "Лаборатории Касперского"
- Подробнее о событиях, генерируемых управляемыми приложениями "Лаборатории Касперского", см. в документации соответствующего приложения.

Просмотреть полный список событий, которые может генерировать приложение, можно на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

Уровень важности события

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- ***Критическое событие*** – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- ***Отказ функционирования*** – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы приложения или выполнения процедуры.
- ***Предупреждение*** – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа приложения может быть восстановлена без потери данных или функциональных возможностей.
- ***Информационное сообщение*** – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе приложения или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

См. также:

События компонентов Kaspersky Security Center	636
Сценарий: настройка экспорта событий в SIEM-системы	879

Об экспорте событий

Вы можете использовать экспорт событий в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ предупреждений систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться в панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Консоли администрирования Kaspersky Security Center. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Kaspersky Security Center, а затем получение событий в SIEM-системе, либо наоборот.

Способы отправки событий из Kaspersky Security Center

Существует три способа отправки событий из Kaspersky Security Center во внешние системы:

- Отправка событий по протоколу Syslog в любую SIEM-систему.

По протоколу Syslog можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. Протокол Syslog – это стандартный протокол регистрации сообщений. Вы можете использовать этот протокол для экспорта событий в любую SIEM-систему.

Для этого нужно отметить события, которые вы хотите передать в SIEM-систему. Вы можете отметить события с помощью Консоли администрирования или Kaspersky Security Center Web Console (см. раздел "Выбор общих событий для экспорта в формате Syslog" на стр. [1574](#)). Только отмеченные события будут передаваться в SIEM-систему. Если вы ничего не отметили, никакие события не будут передаваться.

- Отправка событий по протоколам CEF и LEEF в системы QRadar, Splunk и ArcSight.

Протоколы CEF и LEEF можно использовать для экспорта общих событий (см. раздел "О событиях в Kaspersky Security Center" на стр. [881](#)). При экспорте событий по протоколам CEF и LEEF у вас нет возможности выбора определенных экспортируемых событий. Вместо этого выполняется экспорт всех общих событий. В отличие от протокола Syslog, протоколы CEF и LEEF не являются универсальными. Протоколы CEF и LEEF предназначены для соответствующих SIEM-систем

(QRadar, Splunk и ArcSight). Поэтому при выборе экспорта событий по одному из этих протоколов в SIEM-системе используется нужный анализатор.

- Напрямую из базы данных Kaspersky Security Center в любую SIEM-систему.

Этот способ экспорта событий можно использовать для получения событий напрямую из публичных представлений базы данных с помощью SQL-запросов. Результаты выполнения запроса сохраняются в .xml файл, который можно использовать в качестве входных данных для внешней системы. Напрямую из базы данных можно экспортировать только события, доступные в публичных представлениях.

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky Security Center. Для этого необходимо выполнить настройку SIEM-системы. Конфигурация зависит от конкретной используемой SIEM-системы. Однако в конфигурациях всех SIEM-систем существует ряд общих этапов, таких как настройка приемника и анализатора.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

О настройке экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Kaspersky Security Center.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

Настройка приемника сообщений

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Kaspersky Security Center. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Протокол экспорта или тип входных данных**

Протокол передачи сообщений, TCP/IP или UDP. Необходимо указать тот же протокол, который был выбран в Kaspersky Security Center для передачи событий.

- **Порт**

Номер порта для подключения к Kaspersky Security Center. Необходимо указать тот же номер порта, который был выбран в Kaspersky Security Center для передачи событий.

- **Протокол передачи сообщений или тип исходных данных**

Протокол, используемый для экспорта событий в SIEM-систему. Может являться одним из стандартных протоколов: Syslog, CEF или LEEF. SIEM-система выбирает анализатор событий, соответствующий указанному протоколу.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На рисунке ниже приведен пример настройки приемника в ArcSight.

The screenshot shows the 'Edit Receiver' configuration page in the ArcSight Logger web console. The page has a navigation bar with links: Summary, Analyze, Dashboards, Configuration (selected), and System Admin. Below the navigation bar, the title 'Edit Receiver' is displayed. A note states: 'If a source type that you need does not exist in the Source Type dropdown list below, go to the [Source Types](#) page to add it.' The configuration fields are as follows: Name (text input: tcp cef), IP/Host (dropdown: All), Port (text input: 616), Encoding (dropdown: UTF-8), Source Type (dropdown: CEF), and an Enable checkbox (checked). At the bottom, there are 'Save' and 'Cancel' buttons.

Рисунок 18. Пример настройки приемника сообщений

Анализатор сообщений

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, для того чтобы информация о событиях была должным образом передана в SIEM-систему. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения сообщения на поля, такие как идентификатор сообщения, уровень важности, описание, параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky Security Center, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы[879](#)

Выбор событий для экспорта в SIEM-системы в формате Syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберете экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные

события, которые произошли во всех приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, управляемого этой политикой.

Выбор событий для управляемого приложения. Если вы выбираете экспортируемые события для управляемого приложения, установленного на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этом приложении.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы[879](#)

В этом разделе

О выборе событий для экспорта в SIEM-систему в формате Syslog.....[1572](#)

Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog[1572](#)

Выбор общих событий для экспорта в формате Syslog.....[1574](#)

О выборе событий для экспорта в SIEM-систему в формате Syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберете экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, управляемого этой политикой.
- Выбор событий для управляемого приложения. Если вы выбираете экспортируемые события для управляемого приложения, установленного на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этом приложении.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы[879](#)

Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших в определенном управляемом приложении, установленном на управляемых устройствах, выберите события для экспорта в политике приложения. В этом случае отмеченные события экспортируются со всех устройств, входящих в область действия политики.

► *Чтобы отметить события для экспорта для определенного управляемого приложения:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Выберите политику приложения, для которого нужно отметить события.
Откроется окно свойств политики.
3. Перейти в раздел **Настройка событий**.
4. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.
5. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

6. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.
7. Нажмите на кнопку **Сохранить**.

Отмеченные события из управляемого приложения готовы к экспорту в SIEM-систему.

Вы можете отметить, какие события экспортировать в SIEM-систему для конкретного управляемого устройства. В случае, если ранее экспортируемые события были выбраны в политике приложения, вам не удастся переопределить выбранные события для управляемого устройства.

► *Чтобы выбрать события для управляемого устройства:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
Отобразится список управляемых устройств.
2. Перейдите по ссылке с названием требуемого устройства в списке управляемых устройств.
Откроется окно свойств выбранного устройства.
3. Перейти в раздел **Приложения**.
4. Перейдите по ссылке с названием требуемого приложения в списке приложений.
5. Перейдите в раздел **Настройка событий**.
6. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.
7. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

8. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

Теперь Сервер администрирования отправляет в SIEM-систему выбранные события, если экспорт в SIEM-систему настроен.

См. также:

О событиях в Kaspersky Security Center[881](#)

Выбор общих событий для экспорта в формате Syslog

Вы можете отметить общие события, которые Сервер администрирования будет экспортировать в SIEM-системы, используя формат Syslog.

► Чтобы выбрать общие события для экспорта в SIEM-систему:

1. Выполните одно из следующих действий:

- В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
- В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**, а затем перейдите по ссылке политики.

2. В открывшемся окне перейдите на вкладку **Настройка событий**.

3. Нажмите **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

4. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

Теперь Сервер администрирования отправляет в SIEM-систему выбранные события, если экспорт в SIEM-систему настроен.

См. также:

О событиях в Kaspersky Security Center[881](#)

Об экспорте событий в форматах CEF и LEEF

Форматы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий (см. раздел "О событиях в Kaspersky Security Center" на стр. [881](#)), а также событий, переданных приложениями "Лаборатории Касперского" Серверу администрирования. Набор экспортируемых событий определен заранее, возможность выбирать экспортируемые события отсутствует.

Формат экспорта можно выбрать в зависимости от того, какую SIEM-систему вы используете. В следующей таблице приведены SIEM-системы и соответствующие им форматы экспорта.

Таблица 104. Форматы экспорта событий в SIEM-систему

SIEM-система	Формат экспорта
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) – это специализированный формат событий для IBM Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center (<https://www.ibm.com/support/knowledgecenter/>).
- CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа. Для протокола CEF должна использоваться кодировка UTF-8.

При автоматическом экспорте Kaspersky Security Center отправляет общие события в SIEM-систему. Автоматический экспорт событий начинается сразу после включения. В этом разделе описана процедура включения автоматического экспорта событий.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы [879](#)

Об экспорте событий в формате Syslog

Используя формат Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других приложениях "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Формат Syslog определяется документами Request for Comments (RFC), опубликованными Internet Engineering Task Force. Стандарт RFC 5424 (<https://tools.ietf.org/html/rfc5424>) используется для экспорта событий из Kaspersky Security Center во внешние системы.

В Kaspersky Security Center можно настроить экспорт событий во внешние системы в формате Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Kaspersky Security Center таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky Security Center начинается сразу после включения автоматического экспорта.
2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы[879](#)

Настройка Kaspersky Security Center для экспорта событий в SIEM-систему

Чтобы экспортировать события в SIEM-систему, вам необходимо настроить процесс экспорта из Kaspersky Security Center Web Console.

► *Чтобы настроить экспорт в SIEM-системы из Kaspersky Security Center Web Console:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Экспорт в SIEM-систему**.

3. Перейдите по ссылке **Параметры**.

Откроется раздел **Параметры экспорта**.

4. Укажите параметры в разделе **Параметры экспорта**:

- Адрес сервера SIEM-системы
- Порт SIEM-системы
- Протокол
- Формат данных

Если вы выбрали формат данных Syslog, необходимо указать:

- Максимальный размер сообщения в байтах

5. Заархивированные события можно экспортировать из базы данных Сервера администрирования и задать начальную дату, с которой вы хотите начать экспорт заархивированных событий:

е. Перейдите по ссылке **Установите дату начала экспорта**.

f. В открывшемся разделе укажите дату начала в поле **Дата начала экспорта системных событий**.

g. Нажмите на кнопку **ОК**.

6. Переключите параметр в положение **Автоматически экспортировать события в базу SIEM-системы Включено**.

7. Чтобы убедиться, что соединение с SIEM-системой успешно настроено, нажмите на кнопку **Проверить подключение**.

Отобразится статус подключения.

8. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы	879

Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Kaspersky Security Center, не используя интерфейс Kaspersky Security Center. Можно создавать запросы непосредственно к публичным представлениям и извлекать из них данные о событиях или создавать собственные представления на базе существующих публичных представлений и обращаться к ним для получения требуемых данных.

Публичные представления

Для вашего удобства в базе данных Kaspersky Security Center предусмотрен набор публичных представлений. Описание публичных представлений приведено в документе `klakdb.chm`.

Публичное представление `v_akpub_ev_event` содержит набор полей, соответствующих параметрам событий в базе данных. В документе `klakdb.chm` также содержится информация о публичных представлениях, относящихся к другим объектам Kaspersky Security Center, например, устройствам, приложениям, пользователям. Вы можете использовать эту информацию при создании запросов.

В этом разделе приведены инструкции по созданию SQL-запроса с помощью утилиты `klsql2`, а также пример такого запроса.

Вы также можете использовать любые другие приложения для работы с базами данных для создания SQL-запросов и представлений баз данных. Информация о том, как посмотреть параметры подключения к базе данных Kaspersky Security Center, например, имя инстанса и имя базы данных, приведена в соответствующем разделе.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы	879

В этом разделе

Создание SQL-запроса с помощью утилиты <code>klsql2</code>	895
Пример SQL-запроса, созданного с помощью утилиты <code>klsql2</code>	896
Просмотр имени базы данных Kaspersky Security Center	1579

Создание SQL-запроса с помощью утилиты `klsql2`

В этой статье приведены инструкции по загрузке и использованию утилиты `klsql2`, а также по созданию SQL-запроса с использованием этой утилиты.

► Чтобы использовать утилиту klsql2:

1. Найдите утилиту klsql2 в папке установки Kaspersky Security Center. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Не используйте версии утилиты klsql2, предназначенные для старых версий Kaspersky Security Center.
2. Создайте файл src.sql в любом текстовом редакторе и поместите файл в одну папку с утилитой.
3. В файле src.sql введите требуемый SQL-запрос и сохраните файл.
4. На устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, в командной строке введите следующую команду для запуска SQL-запроса из файла src.sql и сохранения результатов в файл result.xml:

```
klsql2 -i src.sql -u <имя пользователя> -p <пароль> -o result.xml
```

где <имя пользователя> и <пароль> являются учетными данными учетной записи пользователя, имеющего доступ к базе данных.

5. При необходимости введите имя учетной записи и пароль пользователя, имеющего доступ к базе данных.
6. Откройте созданный файл result.xml и посмотрите результаты выполнения SQL-запроса.

Вы можете редактировать файл src.sql и создавать в нем любые SQL-запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить SQL-запрос и сохранить результаты в файл.

См. также

Сценарий: настройка экспорта событий в SIEM-системы[879](#)

Пример SQL-запроса, созданного с помощью утилиты klsql2

В этом разделе приведен пример SQL-запроса, созданного с помощью утилиты klsql2.

Следующий пример показывает, как получить список событий, произошедших на устройствах пользователей за последние 7 дней, и отсортировать его по времени возникновения событий, самые недавние события отображаются первыми.

Пример:

```
SELECT
e.nId,                                /* идентификатор события
*/
e.tmRiseTime,                         /* время возникновения
события */
e.strEventType,                      /* внутреннее имя типа
события */
e.wstrEventTypeDisplayName,          /* отображаемое имя
события */
e.wstrDescription,                  /* отображаемое описание
события */
e.wstrGroupName,                    /* имя группы устройств */
h.wstrDisplayName,                  /* отображаемое имя
устройства, на котором произошло событие */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp      /* IP-адрес
устройства, на котором произошло событие */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

См. также:

Сценарий: настройка экспорта событий в SIEM-системы[879](#)

Просмотр имени базы данных Kaspersky Security Center

Для доступа к базе данных Kaspersky Security Center с помощью SQL Server, MySQL или MariaDB необходимо знать имя базы данных, чтобы иметь возможность подключиться к ней из редактора скриптов SQL.

► Чтобы просмотреть имя базы данных Kaspersky Security Center:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Информация об используемой базе данных**.

Имя базы данных указано в поле **Имя базы данных**. Используйте это имя базы данных для подключения и обращения к базе данных в ваших SQL-запросах.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы 879

Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Kaspersky Security Center события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте и при необходимости исправьте настройки Kaspersky Security Center и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. Например, первое событие – это критическое событие Сервера администрирования: *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.

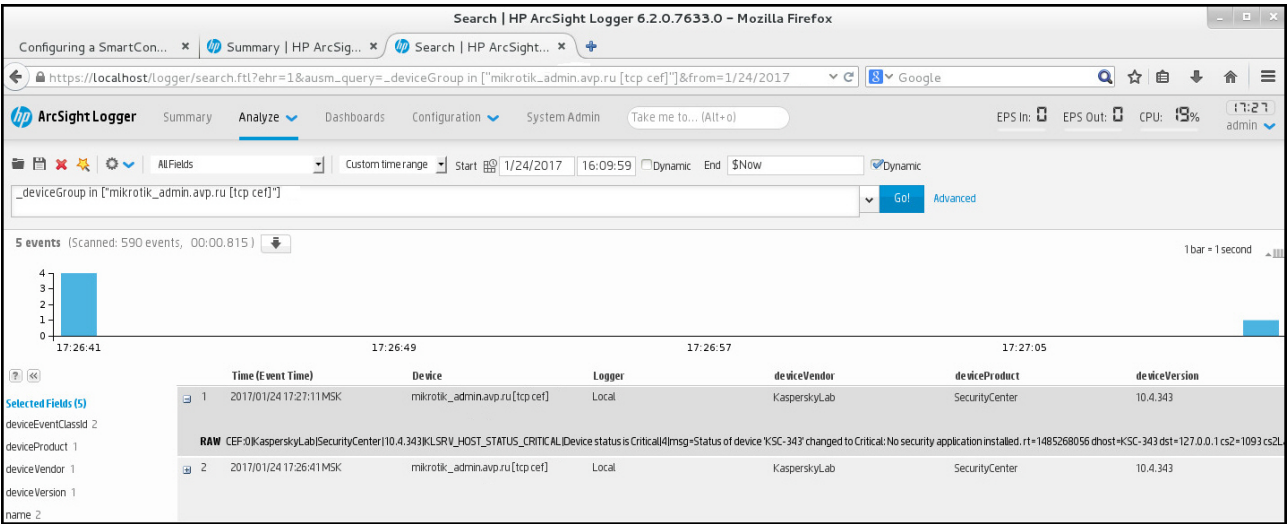


Рисунок 19. Пример событий

См. также:

Сценарий: настройка экспорта событий в SIEM-системы 879

Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах на базе Windows и на базе Linux:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров приложения;

- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- Запуск, остановка и перезапуск приложений

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также если вы обращаетесь в Службу технической поддержки "Лаборатории Касперского", специалист технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

В этом разделе

Открытие окна удаленной диагностики	1581
Включение и выключение трассировки для приложений.....	1582
Загрузка файла трассировки приложения.....	1584
Удаление файлов трассировки	1585
Загрузка параметров приложений	1586
Загрузка журналов событий.....	1586
Запуск, остановка и перезапуск приложения	1586
Запуск удаленной диагностики Агента администрирования Kaspersky Security Center и скачивание результатов	1587
Запуск приложения на клиентском устройстве	1587
Создание файла дампа для приложения	1588
Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux	1589
Загрузка и удаление файлов из Карантина и Резервного хранилища	1590

Открытие окна удаленной диагностики

Чтобы выполнить удаленную диагностику клиентских устройств на базе Windows и на базе Linux, сначала нужно открыть окно удаленной диагностики.

► Чтобы открыть окно удаленной диагностики:

3. Чтобы выбрать устройство, для которого вы хотите открыть окно удаленной диагностики, выполните одно из следующих действий:
 - Если устройство принадлежит к группе администрирования, в главном меню перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

- Если устройство принадлежит к группе нераспределенных устройств, в главном меню перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
4. Нажмите на имя требуемого устройства.
 5. В открывшемся окне свойств устройства выберите вкладку **Дополнительно**.
 6. В появившемся окне нажмите на кнопку **Удаленная диагностика**.

В результате открывается окно **Удаленная диагностика** клиентского устройства. Если отсутствует соединение между Сервером администрирования и клиентским устройством, появится сообщение об ошибке.

Если вам нужно получить сразу всю диагностическую информацию о клиентском устройстве с операционной системой Linux, вы можете запустить на этом устройстве скрипт collect.sh (см. раздел "Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux" см. стр. [1589](#)).

См. также:

Удаленная диагностика клиентских устройств	1580
Включение и выключение трассировки для приложений.....	1582
Загрузка файла трассировки приложения.....	1584
Удаление файлов трассировки	1585
Загрузка параметров приложений	1586
Загрузка журналов событий.....	1586
Запуск, остановка и перезапуск приложения	1586
Запуск удаленной диагностики Агента администрирования Kaspersky Security Center и скачивание результатов	1587
Запуск приложения на клиентском устройстве	1587

Включение и выключение трассировки для приложений

Вы можете включать и выключать трассировку для приложений, включая трассировку xperf.

Включение и выключение трассировки

► Чтобы включить или выключить трассировку на удаленном устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, для которого требуется включить или выключить трассировку.
Откроется список параметров удаленной диагностики.
4. Если вы хотите включить трассировку:

- a. В разделе **Трассировка** нажмите на кнопку **Включить трассировку**.
- b. В открывшемся окне **Изменить уровень трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости специалист Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:
 - **Уровень трассировки**

Уровень трассировки определяет состав информации, которую содержит файл трассировки.

- **Трассировка на основе ротации**

Приложение перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

Этот параметр доступен только для Kaspersky Endpoint Security.

- c. Нажмите на кнопку **Сохранить**.

Трассировка включена для выбранного приложения. В некоторых случаях для включения трассировки приложения безопасности требуется перезапустить это приложение и его задачу.

На клиентских устройствах под управлением Linux трассировка компонента Обновление Агента администрирования регулируется параметрами Агента администрирования. Поэтому параметры **Включить трассировку** и **Изменить уровень трассировки** выключены для этого компонента на клиентских устройствах под управлением Linux.

5. Если вы хотите выключить трассировку для выбранного приложения, нажмите на кнопку **Выключить трассировку**.

Трассировка выключена для выбранного приложения.

Включение трассировки Xperf

Для Kaspersky Endpoint Security специалисты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

► Чтобы включить, настроить или отключить трассировку Xperf:

1. Откройте утилиту удаленной диагностики клиентского устройства (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите Kaspersky Endpoint Security для Windows.
Откроется список параметров удаленной диагностики для Kaspersky Endpoint Security для Windows.
4. В разделе **Трассировка Xperf** нажмите на кнопку **Включить трассировку Xperf**.
Если трассировка Xperf уже включена, отображается кнопка **Выключить трассировку Xperf**. Нажмите на эту кнопку, если хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows.

5. В открывшемся окне **Изменить уровень трассировки Xperf**, в зависимости от запроса специалиста Службы технической поддержки, выполните следующее:
- a. Выберите один из уровней трассировки:
- **Легкий уровень**
Файл трассировки этого типа содержит минимальный объем информации о системе.
По умолчанию выбран этот вариант.
 - **Детальный уровень**
Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит информацию об оборудовании, операционной системе, список запущенных и завершенных процессов и приложений, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.
- b. Выберите один из уровней трассировки Xperf:
- **Базовый тип**
Приложение получает данные трассировки во время работы приложения Kaspersky Endpoint Security.
По умолчанию выбран этот вариант.
 - **Тип перезагрузки**
Приложение получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

Также вам могут предложить включить параметр **Размер файлов ротации (МБ)**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.
- c. Определите размер файла ротации.
- d. Нажмите на кнопку **Сохранить**.
Трассировка Xperf включена и настроена.
6. Если вы хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows, нажмите **Выключить трассировку Xperf** в разделе **Трассировка Xperf**.
Трассировка Xperf выключена.

Загрузка файла трассировки приложения

► Чтобы загрузить файл трассировки приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите приложение, для которого вы хотите загрузить файл трассировки.
4. В разделе **Трассировка** нажмите на кнопку **Файлы трассировки**.

Откроется окно **Журналы событий трассировки устройства**, где отображается список файлов трассировки.

5. В списке файлов трассировки выберите файл, который вы хотите загрузить.
6. Выполните одно из следующих действий:
 - Загрузите выбранный файл, нажав на кнопку **Загрузить**. Вы можете выбрать один или несколько файлов для загрузки.
 - Загрузите часть выбранного файла:
 - a. Нажмите на кнопку **Загрузить часть**.

Одновременная частичная загрузка нескольких файлов невозможна. Если вы выберете более одного файла трассировки, кнопка **Загрузить часть** будет неактивна.

- b. В открывшемся окне укажите имя и часть файла для загрузки в соответствии с вашими требованиями.

Для устройств под управлением Linux изменение имени части файла недоступно.

- c. Нажмите на кнопку **Загрузить**.

Выбранный файл или его часть загружается в указанное вами расположение.

Удаление файлов трассировки

Вы можете удалить файлы трассировки, которые больше не нужны.

► Чтобы удалить файл трассировки, выполните следующее действие:

1. Откройте утилиту удаленной диагностики клиентского устройства (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)).
2. В открывшемся окне удаленной диагностики выберите раздел **Журналы событий**.
3. В разделе **Файлы трассировки** нажмите **Журналы службы Центра обновления Windows** или **Журналы удаленной установки**, в зависимости от того, какие файлы трассировки вы хотите удалить.

Ссылка **Журналы службы Центра обновления Windows** доступна только для клиентских устройств под управлением Windows.

Откроется окно **Журналы событий трассировки устройства**, где отображается список файлов трассировки.

4. В списке файлов трассировки выберите один или несколько файлов, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить**.

Выбранные файлы трассировки удалены.

Загрузка параметров приложений

► Чтобы загрузить с клиентского устройства параметры приложений:

1. Откройте утилиту удаленной диагностики клиентского устройства (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
3. В разделе **Параметры приложения** нажмите на кнопку **Загрузить** для загрузки информации о параметрах приложения, установленных на клиентском устройстве.

ZIP-архив с информацией загрузится в указанное расположение.

Загрузка журналов событий

► Чтобы загрузить с удаленного устройства журнал событий:

1. Откройте утилиту удаленной диагностики клиентского устройства (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)).
2. В разделе **Журналы событий** в окне удаленной диагностики выберите **Журнал событий всех устройств**.
3. В окне **Журнал событий всех устройств** выберите один или несколько журналов событий.
4. Выполните одно из следующих действий:
 - Загрузите выбранный журнал событий, нажав на кнопку **Загрузить весь файл**.
 - Загрузите часть выбранного журнала событий:
 - d. Нажмите на кнопку **Загрузить часть**.

Одновременная частичная загрузка нескольких журналов событий невозможна. Если вы выберете более одного журнала событий, кнопка **Загрузить часть** будет неактивна.
 - e. В открывшемся окне укажите имя и часть журнала событий для загрузки в соответствии с вашими требованиями.

Для устройств под управлением Linux изменение имени части журнала событий недоступно.
 - f. Нажмите на кнопку **Загрузить**.

Выбранный журнал событий или его часть загрузится в указанное расположение.

Запуск, остановка и перезапуск приложения

Вы можете запускать, останавливать и перезапускать приложения на клиентском устройстве.

► Чтобы запустить, остановить или перезапустить приложение:

1. Откройте утилиту удаленной диагностики клиентского устройства (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите приложение, которое вы хотите запустить, остановить или перезапустить.
4. Выберите действие, нажав на одну из следующих кнопок:

- **Остановить приложение**

Эта кнопка доступна, только если приложение в данный момент запущено.

- **Перезапустить приложение**

Эта кнопка доступна, только если приложение в данный момент запущено.

- **Запустить приложение**

Эта кнопка доступна, только если приложение в данный момент не запущено.

В зависимости от выбранного вами действия требуемое приложение запустится, остановится или перезапустится на клиентском устройстве.

Если вы перезапустите Агент администрирования, появится сообщение о том, что текущее соединение устройства с Сервером администрирования будет потеряно.

Запуск удаленной диагностики Агента администрирования Kaspersky Security Center и скачивание результатов

► Чтобы запустить диагностику Агента администрирования Kaspersky Security Center на удаленном устройстве и загрузить ее результаты:

1. Откройте утилиту удаленной диагностики клиентского устройства (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В разделе списке приложений выберите **Агент администрирования Kaspersky Security Center Network**.
Откроется список параметров удаленной диагностики.
4. В разделе **Отчет диагностики** нажмите на кнопку **Выполнить диагностику**.
Запускается процесс удаленной диагностики и генерируется отчет о диагностике. По завершении процесса диагностики кнопка **Загрузить отчет диагностики** становится доступной.
5. Нажмите на кнопку **Загрузить отчет диагностики**, чтобы загрузить отчет.
Отчет загрузится в указанное расположение.

Запуск приложения на клиентском устройстве

Вам может потребоваться запустить приложение на клиентском устройстве, если вас об этом попросит специалист Службы технической поддержки "Лаборатории Касперского". Вам не нужно устанавливать приложение самостоятельно на этом устройстве.

► *Чтобы запустить приложение на клиентском устройстве:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)).
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.
3. В разделе **Файлы приложения** нажмите на кнопку **Обзор** для выбора ZIP-архива с приложением, которое вы хотите запустить на клиентском устройстве.

ZIP-архив должен содержать папку утилиты. Эта папка содержит исполняемый файл для запуска на удаленном устройстве.

При необходимости можно указать имя исполняемого файла и аргументы командной строки. Для этого заполните поля **Исполняемый файл в архиве для запуска на удаленном устройстве** и **Аргументы командной строки**.

4. Нажмите на кнопку **Загрузить и запустить** для запуска указанного приложения на клиентском устройстве.
5. Следуйте указаниям сотрудника службы поддержки "Лаборатории Касперского".

Создание файла дампа для приложения

Файл дампа приложения позволяет просматривать параметры приложения, работающего на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для приложения.

Получение файлов дампа с клиентских устройств с операционной системой Linux не поддерживается.

Чтобы получить файлы дампа с помощью удаленной диагностики, используется утилита kldumper. Эта утилита предназначена для получения файлов дампа процессов приложений "Лаборатории Касперского" по запросу специалистов Службы технической поддержки. Подробную информацию о требованиях к использованию утилиты kldumper приведена в Базе знаний Kaspersky Security Center.

► *Чтобы создать файл дампа для приложения:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)).
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.
3. В разделе **Формирование дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.
4. Нажмите на кнопку **Загрузить дамп файла**.

Архив с файлом дампа для указанного приложения загружен.

Если указанное приложение не запущено на клиентском устройстве, папка "result" в загруженном архиве будет пустой.

Если указанное приложение запущено, но загрузка завершается с ошибкой или папка "result" в загруженном архиве пуста, см. Базу знаний Kaspersky Security Center.

Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux

Kaspersky Security Center позволяет загружать основную диагностическую информацию с клиентского устройства (см. раздел "Удаленная диагностика клиентских устройств" на стр. [1580](#)). Кроме того, вы можете получить диагностическую информацию об устройстве с операционной системой Linux с помощью скрипта collect.sh "Лаборатории Касперского". Этот скрипт запускается на клиентском устройстве с операционной системой Linux, которое необходимо диагностировать. Затем создается файл с диагностической информацией, системной информацией об этом устройстве, файлами трассировки приложений, журналами событий устройства и файлом дампа для аварийных ситуаций, прерванных приложений.

Рекомендуется использовать скрипт collect.sh для получения сразу всей диагностической информации о клиентском устройстве с операционной системой Linux. Если вы загружаете диагностическую информацию удаленно через Kaspersky Security Center, вам нужно будет пройти все разделы интерфейса удаленной диагностики (см. раздел "Открытие окна удаленной диагностики" на стр. [1581](#)). Кроме того, диагностическая информация для устройства с операционной системой Linux, вероятно, не будет получена полностью.

Если вам необходимо отправить сформированный файл с диагностической информацией в Службу технической поддержки "Лаборатории Касперского", удалите всю конфиденциальную информацию перед отправкой файла.

► Чтобы загрузить диагностическую информацию с клиентского устройства с операционной системой Linux с помощью скрипта collect.sh:

1. Скачайте скрипт collect.sh
https://box.kaspersky.com/f/00a1a6d8beb24554a72d?_ga=2.227118109.1421819605.1691580180-1314822200.1681888137, который запакован в архив collect.tar.gz.
2. Скопируйте загруженный архив на клиентское устройство с операционной системой Linux, которое необходимо диагностировать.
3. Выполните следующую команду, чтобы распаковать архив collect.tar.gz:

```
# tar -xzf collect.tar.gz
```
4. Выполните следующую команду, чтобы указать права на выполнение скрипта:

```
# chmod +x collect.sh
```
5. Запустите сценарий collect.sh под учетной записью с правами администратора:

```
# ./collect.sh
```

Файл с диагностической информацией будет сформирован и сохранен в папке /tmp/\$HOST_NAME-collect.tar.gz.

Загрузка и удаление файлов из Карантина и Резервного хранилища

В этом разделе представлена информация о том, как загрузить и удалить файлы из Карантина и Резервного хранилища в Kaspersky Security Center Web Console.

Загрузка файлов из Карантина и Резервного хранилища

Вы можете загрузить файлы из Карантина и Резервного хранилища, только если выполняется одно из двух условий: либо включен параметр **Не разрывать соединение с Сервером администрирования** в свойствах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

► *Чтобы сохранить копию файла из карантина или резервного хранилища на жесткий диск:*

1. Выполните одно из следующих действий:
 - Если вы хотите сохранить копию файла из Карантина, в главном меню перейдите в раздел **Операции** → **Хранилища** → **Карантин**.
 - Если вы хотите сохранить копию файла из Резервного хранилища, в главном меню перейдите в раздел **Операции** → **Хранилища** → **Резервное хранилище**.
2. В открывшемся окне выберите файл, который вы хотите загрузить, и нажмите **Загрузить**.

Начнется загрузка. Копия файла, помещенного в Карантин на клиентском устройстве, сохраняется в указанную папку.

Об удалении объектов из Карантина, Резервного хранилища или Активных угроз

Когда приложения безопасности "Лаборатории Касперского", установленные на клиентских устройствах, помещают объекты на Карантин, в Резервное хранилище или Активные угрозы, они передают информацию о добавленных объектах в разделы **Карантин**, **Резервное хранилище** или **Активные угрозы** в Kaspersky Security Center. При открытии одного из этих разделов выберите объект из списка и нажмите на кнопку **Удалить**, Kaspersky Security Center выполняет одно из следующих действий или оба действия:

- Удаляет выбранный объект из списка.
- Удаляет выбранный объект из хранилища.

Действие, которое необходимо выполнить, определяется приложением "Лаборатории Касперского", поместившим выбранный объект в хранилище. Приложение "Лаборатории Касперского" указано в поле **Запись добавлена**. Подробную информацию о том, какое действие необходимо выполнить, см. в документации к приложению "Лаборатории Касперского".

Изменение языка интерфейса Kaspersky Security Center Web Console

Вы можете выбрать язык интерфейса Kaspersky Security Center Web Console.

► *Чтобы изменить язык интерфейса:*

1. В главном окне приложения перейдите в раздел **Параметры** → **Язык**.
2. Выберите необходимый язык интерфейса.

Приложение. Сертифицированное состояние приложения: параметры и их значения

Этот раздел содержит перечень параметров приложения, влияющих на безопасное состояние приложения, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированной конфигурации на другие значения выводит программу из безопасного состояния.

Таблица 105. Параметры и их значения для программы в сертифицированном состоянии

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Месторасположение папки общего доступа	При установке Kaspersky Security Center папка общего доступа, которая по умолчанию называется KLSHARE, находится не в папке установки Сервера администрирования. По умолчанию указана папка <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.	Не в папке, где установлен Сервер администрирования Kaspersky Security Center.
Политики	Для каждого управляемого приложения создана политика.	
Пароль на деинсталляцию Агента администрирования	В политике Агента администрирования установлен пароль на удаление Агента администрирования. Возможные значения: - установлен; - снят.	Установлен.
Защита паролем политики Kaspersky Endpoint Security для Windows. Параметр приложения Kaspersky Endpoint Security для Windows, если это приложение установлено.	Защита паролем позволяет установить ограничение на управление всеми или отдельными функциями и параметрами Kaspersky Endpoint Security для Windows, снижая вероятность несанкционированного или непреднамеренного внесения	Установлена.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
	изменений в работу программы. Возможные значения: - установлена; - снята.	
Автоматическое обновление модулей Агентов администрирования	Обновления модулей Агента администрирования устанавливаются автоматически, после того как Сервер администрирования завершает задачу получения обновлений. Возможные значения: - включен; - выключен.	Выключен.
Установка применимых обновлений со статусом одобрения <i>Не определено</i>	Патчи "Лаборатории Касперского" со статусом одобрения <i>Не определено</i> устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Возможные значения: - включен; - выключен.	Выключен.
Запуск задачи Загрузка обновлений в хранилище	Задача Загрузка обновлений в хранилище выполняет загрузку обновлений баз и модулей приложений, которые копируются с источника обновлений и размещаются в папке общего доступа. Возможные значения: - вручную; - автоматически по расписанию.	Автоматически по расписанию. Рекомендуемый интервал запуска задачи – один раз в час.
Запуск задачи Установка обновлений	Задача Установка обновлений выполняет установку ранее загруженных в хранилище обновлений на клиентские устройства.	Автоматически, по завершении задачи Загрузка обновлений в хранилище.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
	Возможные значения: • вручную; • автоматически по расписанию.	
Передача данных сервису KSN	Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Возможные значения передачи данных приложения сервису KSN: • отключена; • включена.	Отключена.
Источник обновлений задачи Загрузка обновлений в хранилище	Источник обновлений баз и модулей управляемых приложений "Лаборатории Касперского". Возможные значения: • Серверы обновлений "Лаборатории Касперского"; • Главный Сервер администрирования; • Локальная или сетевая папка.	• Главный Сервер администрирования; • Локальная или сетевая папка. Источник обновлений <i>Серверы обновлений "Лаборатории Касперского"</i> удален, чтобы программа не передавала информацию на серверы обновлений "Лаборатории Касперского".
Способ активации Сервера администрирования	Возможные значения: • с помощью файла ключа; • с помощью кода активации.	С помощью файла ключа.
Служба прокси-сервера активации "Лаборатории Касперского"	Служба прокси-сервера активации "Лаборатории Касперского" используется для	Отключена

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
	обеспечения передачи запросов на активацию от управляемых приложений к серверам активации "Лаборатории Касперского". Возможные значения: - отключена; - включена.	
Доверенные каналы с использованием SSL-протокола	Протокол SSL позволяет идентифицировать стороны, взаимодействующие при подключении (взаимодействие между Севером администрирования и устройствами), осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. Возможные значения: - используется; - не используется.	Используется.
Права пользователей	Права обеспечивают доступ администраторов, пользователей и групп пользователей к разным функциям приложения.	Минимально необходимые права настроены: только уполномоченные роли имеют права изменять параметры защиты.
Условия для статуса <i>Критический</i>	Набор условий при котором устройство принимает статус <i>Критический</i> .	Выбрано условие Найдено много вирусов . Параметр Более чем равен значению 0.
Максимальное количество событий, хранящихся в базе данных Сервера администрирования	Максимальное количество событий, которое хранится в базе данных Сервера администрирования, необходимое для проведения аудита приложения.	Рекомендуется установить значение не меньше 400 000 событий.
Срок хранения событий	Срок, в течение которого события хранятся в базе данных Сервера администрирования, необходимый для проведения аудита приложения.	Рекомендуется установить значения: - Для событий с уровнем важности <i>Критические</i> – не меньше 180 дней. - Для событий с уровнем важности <i>Предупреждение</i> – не меньше 90 дней.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
		Для событий с уровнем важности <i>Информационное сообщение</i> – не меньше 30 дней.
Срок хранения ревизий изменений объектов	Срок, в течение которого хранятся ревизии изменений объектов, необходимый для проведения регулярного аудита приложения.	Рекомендуется установить значение не меньше 90 дней.
Права доступа к возможностям шифрования	Права доступа пользователей и ролей пользователей к возможностям шифрования данных.	Запрещено.

- Просмотр результатов выполнения задач, хранящихся на Сервере администрирования
- Проверка целостности модулей с помощью утилит `klscmodchk` и `integrity_checker`
- Разделение доступа к функциям приложения по пользовательским ролям
- Обновление антивирусных баз в ручном режиме
- Устранение уязвимостей и установка критических обновлений в приложении
- Действия после сбоя или неустранимой ошибки в работе приложения

Проверка целостности модулей с помощью утилит `klscmodchk` и `integrity_checker`

Приложение Kaspersky Security Center содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленники могут заменить один или несколько исполняемых модулей или файлов приложения другими файлами, содержащими вредоносный код. Чтобы избежать подмены модулей и файлов приложения, в приложении Kaspersky Security Center предусмотрена проверка целостности компонентов приложения с помощью утилит `klscmodchk` и `integrity_checker`. Утилиты проверяют модули и файлы на наличие неавторизованных изменений или повреждений. Если модуль или файл приложения имеет некорректную контрольную сумму, то он считается поврежденным.

Утилита `klscmodchk` выполняет проверку целостности для следующих компонентов:

- Сервер администрирования
- Агент администрирования

Утилита `integrity_checker` выполняет проверку целостности для следующих компонентов:

- Сервер администрирования
- Агент администрирования
- Веб-консоль

Обе утилиты проверяют целостность модулей на основе файла манифеста `kl_file_integrity_manifest.xml`, который входит в состав сборки Kaspersky Security Center и расположен в папке установки приложения. Файл манифеста компонента приложения содержит файлы, целостность которых важна для корректной работы компонента приложения. Целостность самих файлов манифеста также проверяется.

Не рекомендуется вносить изменения в файл манифеста `kl_file_integrity_manifest.xml`, так как это приведет к изменению цифровой подписи файла и ошибкам в работе утилиты.

► Чтобы проверить целостность компонента приложения, выполните любую из следующих команд:

- `$ klscmodchk`

Утилита `klscmodchk` запускает приложение `integrity_checker` с нужными параметрами и таким образом проверяет целостность модулей.

- `$ integrity_checker [параметры] <путь к файлу манифеста>`

Опции приложения `integrity_checker`:

- `--help`: вывести на экран справку утилиты.
- `--version`: вывести на экран версию утилиты.
- `--verbose`: вывести на экран информацию о работе утилиты.

- `--trace <имя файла>`: файл для записи журнала на уровне DEBUG.
- `--signature-type <dskm2 | kds | kds-with-filename>`: тип проверяемой сигнатуры, по умолчанию dskm2.
- `--crl <директория>`: путь к директории, которая содержит отозванные сертификаты и подписи (CRL) для KDS. Значение игнорируется, если директория не существует или пуста.

Результат проверки каждого файла манифеста выводится рядом с названием файла манифеста в следующем виде:

- SUCCEEDED – целостность файлов подтверждена (код возврата 0).
- FAILED – целостность файлов не подтверждена (код возврата не 0).

Рекомендуется запускать утилиту проверки целостности с сертифицированного компакт-диска, чтобы гарантировать целостность утилиты. При запуске с компакт-диска требуется указать полный путь к файлу манифеста в папке приложения.

Настройка эталонных значений параметров приложения Kaspersky Security Center Web Console

Этот раздел содержит инструкции по установке эталонных значений параметров приложения Kaspersky Security Center Web Console. Настройка приложения по эталонным параметрам необходима для работы сертифицированной конфигурации приложения.

Месторасположение папки общего доступа Сервера администрирования

Папка общего доступа не должна находиться в папке установки Сервера администрирования.

► *Чтобы изменить папку общего доступа установленного Сервера администрирования:*

1. Выберите Сервер администрирования.
2. Нажмите на иконку **Свойства** (⚙️).
3. На вкладке **Общие** выберите **Папка общего доступа Сервера администрирования**.
4. В поле **Путь к папке общего доступа** измените расположение папки общего доступа.

Расположение **Папки общего доступа Сервера администрирования** изменится на указанное.

Политики

Для политики Агента администрирования необходимо установить пароль на удаление приложения Агента администрирования. Для политики Kaspersky Endpoint Security для Windows необходимо настроить защиту паролем на удаление, изменение или восстановление приложения Kaspersky Endpoint Security для Windows. В политике Kaspersky Endpoint Security для Windows необходимо настроить отправку уведомлений по электронной почте при возникновении событий об обнаружении вредоносного ПО.

Пароль на деинсталляцию Агента администрирования

Необходимо установить пароль на удаление приложения Агента администрирования.

► *Чтобы установить пароль на деинсталляцию приложения Агента администрирования, выполните следующие действия:*

1. В разделе **Устройства** выберите **Политики и профили политик**.
2. Выберите политику Агента администрирования.
Откроется окно свойств политики.
3. В окне свойств политики в разделе **Параметры приложения** выберите подраздел **Параметры**.
4. Включите параметр **Использовать пароль деинсталляции**.
5. В поле **Пароль** введите пароль на деинсталляцию приложения.
6. Нажмите на кнопку **Сохранить**.

Пароль на удаление приложения Агента администрирования установлен.

Защита паролем политики Kaspersky Endpoint Security для Windows

Необходимо установить защиту паролем на удаление, изменение или восстановление приложения Kaspersky Endpoint Security для Windows.

► *Чтобы установить защиту паролем на удаление, изменение или восстановление приложения Kaspersky Endpoint Security для Windows, выполните следующие действия:*

1. На вкладке **Устройства** выберите **Политики и профили политик**.
2. Выберите политику, которую требуется изменить.
Откроется окно свойств политики.
3. В окне свойств политики в разделе **Дополнительные параметры** выберите подраздел **Параметры приложения**.
4. В разделе **Параметры приложения** в блоке **Защита паролем** нажмите на кнопку **Настроить**.
5. В окне **Защита паролем** установите флажок **Включить защиту паролем**.
6. В окне **Защита паролем** в блоке **Область действия пароля** установите флажок **Удаление / Изменение / Восстановление приложения**.
7. Нажмите на кнопку **ОК**.

Защита паролем на удаление, изменение или восстановление приложения Kaspersky Endpoint Security для Windows установлена.

Автоматическое обновление модулей Агентов администрирования

По умолчанию обновления модулей Агента администрирования устанавливаются автоматически, после того как Сервер администрирования завершает задачу получения обновлений. Необходимо отключить автоматическое обновление модулей Агента администрирования. Сертификации подлежат только определенные версии исполняемых модулей приложения.

► *Чтобы отключить автоматическое обновление исполняемых модулей приложения, выполните следующие действия:*

1. В разделе **Устройства** выберите раздел **Задачи**.
2. Выберите задачу **Загрузка обновлений в хранилище Сервера Администрирования**.
Откроется окно свойств задачи.
3. В окне задачи выберите раздел **Параметры приложения**.
4. В разделе **Прочие настройки** выберите **Прочие параметры** и перейдите по ссылке **Настроить**.
Откроется окно параметров.
5. Выключите параметр **Обновлять модули Агентов администрирования**.
Если параметр выключен, автоматическая установка обновлений не выполняется. Полученные обновления модулей Агента администрирования можно установить вручную.
6. Нажмите на кнопку **ОК**.

Автоматическое обновление исполняемых модулей приложения отключено.

Если в сети вашей организации назначены точки распространения, то для всех точек распространения также требуется отключить автоматическое обновление модулей Агента администрирования.

- Чтобы отключить автоматическое обновление исполняемых модулей приложения точкой распространения, выполните следующие действия:

1. В разделе **Устройства** выберите раздел **Задачи**.
2. Выберите задачу **Загрузка обновлений в хранилища точек распространения**.

В результате откроется окно свойств задачи.

3. В окне задачи выберите раздел **Параметры приложения**.
4. Выключите параметр **Обновлять модули Агентов администрирования**.

Если параметр выключен, автоматическая установка обновлений не выполняется. Полученные обновления модулей Агента администрирования можно установить вручную.

5. Нажмите на кнопку **ОК**.

Автоматическое обновление исполняемых модулей приложения точкой распространения отключено.

Установка применимых обновлений со статусом одобрения "Не определено"

По умолчанию патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Необходимо отключить автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения *Не определено*.

- Чтобы отключить автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения *Не определено*, выполните следующие действия:

1. В разделе **Устройства** выберите раздел **Политики и профили политик**.
2. Выберите политику Агента администрирования.
Откроется окно свойств политики.
3. В открывшемся окне свойств политики выберите вкладку **Параметры и приложения**.
4. Выберите раздел **Управление патчами и обновлениями** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**.
5. Если флажок **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрено*.
6. Нажмите на кнопку **Сохранить**.

Автоматическая установка патчей "Лаборатории Касперского" со статусом одобрения *Не определено* отключено.

Запуск задач Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения

Необходимо настроить автоматический запуск задач **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилища точек распространения**.

Рекомендуемый интервал автоматического запуска задач Сервера администрирования **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилища точек распространения** составляет один раз в час.

- Чтобы настроить автоматический запуск задачи Сервера администрирования **Загрузка обновлений в хранилище Сервера администрирования** один раз в час, выполните следующие действия:

1. В разделе **Устройства** выберите раздел **Задачи**.
2. Выберите задачу **Загрузка обновлений в хранилище Сервера администрирования**.
Откроется окно свойств задачи.
3. В окне свойств выберите вкладку **Расписание**.
4. В поле **Запуск по расписанию** выберите значение **Каждый N час**.
5. В поле **Интервал запуска (ч)** установите значение 1.
6. Нажмите на кнопку **Сохранить**.

Автоматический запуск задачи Сервера администрирования **Загрузка обновлений в хранилище Сервера администрирования** один раз в час настроен.

Если в сети организации назначены точки распространения, необходимо также настроить автоматический запуск задачи **Загрузка обновлений в хранилища точек распространения**. Для этого необходимо повторить действия, описанные выше для задачи **Загрузка обновлений в хранилище Сервера администрирования**.

Запуск задачи Установка обновлений

После выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования** необходимо настроить запуск задачи **Установка обновлений**.

- Чтобы настроить автоматический запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования**:

1. В разделе **Устройства** выберите раздел **Задачи**.
2. Выберите задачу **Установка обновлений**.
В результате откроется окно свойств задачи.
3. В окне свойств выберите вкладку **Расписание**.
4. В поле **Запуск по расписанию** выберите значение **По завершении другой задачи**.
5. В поле **Результат выполнения** выберите значение **Завершена успешно**.
6. В поле **Имя** выберите задачу **Загрузка обновлений в хранилище Сервера администрирования**.
7. Нажмите на кнопку **Сохранить**.

Автоматический запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования** настроен.

Передача данных сервису KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний (см. раздел "О KSN и KPSN" на стр. [873](#)).

Для работы приложения в сертифицированной конфигурации службы, которые связаны с отправкой данных на внешние сервера и получением команд от внешних серверов (за периметром сети организации), должны быть отключены.

► *Чтобы отключить передачу данных сервису KSN, выполните следующие действия:*

1. Выберите Сервер администрирования, для которого нужно отключить передачу данных к сервису KSN.
2. Нажмите на кнопку **Свойства**.
3. В результате откроется окно свойств Сервера администрирования.
4. В окне свойств Сервера администрирования на вкладке **Общие** выберите **Параметры прокси-сервера KSN**.
5. Снимите флажок **Я принимаю условия использования Kaspersky Security Network**, чтобы выключить автоматическую передачу данных "Лаборатории Касперского" о работе установленных на устройствах приложений "Лаборатории Касперского".
6. При необходимости снимите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы выключить службу прокси-сервера KSN.
7. Нажмите на кнопку **Сохранить**.

Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

► *Чтобы отключить передачу данных сервису KSN точкой распространения, выполните следующие действия:*

1. Выберите Сервер администрирования, для которого нужно отключить передачу данных к сервису KSN.
2. Нажмите на кнопку **Свойства**.
3. В результате откроется окно свойств Сервера администрирования.
4. В окне свойств Сервера администрирования на вкладке **Общие** выберите **Точки распространения**.
5. В поле **Устройство** выберите нужное устройство.
Откроется окно свойств точки распространения,
6. В окне свойств точки распространения выберите раздел **Прокси-сервер KSN**.
7. Выключите параметр **Включить прокси-сервер KSN на стороне точек распространения**, чтобы выключить службу прокси-сервера KSN.
8. Нажмите на кнопку **ОК**.

Если флажок снят, передача данных в KSN от точки распространения и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

Передача данных сервису KSN должна быть отключена во всех управляемых приложениях.

Альтернативой отказу от использования KSN может стать использование KPSN. В этом случае вы получите доступ к оперативной базе знаний "Лаборатории Касперского", но информация о работе приложений "Лаборатории Касперского" не будет передаваться на сервера "Лаборатории Касперского". Подробнее см. в разделе Kaspersky Security Network (KSN) (см. раздел "Kaspersky Security Network и Kaspersky Private Security Network" на стр. [873](#)).

Источник обновлений задачи Загрузка обновлений в хранилище и задачи Загрузка обновлений в хранилище точек распространения

Для отключения передачи данных приложением серверу обновлений "Лаборатории Касперского" необходимо удалить серверы обновлений "Лаборатории Касперского" в задачах **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилище точек распространения**.

► *Чтобы удалить серверы обновлений "Лаборатории Касперского" в задаче Загрузка обновлений в хранилище Сервера администрирования из источников обновлений:*

1. На вкладке **Устройства** выберите **Задачи**.
2. Выберите задачу **Загрузка обновлений в хранилище Сервера администрирования**.
3. В окне свойств задачи перейдите в раздел **Параметры приложения**.
4. В подразделе **Источники обновлений** перейдите по ссылке **Настроить**.
5. В окне **Источники обновлений** удалите значение *Серверы обновлений "Лаборатории Касперского"*.
6. Нажмите на кнопку **ОК**.

Настройку необходимо выполнить для задачи **Загрузка обновлений в хранилище Сервера администрирования** и для задачи **Загрузка обновлений в хранилище точек распространения** для всех точек распространения.

Способ активации Сервера администрирования

Сервер администрирования необходимо активировать только при помощи файлов ключа.

► *Чтобы активировать Сервер администрирования с помощью файла ключа:*

1. Выберите Сервер администрирования, который вы хотите активировать.
2. Нажмите на кнопку **Свойства**.
Откроется окно свойств Сервера администрирования.
3. В открывшемся окне свойств Сервера администрирования выберите вкладку **Общие** → **Лицензионные ключи**.
4. В поле **Действующая лицензия** укажите файл ключа, на основании которого ключ будет добавлен в приложение.
5. Нажмите на кнопку **ОК**.

Сервер администрирования необходимо активировать при помощи файлов ключа, так как при активации приложения с помощью кода активации приложения регулярно отправляет запросы на серверы активации "Лаборатории Касперского" для проверки текущего статуса ключа.

Служба прокси-сервера активации "Лаборатории Касперского"

Необходимо отключить службу прокси-сервера активации "Лаборатории Касперского".

► *Чтобы отключить службу прокси-сервера активации "Лаборатории Касперского":*

1. Откройте список служб вашего устройства.
2. Выберите в списке службу прокси-сервера активации "Лаборатории Касперского".
3. В контекстном меню службы выберите раздел **Свойства**.
4. В окне свойства службы на вкладке **Общие** в поле **Тип запуска** выберите значение **Отключена**.
5. Нажмите на кнопку **Остановить**.
6. Нажмите на кнопку **ОК**.

Служба прокси-сервера активации "Лаборатории Касперского" остановлена.

Доверенные каналы с использованием SSL-протокола

Для гарантированной доставки информации по доверенному каналу необходимо настроить использование SSL-соединений. В сертифицированной конфигурации приложение должно использовать только доверенные каналы. Для этого на устройстве с установленным Сервером администрирования необходимо закрыть не использующие SSL-протоколы порты, по которым происходит соединение с Сервером администрирования извне. По умолчанию используется порт 14000. В политике Агента администрирования необходимо настроить использование SSL-соединения.

► *Чтобы настроить использование SSL-соединения в политике Агента администрирования:*

1. В разделе **Устройства** выберите раздел **Политики и профили политик**.
2. Выберите политику **Агент администрирования**.
Откроется окно свойств политики.
3. В окне свойств политики перейдите в раздел **Параметры приложения**.
4. Выберите подраздел **Сеть**.
5. В подразделе **Сеть** выберите вложенный раздел **Подключения** и нажмите на кнопку **Параметры**.
6. В окне свойств профиля подключения установите флажок **Использовать SSL-соединение**.
Флажок **Использовать SSL-соединение** необходимо установить для всех профилей подключений.
7. Нажмите на кнопку **ОК**.

Подключение Агента администрирования к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

Права пользователей

Внутренним пользователям Kaspersky Security Center должны быть назначены минимально необходимые права для выполнения их функций в приложении. Для этого вы можете назначить пользователю или группе пользователей роль с набором прав на работу с Сервером администрирования.

► *Чтобы назначить роль пользователю или группе пользователей:*

1. В разделе **Пользователи и роли** выберите раздел **Пользователи**.
2. В поле **Полное имя** выберите пользователя или группу пользователей, которым нужно присвоить роль.

Если пользователь или группа отсутствуют в поле, добавьте их по кнопке **Добавить**.

3. Перейдите на вкладку **Роли** и нажмите на кнопку **Добавить**.

Откроется окно **Роли пользователей**. В окне отображаются созданные роли пользователей.

4. В окне **Роли пользователей** выберите роль для группы пользователей.
5. Нажмите на кнопку **ОК**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе пользователей. Назначенные роли отображаются на вкладке **Роли** в разделе **Безопасность** окна свойств Сервера администрирования.

Условия для статуса "Критический"

При обнаружении на устройстве хотя бы одного вируса необходимо настроить на нем изменение статуса на *Критический*.

► *Чтобы настроить изменение статуса устройства на Критический:*

1. В разделе **Устройства** выберите **Изменить группы**.
2. Выберите группу администрирования.
В результате откроется окно свойств группы администрирования.
3. В окне свойств перейдите в раздел **Статус устройства**.
4. В блоке **Критический** в графе **Установить статус "Критический", если:** выберите и установите тогл для условия **Найдено много вирусов**.
5. Нажмите на кнопку **Изменить**.
6. Для условия **Найдено много вирусов** установите значение 1.
7. Нажмите на кнопку **Сохранить**.

Изменение статуса устройства на *Критический*, при обнаружении на нем хотя бы одного вируса, настроено.

Максимальное количество событий, хранящихся в базе данных Сервера администрирования

Установите максимальное количество событий, хранящихся в базе данных Сервера администрирования, необходимое для проведения аудита приложения. Рекомендуется хранить не менее 400 000 событий в базе данных Сервера администрирования.

► *Чтобы изменить максимальное количество событий, хранящихся в базе данных Сервера администрирования:*

1. Выберите Сервер администрирования, для которого нужно настроить максимальное количество событий, хранящихся на Сервере.
2. Нажмите на кнопку **Свойства**.
Откроется окно свойств Сервера администрирования.
3. На вкладке **Общие** выберите **Хранилище событий**.
4. В поле **Максимальное количество событий, хранящихся в базе данных** установите рекомендуемое значение, не меньше 400 000 событий.

Максимальное количество событий, хранящихся в базе данных Сервера администрирования, установлено.

По умолчанию емкость базы данных Сервера администрирования составляет 400 000 событий. Максимальная рекомендованная емкость базы данных – 15 000 000 событий. Если количество событий в базе данных достигает указанного администратором максимального значения, приложение удаляет самые старые события и записывает новые.

Срок хранения событий

Для проведения аудита приложения, необходимо настроить срок хранения событий в базе данных Сервера администрирования.

► *Чтобы изменить срок хранения событий:*

1. Выберите Сервер администрирования, для которого нужно настроить срок хранения изменений объектов.
2. Нажмите на кнопку **Свойства**.
Откроется окно свойств Сервера администрирования.
3. В окне свойств Сервера администрирования выберите раздел **Настройка событий**.
4. Установите время хранения событий по уровню их важности:
 - На вкладке **Критическое событие** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
 - На вкладке **Отказ функционирования** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
 - На вкладке **Предупреждение** выберите нужное событие установите необходимое значение (не меньше 90 дней).
 - На вкладке **Информационное сообщение** выберите нужное событие установите необходимое значение (не меньше 30 дней).
5. Нажмите на кнопку **ОК**.

Срок хранения событий изменен.

Срок хранения событий можно настроить также в свойствах политики Сервера администрирования.

► *Чтобы настроить срок хранения событий в свойствах политики Сервера администрирования:*

1. В разделе **Устройства** выберите раздел **Политики и профили политики**.
 2. В поле **Имя политики** выберите политику, для которой нужно настроить срок хранения событий.
Откроется окно свойств политики.
 3. В окне свойств политики Сервера администрирования перейдите в раздел **Настройка событий**.
 4. Установите время хранения событий, в зависимости от уровня важности событий:
 - На вкладке **Критическое событие** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
 - На вкладке **Отказ функционирования** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
 - На вкладке **Предупреждение** выберите нужное событие установите необходимое значение (не меньше 90 дней).
 - На вкладке **Информационное сообщение** выберите нужное событие установите необходимое значение (не меньше 30 дней).
 5. Нажмите на кнопку **ОК**.
- Срок хранения событий изменен.

Срок хранения ревизии изменений объектов

Необходимо настроить срок хранения ревизии объектов, необходимый для проведения аудита приложения. Рекомендуемый срок хранения ревизии изменения объектов 90 дней. Такой срок достаточен для проведения регулярного аудита приложения.

► *Чтобы изменить срок хранения ревизии изменения объектов, выполните следующие действия:*

1. Выберите Сервер администрирования, для которого нужно настроить срок хранения изменений объектов.
 2. Нажмите на кнопку **Свойства**.
Откроется окно свойств Сервера администрирования.
 3. В окне свойств Сервера администрирования на вкладке **Общие** выберите раздел **Хранилище истории ревизии**.
 4. В поле **Срок хранения ревизии изменения объекта** установите значение не меньше 90.
 5. Нажмите на кнопку **Сохранить**.
- Срок хранения ревизии изменения объектов изменен.

Права доступа к возможностям шифрования

Настройте запрет доступа к возможностям шифрования данных для всех ролей и пользователей.

► *Чтобы запретить доступ роли к возможностям шифрованию данных, выполните следующие действия:*

1. Выберите Сервер администрирования.

2. Нажмите на кнопку **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Роли пользователей**.
4. Выберите роль и нажмите на кнопку **Изменить**.
5. В окне свойств роли пользователей перейдите в раздел **Права**.
6. В блоке прав для приложения Kaspersky Endpoint Security в области **Шифрование** установите флажок **Запретить**.

Шифрование данных для выбранной запрещено.

► *Чтобы запретить доступ пользователя к возможностям шифрованию данных, выполните следующие действия:*

1. Выберите Сервер администрирования.
2. Нажмите на кнопку **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Безопасность**.
4. Выберите пользователя и перейдите на вкладку **Права**.
5. На вкладке **Права** в блоке прав для приложения Kaspersky Endpoint Security в области **Шифрование** установите флажок **Запретить**.

Шифрование данных для выбранного пользователя запрещено.

Контроль целостности исполняемых модулей приложения

Запустите утилиту klscmodchk для проверки целостности исполняемых модулей приложения, как описано в инструкции (см. раздел "Проверка целостности модулей с помощью утилит klscmodchk и integrity_checker" на стр. 1629).

Выключение объявлений, связанных с безопасностью

Выключите объявления "Лаборатории Касперского", связанные с безопасностью, как описано в инструкции (см. раздел "Выключение объявлений "Лаборатории Касперского"" на стр. [1557](#)).

Справочное руководство API

Справочное руководство по Kaspersky Security Center OpenAPI предназначено для решения следующих задач:

- Автоматизация и настройка. Вы можете автоматизировать задачи, которые, возможно, не хотите выполнять вручную, с помощью Консоли администрирования. Вы также можете использовать собственные сценарии, которые еще не поддерживаются в Консоли администрирования. Например, как администратор вы можете использовать Kaspersky Security Center OpenAPI для создания и запуска сценариев, которые упростят разработку структуры групп администрирования и поддержат ее в актуальном состоянии.
- Пользовательская разработка. Например, вы можете разработать альтернативную Консоль администрирования на основе консоли Microsoft Management Console (MMC) для своих клиентов, которая разрешает ограниченный набор действий.

Вы можете использовать поле поиска в правой части экрана, чтобы найти нужную информацию в справочном руководстве OpenAPI.



Справочное руководство OpenAPI <https://support.kaspersky.com/help/KSC/15.1/KSCAPI/index.html>

Примеры сценариев

Справочное руководство по OpenAPI содержит примеры сценариев Python, перечисленные в таблице ниже. Примеры показывают, как вы можете вызывать методы OpenAPI и автоматически выполнять различные задачи по защите вашей сети, например, создавать иерархию "главный/подчиненный", запускать задачи в Kaspersky Security Center или назначать точки распространения. Вы можете запускать примеры как есть или создавать собственные сценарии на их основе.

► Чтобы вызвать методы OpenAPI и запустить сценарии:

1. Загрузите архив KIAkOAPI.tar.gz <https://support.kaspersky.com/help/KSC/15.1/KSCAPI/common/KIAkOAPI-15.1.tar.gz>. Этот архив включает в себя пакет KIAkOAPI и примеры (их можно скопировать из архива или справочного руководства по OpenAPI). Также архив KIAkOAPI.tar.gz находится в папке установки Kaspersky Security Center Linux.
2. Установите пакет KIAkOAPI <https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00454.html> из из архива KIAkOAPI.tar.gz на устройстве, на котором установлен Сервер администрирования.

Вызывать методы OpenAPI, запускать примеры и свои сценарии можно только на устройствах, на которых установлены Сервер администрирования и пакет KIAkOAPI.

Таблица 106. Сопоставление пользовательских сценариев и примеров методов Kaspersky

Пример	Назначение примера	Сценарий
Журнал событий KIAkParams https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00437.html	Вы можете извлекать и обрабатывать данные, используя <code>KIAkParams</code> структуру данных. В примере показано, как работать с этой структурой данных. Пример вывода может быть представлен по-разному. Вы можете получить данные для отправки HTTP-метода или использовать их в своем коде.	Мониторинг и отчеты
Создание и удаление иерархии "главный/подчиненный" https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00438.html	Вы можете добавить подчиненный Сервер администрирования и установить таким образом отношение иерархии "главный Сервер – подчиненный Сервер". Или вы можете исключить подчиненный Сервер администрирования из иерархии.	- Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования (см. стр. 1020) - Удаление иерархии Серверов администрирования (см. стр. 1023)
Создайте иерархию группы со структурой на основе подразделения Active Directory. https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00439.html	Вы можете выполнить опрос подразделения Active Directory и сформировать иерархию обнаруженных групп устройств.	Создание групп администрирования (на стр. 1194)
Создайте иерархию группы со структурой на основе кешированного подразделения Active Directory. https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00440.html	Вы можете сформировать иерархию групп управляемых устройств на основе ранее выполненного опроса подразделения Active Directory. Если новые устройства появляются в Active Directory после последнего опроса, они будут добавлены в группу, так как их нет в сохраненных результатах опроса.	Создание групп администрирования (на стр. 1194)

Пример	Назначение примера	Сценарий
Загрузите файлы списка сетей с помощью шлюза соединения на указанное устройство https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00441.html	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем загрузить файл со списком сетей на свой компьютер.	Настройка точек распространения и шлюзов соединений (на стр. 685)
Установить лицензионный ключ, хранящийся в хранилище главного Сервера администрирования, на подчиненные Серверы администрирования https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00442.html	Вы можете подключиться к главному Серверу администрирования, загрузить с него необходимый лицензионный ключ и передать этот ключ на все подчиненные Серверы администрирования, входящие в иерархию.	Лицензирование управляемых приложений
Создайте отчет об эффективных правах пользователей https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00443.html	Вы можете создать разные отчеты https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00032.html . Например, вы можете сгенерировать отчет об эффективных правах пользователя, используя этот пример. В этом отчете представлена информация о правах, которыми обладает пользователь в зависимости от его группы и роли. Вы можете загрузить отчет в формате HTML, PDF или Excel.	Генерация и просмотр отчета (на стр. 1479)
Запустить задачу для устройства. https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00444.html	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем запустить необходимую задачу.	Запуск задачи вручную (см. стр. 1175)

Пример	Назначение примера	Сценарий
Создание IP-подсетей на основе сайта и служб Active Directory https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00445.html	Вы можете создать IP-подсеть на основе используемого подразделения Active Directory. В примере запускается опрос указанного диапазона IP-адресов и удаляются обнаруженные подсети, чтобы избежать их конфликта с новой подсетью. Поэтому не запускайте такой пример в сети, где важно сохранить подсети. После опроса пример кода обращается к Active Directory, проверяет каждое устройство в нем и создает IP-подсеть. Для этого в примере используются маски и IP-адреса всех устройств.	Настройка защиты сети (на стр. 401)
Регистрация точек распространения для устройств в группе https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00446.html	Вы можете назначить управляемые устройства точками распространения (ранее они назывались "агенты обновлений").	Обновление баз и приложений "Лаборатории Касперского" (на стр. 1335)
Перечисление всех групп https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00447.html	Вы можете выполнять различные действия с группами администрирования. В примере показано, как выполнить следующее: • Получить идентификатор корневой группы "Управляемые устройства". • Переместить по иерархии групп. • Получить полную развернутую иерархию групп с их именами и вложенностью.	Настройка Сервера администрирования (см. стр. 1016)
Перечисление задач, запрос статистики задач и запуск задач https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00448.html	Вы можете ознакомиться со следующей информацией: • Историей выполнения задачи. • Текущим статусом задачи. • Количеством задач в разных статусах. Вы также можете запустить задачу. По умолчанию пример запускает задачу после вывода статистики.	Наблюдение за ходом выполнения задачи

Пример	Назначение примера	Сценарий
Создание и запуск задачи https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00449.html	Вы можете создать задачу. Укажите в примере следующие параметры задачи: • Тип. • Способ запуска. • Название. • Группа устройств, для которой будет использоваться задача. По умолчанию в примере создается задача типа "Показать сообщение". Вы можете запустить эту задачу для всех управляемых устройств Сервера администрирования. При необходимости вы можете указать свои параметры задачи https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00030.html.	Создание задачи
Перечисление лицензионных ключей https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00450.html	Вы можете получить список всех активных лицензионных ключей для приложений "Лаборатории Касперского", установленных на управляемых устройствах Сервера администрирования. Список содержит подробные сведения https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00122.html о каждом лицензионном ключе, такие как имя, тип или срок действия.	Просмотр информации об используемых лицензионных ключах
Создание и поиск внутреннего пользователя https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00451.html	Вы можете создать учетную запись для дальнейшей работы.	Выбор учетной записи для запуска Сервера администрирования
Создание пользовательской категории https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00452.html	Вы можете создать категорию программ с требуемыми параметрами https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00460.html .	Создание пополняемой вручную категории приложений (на стр. 1446)
Перечисление пользователей с помощью SrvView https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00453.html	Вы можете использовать класс SrvView https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00599.html для запроса подробной информации https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00159.html с Сервера администрирования. Например, вы можете получить список пользователей, используя этот пример.	Управление учетными записями пользователей

Приложения, взаимодействующие с Kaspersky Security Center через OpenAPI

Некоторые приложения взаимодействуют с Kaspersky Security Center через OpenAPI. К таким приложениям относятся, например, Kaspersky Anti Targeted Attack Platform или Kaspersky Security для виртуальных сред. Это также может быть пользовательское клиентское приложение, разработанное вами на основе OpenAPI.

Приложения, взаимодействующие с Kaspersky Security Center через OpenAPI, подключаются к Серверу администрирования. Если вы настроили список разрешенных IP-адресов для подключения к Серверу администрирования, добавьте IP-адреса устройств, на которых установлены приложения, использующие Kaspersky Security Center OpenAPI. Чтобы узнать, работает ли используемое вами приложение с OpenAPI, обратитесь к справке этого приложения.

Руководство по масштабированию

В этом руководстве представлена информация по масштабированию Kaspersky Security Center
<https://support.kaspersky.com/KSC/15.1/ru-RU/162088.htm>.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки	1616
Техническая поддержка через Kaspersky CompanyAccount	1617
Получение файлов дампа Сервера администрирования	1617

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Security Center, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Security Center.

Kaspersky предоставляет поддержку Kaspersky Security Center в течение жизненного цикла (см. страницу жизненного цикла приложений (<https://support.kaspersky.ru/corporate/lifecycle>)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules/ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки (<https://support.kaspersky.com/b2b>);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

Получение файлов дампа Сервера администрирования

Файлы дампа Сервера администрирования содержат всю информацию о процессах Сервера администрирования на определенный момент времени. Файлы дампа Сервера администрирования хранятся в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps. Файлы дампа хранятся, пока используется Kaspersky Security Center, и удаляются безвозвратно при удалении приложения. Файлы дампа не отправляются в "Лабораторию Касперского" автоматически.

В случае сбоя Сервера администрирования вы можете обратиться в Службу технической поддержки "Лаборатории Касперского". Специалист Службы технической поддержки может попросить вас отправить файлы дампа Сервера администрирования для дальнейшего анализа в "Лаборатории Касперского".

Файлы дампа могут содержать персональные данные. Перед отправкой в "Лабораторию Касперского" рекомендуется защитить информацию от несанкционированного доступа.

Источники информации о приложении

Страница Kaspersky Security Center на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security Center (<https://www.kaspersky.com/small-to-medium-business-security/security-center>) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Security Center в Базе знаний

База знаний – это раздел на веб-сайте Службы технической поддержки "Лаборатории Касперского".

На странице Kaspersky Security Center в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи в Базе знаний могут дать ответы на вопросы, связанные с Kaspersky Security Center и с другими приложениями "Лаборатории Касперского". Также в статьях Базы знаний могут быть новости Службы технической поддержки.

Обсуждение приложений "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме

(<https://forum.kaspersky.com/forum/%D1%80%D1%83%D1%81%D1%81%D0%BA%D0%BE%D1%8F%D0%B7%D1%8B%D1%87%D0%BD%D1%8B%D0%B9-%D1%84%D0%BE%D1%80%D1%83%D0%BC-162/>).

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Для отображения справки требуется соединение с интернетом.

Если вы не нашли решения вашего вопроса, обратитесь в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. [1616](#)).

Глоссарий

А

AWS Application Program Interface (AWS API)

Программный интерфейс приложения платформы AWS, который используется приложением Kaspersky Security Center. Средствами AWS API проводится, в частности, опрос облачных сегментов и установка Агента администрирования на инстансы.

С

Cloud Discovery

Cloud Discovery представляет собой компонент решения Cloud Access Security Broker (CASB), которое предназначено для защиты облачной инфраструктуры организации. Cloud Discovery управляет доступом пользователей к облачным сервисам. К облачным сервисам относятся, например, Microsoft Teams, Salesforce, Microsoft Office 365. Облачные сервисы сгруппированы в категории, например, категории *Обмен данными*, *Мессенджеры*, *Электронная почта*.

Connection gateway

Шлюз соединения – это Агент администрирования, работающий в особом режиме. Шлюз соединения принимает соединения от других Агентов администрирования и туннелирует их к Серверу администрирования через собственное соединение с Сервером. В отличие от обычного Агента администрирования, шлюз соединения ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования.

Е

Event repository

A part of the Administration Server database dedicated to storage of information about events that occur in Kaspersky Security Center.

Н

HTTPS

Безопасный протокол передачи данных между браузером и веб-сервером с использованием шифрования. HTTPS используется для доступа к закрытой информации, такой как корпоративные или финансовые данные.

И

IAM-пользователь

Пользователь сервисов AWS. IAM-пользователь может обладать правами на опрос облачного сегмента.

IAM-роль

Совокупность прав для выполнения запросов к сервисам AWS. IAM-роли не связаны ни с каким конкретным пользователем или группой и обеспечивают права доступа без использования ключей доступа IAM AWS. IAM-роль можно присвоить пользователям IAM, экземплярам EC2, приложениям или сервисам AWS.

Identity and Access Management (IAM)

Сервис AWS, который позволяет управлять доступом пользователей к другим сервисам и ресурсам AWS.

iOS MDM-профиль

Набор параметров подключения мобильных устройств iOS к Серверу администрирования. iOS MDM-профиль устанавливается пользователем на мобильное устройство, после чего это мобильное устройство подключается к Серверу администрирования.

iOS MDM-устройство

Мобильное устройство, которое подключается к Серверу iOS MDM по протоколу iOS MDM. По протоколу iOS MDM могут подключаться и управляться устройства с операционной системой iOS.

Ж

JavaScript

Язык программирования, расширяющий возможности веб-страниц. Веб-страницы, созданные с использованием JavaScript, способны выполнять дополнительные действия (например, изменять вид элементов интерфейса или открывать дополнительные окна) без обновления веб-страницы данными с веб-сервера. Чтобы просматривать веб-страницы, созданные с использованием JavaScript, в параметрах браузера надо включить поддержку JavaScript.

К

Kaspersky Security Center System Health Validator (SHV)

Компонент приложения Kaspersky Security Center, предназначенный для проверки работоспособности операционной системы при совместной работе приложения Kaspersky Security Center с Microsoft NAP.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

KES-устройство

Мобильное устройство, которое подключается к Серверу администрирования и управляется с помощью мобильного приложения Kaspersky Endpoint Security для Android.

M

MITM-атака

Man in The Middle (человек посередине). Атака на IT-инфраструктуру организации, при которой злоумышленник перехватывает канал связи между двумя точками доступа, ретранслирует и при необходимости изменяет связь между этими точками доступа.

P

Provisioning-профиль

Набор параметров для работы приложений на мобильных устройствах iOS. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

S

SSL

Протокол шифрования данных в локальных сетях и в интернете. SSL используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

W

Windows Server Update Services (WSUS)

Приложение, которое используется для распространения обновлений приложений Microsoft на компьютерах пользователей в сети организации.

A

Агент администрирования

Компонент приложений Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех приложений компании для Windows. Для приложений "Лаборатории Касперского" для Novell®, Unix™ и Mac существуют отдельные версии Агента администрирования.

Агент аутентификации

Интерфейс, позволяющий после шифрования загрузочного жесткого диска пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы.

Агент обновлений

Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, удаленной установки приложений, получения информации об устройствах в составе группы администрирования и/или широковеб-домена. Агенты обновлений предназначены для уменьшения нагрузки на Сервер администрирования при распространении обновлений и для оптимизации

трафика в сети. Агенты обновлений могут быть назначены автоматически Сервером администрирования или вручную администратором.

Административные права

Уровень прав и полномочий пользователя для администрирования объектов Exchange внутри организации Exchange.

Администратор Kaspersky Security Center

Лицо, управляющее работой приложения через систему удаленного централизованного администрирования Kaspersky Security Center.

Администратор клиента

Сотрудник организации-клиента, который отвечает за обеспечение антивирусной безопасности организации-клиента.

Администратор поставщика услуг

Сотрудник организации-поставщика услуг антивирусной защиты. Выполняет работы по установке, эксплуатации систем антивирусной защиты, созданных на основе решений "Лаборатории Касперского", а также осуществляет техническую поддержку клиентов.

Активный ключ

Ключ, используемый в текущий момент для работы приложения.

Антивирусная безопасность сети

Комплекс технических и организационных мер, снижающих вероятность проникновения на устройства сети организации вирусов и спама, предотвращающих сетевые атаки, фишинг и другие угрозы. Антивирусная безопасность сети повышается при использовании приложений защиты и сервисов, а также при наличии и соблюдении политики информационной безопасности в организации.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

В

Веб-сервер Kaspersky Security Center

Компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

Виртуальный Сервер администрирования

Компонент приложения Kaspersky Security Center, предназначенный для управления системой защиты сети организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования при работе использует основную базу данных главного Сервера администрирования. Задачи резервного копирования и восстановления данных, а также задачи проверки и загрузки обновлений, не поддерживаются на виртуальном Сервере администрирования.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Вирусная атака

Ряд целенаправленных попыток заразить устройство вирусом.

Владелец устройства

Владелец устройства – это пользователь устройства, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с устройством.

Внутренние пользователи

Учетные записи внутренних пользователей используются для работы с виртуальными Серверами администрирования. Под именем учетной записи внутреннего пользователя администратор виртуального Сервера может запускать Kaspersky Security Center Web Console для просмотра сведений о состоянии антивирусной безопасности сети. В рамках функциональности приложения Kaspersky Security Center внутренние пользователи обладают правами реальных пользователей.

Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

Восстановление данных Сервера администрирования

Восстановление данных Сервера администрирования при помощи утилиты резервного копирования на основании информации, сохраненной в резервном хранилище. Утилита позволяет восстанавливать:

- информационную базу Сервера администрирования (политики, задачи, параметры приложения, сохраненные на Сервере администрирования события);

- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Г

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором приложений "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждого из установленных в группе приложений могут быть созданы групповые политики и сформированы групповые задачи.

Группа лицензионных программ

Группа программ, созданная на основании заданных администратором критериев (например, по производителю), для которых ведется учет установок на клиентских устройствах.

Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех клиентских устройствах, входящих в состав этой группы администрирования.

Д

Демилитаризованная зона (DMZ)

Демилитаризованная зона – это сегмент локальной сети, в которой находятся серверы, отвечающие на запросы из глобальной сети. В целях обеспечения безопасности локальной сети организации доступ в локальную сеть из демилитаризованной зоны ограничен и защищен сетевым экраном.

Домашний Сервер администрирования

Домашний Сервер администрирования – это Сервер администрирования, который был задан при установке Агента администрирования. Домашний Сервер администрирования может использоваться в параметрах профилей подключения Агента администрирования.

Дополнительный ключ

Ключ, подтверждающий право на использование приложения, но не используемый в текущий момент.

Доступное обновление

Пакет обновлений модулей приложения "Лаборатории Касперского", в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре приложения.

3

Задача

Функции, выполняемые приложением "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Задача для набора устройств

Задача, определенная для набора клиентских устройств из произвольных групп администрирования и выполняемая на них.

И

Инсталляционный пакет

Набор файлов, формируемый для удаленной установки приложения "Лаборатории Касперского" при помощи системы удаленного управления Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки приложения и обеспечения его работоспособности сразу после установки. Значения параметров соответствуют значениям параметров приложения по умолчанию. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива приложения.

Инстанс Amazon EC2

Виртуальная машина, созданная на основе образа AMI с использованием Amazon Web Services.

К

Клиент Сервера администрирования (Клиентское устройство)

Устройство, сервер или рабочая станция, на котором установлены Агент администрирования и управляемые приложения "Лаборатории Касперского".

Ключ доступа IAM AWS

Комбинация, состоящая из ID ключа (вида "AKIAIOSFODNN7EXAMPLE") и секретного ключа (вида "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Пара принадлежит IAM-пользователю и используется для получения доступа к сервисам AWS.

Консоль AWS

Веб-интерфейс для управления инстансами Amazon EC2. Консоль AWS доступна в интернете на странице <https://aws.amazon.com/console/>.

Консоль администрирования

Компонент приложения Kaspersky Security Center, предоставляющий пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

Конфигурационный профиль

Политика, содержащая набор параметров и ограничений для мобильного устройства iOS MDM.

Л

Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском устройстве.

Локальная установка

Установка приложения защиты на устройство сети организации, которая предусматривает ручной запуск установки из дистрибутива приложения защиты или ручной запуск опубликованного инсталляционного пакета, предварительно загруженного на устройство.

М

Магазин приложений

Компонент приложения Kaspersky Security Center. Магазин приложений используется для установки приложений на Android-устройства пользователей. В магазине приложений можно публиковать арк-файлы приложений и ссылки на приложения в Google Play.

Н

Настройки задачи

Настройки работы приложения, специфичные для каждого типа задач.

Непосредственное управление приложением

Управление приложением через локальный интерфейс.

Несовместимое приложение

Антивирусное приложение стороннего производителя или приложение "Лаборатории Касперского", не поддерживающее управление через Kaspersky Security Center.

О

Облачное окружение

Виртуальные машины на базе облачной платформы, объединенные в сети.

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Образ AMI

Шаблон с необходимой для запуска виртуальной машины конфигурацией программного обеспечения. На основе одного образа AMI можно создать несколько инстансов.

Общий сертификат

Сертификат, предназначенный для идентификации мобильного устройства пользователя.

Оператор Kaspersky Security Center

Пользователь, который ведет наблюдение за состоянием и работой системы защиты, управляемой при помощи Kaspersky Security Center.

П

Параметры приложения

Параметры работы приложения, общие для всех типов его задач и отвечающие за работу приложения в целом, например: параметры производительности приложения, параметры ведения отчетов, параметры резервного хранилища.

Плагин управления приложением

Специализированный компонент, предоставляющий интерфейс для управления работой приложения через Консоль администрирования. Для каждого приложения существует свой плагин управления. Он входит в состав всех приложений "Лаборатории Касперского", управление которыми может осуществляться при помощи Kaspersky Security Center.

Политика

Политика определяет параметры работы приложения и доступ к настройке приложения, установленного на устройствах группы администрирования. Для каждого приложения требуется создать свою политику. Вы можете создать неограниченное количество различных политик для приложений, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться одновременно к каждому приложению.

Порог вирусной активности

Максимально допустимое количество событий заданного типа в течение ограниченного времени, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Поставщик услуг антивирусной защиты

Организация, предоставляющая услуги антивирусной защиты сетей организации-клиента на основе решений "Лаборатории Касперского".

Р

Рабочее место администратора

Устройство, на котором установлена Консоль администрирования – компонент, предоставляющий интерфейс управления Kaspersky Security Center.

С рабочего места администратор управляет серверной частью Kaspersky Security Center: выстраивает систему централизованной защиты сети организации, сформированную на базе приложений "Лаборатории Касперского", и контролирует ее.

Резервное копирование данных Сервера администрирования

Копирование данных Сервера администрирования для резервного хранения и последующего восстановления, осуществляемое при помощи утилиты резервного копирования. Утилита позволяет сохранять:

- информационную базу Сервера администрирования (политики, задачи, параметры приложения, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Руководство по усилению защиты

Рекомендации и особенности настройки Kaspersky Security Center Linux и его компонентов для снижения рисков его компрометации.

Ручная установка

Установка приложения защиты на устройство сети организации из дистрибутива приложения защиты. Ручная установка требует непосредственного участия администратора или другого IT-специалиста. Обычно ручная установка применяется, если удаленная установка завершилась с ошибкой.

С

Сервер iOS MDM

Компонент Kaspersky Security Center, который устанавливается на клиентское устройство и позволяет подключать мобильные устройства iOS к Серверу администрирования и управлять ими с помощью сервиса Apple Push Notifications (APNs).

Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

Сервер мобильных устройств

Компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования.

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.

Сертификат Сервера администрирования

Сертификат, на основании которого осуществляется аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмене информацией с клиентскими устройствами. Сертификат Сервера администрирования создается при установке Сервера администрирования и хранится на Сервере администрирования в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности устройства.

Состояние защиты сети

Текущее состояние защиты, характеризующее степень защищенности устройств сети организации. Состояние защиты сети включает такие факторы, как наличие на устройствах сети установленных приложений защиты, использование ключей, количество и виды обнаруженных угроз.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями приложения и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

У

Удаленная установка

Установка приложений "Лаборатории Касперского" при помощи инструментов, предоставляемых приложением Kaspersky Security Center.

Управляемые устройства

Устройства сети организации, включенные в одну из групп администрирования.

Уровень важности патча

Характеристика патча. Для патчей сторонних производителей или Microsoft существует пять уровней важности:

- Предельный.
- Высокий.

- Средний.
- Низкий.
- Неизвестно.

Уровень важности патча стороннего производителя или Microsoft определяется наиболее неблагоприятным уровнем критичности уязвимости, которую закрывает патч.

Уровень важности события

Характеристика события, зафиксированного в работе приложения "Лаборатории Касперского". Существуют четыре уровня важности:

- Критическое событие.
- Отказ функционирования.
- Предупреждение.
- Информационное сообщение.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Устройство с защитой на уровне UEFI

Устройство со встроенным на уровне BIOS программным обеспечением Антивирус Касперского для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска приложения защиты.

Уязвимость

Недостаток в операционной системе или приложении, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или приложение и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных приложений.

Ф

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать приложение "Лаборатории Касперского" по пробной или коммерческой лицензии. Вы можете использовать приложение только при наличии файла ключа.

Форсированная установка

Метод удаленной установки приложения "Лаборатории Касперского", который позволяет провести удаленную установку программного обеспечения на конкретные клиентские устройства. Для успешного выполнения задачи методом форсированной установки учетная запись для запуска задачи должна

обладать правами на удаленный запуск приложений на клиентских устройствах. Данный метод рекомендуется для установки приложений на устройства, работающие под управлением операционных систем Microsoft Windows NT / 2000 / 2003 / XP, в которых поддерживается такая возможность.

Х

Хранилище резервных копий

Специальная папка для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

Ц

Централизованное управление приложением

Удаленное управление приложением при помощи сервисов администрирования, предоставляемых Kaspersky Security Center.

Ш

Широковещательный домен

Логический участок компьютерной сети, в котором все узлы могут передавать данные друг другу с помощью широковещательного канала на уровне сетевой модели OSI (Open Systems Interconnection Basic Reference Model).

Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft, MultiPoint, MS-DOS, PowerShell, PowerPoint, SQL Server, OneNote, Outlook, Tahoma, Win32, Windows, Windows PowerShell, Windows Server, Windows Phone, Windows Vista, Windows Azure – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах. являются товарными знаками группы компаний Microsoft.

Adobe является либо зарегистрированным товарным знаком, либо товарным знаком компании Adobe в США и/или других странах.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, Touch ID – товарные знаки Apple Inc. – товарные знаки Apple Inc.

AMD, AMD64 – товарные знаки или зарегистрированные товарные знаки Advanced Micro Devices, Inc.

Apache является либо зарегистрированным товарным знаком, либо товарным знаком Apache Software Foundation.

BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Cisco, Cisco Systems, IOS являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Citrix, XenServer являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Android, Chrome, Dalvik, Google, Google Play, Google Карты, Google Analytics, Hangouts, YouTube – товарные знаки Google, Inc. – товарные знаки Google LLC.

Firefox является товарным знаком Mozilla Foundation в США и других странах.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

JavaScript, Python, TouchDown, Oracle и Java – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

QRadar, IBM – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Intel, Xeon – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CentOS, Fedora, Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Novell – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

Parallels, логотип Parallels и Coherence являются товарными знаками или зарегистрированными товарными знаками Parallels International GmbH.

SPL, Splunk – товарные знаки и зарегистрированные в США и других странах товарные знаки Splunk, Inc.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

VMware, VMware vSphere – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

Список ограничений

Kaspersky Security Center Web Console имеет ряд ограничений, не критичных для работы приложения:

- При изменении времени или часовой зоны на устройстве необходимо перезапустить службу Kaspersky Security Center Web Console.
- Если на устройстве используется прокси-сервер и заданы переменные окружения прокси-сервера, приложение установки Kaspersky Security Center Web Console может зависнуть.
- При импорте задачи *Загрузить обновления в хранилища точек распространения* или задачи *Проверка обновлений* параметр **Выбор устройств, которым будет назначена задача** включен. Эти задачи невозможно назначить выборкам устройств или заданным устройствам. Если вы назначите задачу *Загрузить обновления в хранилища точек распространения* или задачу *Проверка обновлений* на определенные устройства, задача будет импортирована некорректно.
- Если вы используете точку распространения с операционной системой Linux с установленным Агентом администрирования версии 15, вы можете опрашивать только те домены Active Directory, для которых вы указываете адрес и учетные данные пользователя. Опрос текущего домена Active Directory и леса доменов Active Directory недоступен.
- Если правило Контроля приложений основано на категории приложений, в которую входят приложения, обнаруженные на устройствах с операционной системой Linux, правило не работает. При выборе приложений из реестра приложений, для их добавления в категорию приложений убедитесь, что вы выбираете приложения, обнаруженные на устройствах с операционной системой Windows.
- Если на устройстве с операционной системой Linux обнаружено приложение из раздела **Реестр приложений**, в свойствах приложения отсутствует информация о связанных с ней исполняемых файлах.
- Если вы устанавливаете Агент администрирования на устройство под управлением операционной системы ALT Linux с помощью задачи удаленной установки и запускаете эту задачу под учетной записью с правами, отличными от root, задача не будет выполнена. Запустите задачу удаленной установки под учетной записью root или создайте и используйте автономный инсталляционный пакет Агента администрирования для локальной установки приложения.
- Если список содержит более 20 записей, которые отображаются на нескольких страницах, и вы установили флажок **Выделить все**, Web Console выбирает только те записи, которые отображаются на текущей странице. Обратите внимание, что это не относится к спискам в разделах **Управляемые устройства**, **Выборки устройств** и **Задачи**, где можно выбрать все элементы из списка.
- Клиентские устройства могут быть не найдены после запуска опроса сети Windows.
- В политике Kaspersky Endpoint Security для Windows при выборе и применении категории приложений при настройке функции Контроля приложений категория применяется, но не отображается как выбранная после сохранения и повторного открытия политики.
- После отключения службы прокси-сервера KSN, устройства в группе Управляемые устройства меняют свой статус на *Критический*, а устройства в подгруппах отображаются со статусом *ОК*.
- Если для базы данных, которую вы используете для Kaspersky Security Center, настроена сортировка с учетом регистра, используйте тот же регистр при указании DNS-имени устройства в правилах перемещения устройств и правилах автоматического назначения тегов. Иначе правила не будут работать.

- Если в **Мастер добавления подчиненного Сервера администрирования** указать учетную запись с включенной двухэтапной проверкой для аутентификации, на будущем подчиненном Сервере, мастер завершает работу с ошибкой. Чтобы решить эту проблему, укажите учетную запись, для которой отключена двухэтапная проверка, или создайте иерархию из будущего подчиненного Сервера.
- При входе в Kaspersky Security Center Web Console, если вы используете доменную аутентификацию и указываете виртуальный Сервер администрирования для подключения, затем выходите из приложения и пытаетесь войти на главный Сервер администрирования, Kaspersky Security Center Web Console все равно подключается к виртуальному Серверу администрирования. Чтобы подключиться к главному Серверу администрирования, повторно откройте браузер.
- Быстрый/полный опрос сети Windows возвращает пустой результат.
- Если вы устанавливаете Kaspersky Security Center Web Console с Identity and Access Manager, а затем меняете Сервер администрирования Kaspersky Security Center Web Console, компонент Identity and Access Manager не получает информацию о новом Сервере администрирования.
- Если вы открываете Kaspersky Security Center Web Console в разных браузерах и загружаете файл сертификата Сервера администрирования в окне свойств Сервера администрирования, загруженные файлы имеют разные имена.
- Ошибка возникает при попытке восстановить объект из хранилища **Резервное хранилище (Операции → Хранилища → Резервное хранилище)** или при отправке объекта в "Лабораторию Касперского".
- Управляемое устройство, имеющее более одного сетевого адаптера, отправляет Серверу администрирования информацию о MAC-адресе сетевого адаптера, отличного от того, который используется для подключения к Серверу администрирования.
- Если вы устанавливаете Kaspersky Security Center Web Console с Identity and Access Manager, а затем меняете Сервер администрирования Kaspersky Security Center Web Console, компонент Identity and Access Manager не получает информацию о новом Сервере администрирования.
- Если вы запустите задачу Удаленное выполнение скриптов для указанной учетной записи и измените в параметрах задачи учетную запись, для которой она назначена, изменения не сохранятся. Чтобы изменить учетную запись, которой назначена задача, остановите задачу в параметрах задачи и перезапустите ее.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 107. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
приложение	продукт, объект оценки, программное изделие
виртуальная инфраструктура VMware	среда функционирования
файл виртуальной машины	объект воздействия
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы приложения	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь