

kaspersky

Kaspersky Endpoint Security для Windows

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 11.3.0.773

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 "Лаборатория Касперского" (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: 17.03.2020

Обозначение документа: 643.46856491.00100-03 90 01

© 2020 АО "Лаборатория Касперского"

<https://www.kaspersky.ru>

<https://support.kaspersky.ru>

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

Оглавление

Об этом документе	11
Источники информации о программе	12
О программе	13
Требования	14
Аппаратные и программные требования	14
Указания по эксплуатации и требования к среде	15
Установка программы с помощью мастера	16
Активация программы с помощью мастера активации программы	20
Удаление программы	21
Процедура приемки	22
Безопасное состояние	22
Проверка работоспособности. Тестовый файл EICAR	22
Разделение доступа к функциям программы по пользовательским ролям	27
Управление программой через Консоль администрирования Kaspersky Security Center	29
Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере	29
Настройка параметров Kaspersky Endpoint Security	30
Управление задачами	31
Настройка режима работы с задачами	33
Создание локальной задачи	34
Создание групповой задачи	34
Создание задачи для выборки устройств	34
Запуск, остановка, приостановка и возобновление выполнения задачи	35
Изменение параметров задачи	37
Параметры задачи инвентаризации	38
Управление политиками	39
Создание политики	40
Изменение параметров политики	41
Индикатор уровня защиты в окне свойств политики	42
Интерфейс программы	43
Значок программы в области уведомлений	45
Упрощенный интерфейс программы	46
Настройка отображения интерфейса программы	47
Запуск и остановка программы	48
Автоматический запуск программы	49
Приостановка и возобновление защиты и контроля компьютера	50
Проверка компьютера	51
Запуск и остановка задачи проверки	52
Изменение уровня безопасности	53
Изменение действия над зараженными файлами	54

Формирование списка проверяемых объектов	54
Выбор типа проверяемых файлов	55
Оптимизация проверки файлов.....	56
Проверка составных файлов	57
Использование методов проверки	58
Использование технологий проверки	58
Выбор режима запуска для задачи проверки.....	59
Настройка запуска задачи проверки с правами другого пользователя	60
Проверка съемных дисков при подключении к компьютеру	60
Фоновая проверка.....	61
Доверенная зона	63
Создание исключения из проверки	65
Изменение исключения из проверки.....	67
Удаление исключения из проверки	68
Запуск и остановка работы исключения из проверки.....	68
Формирование списка доверенных программ.....	69
Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ.....	70
Использование доверенного системного хранилища сертификатов.....	71
Работа с активными угрозами	72
Работа со списком активных угроз.....	72
Запуск задачи выборочной проверки файлов из списка активных угроз	73
Удаление записей из списка активных угроз	73
Обновление баз и модулей программы.....	75
Добавление источника обновлений	76
Выбор региона сервера обновлений	77
Настройка обновления из папки общего доступа	78
Выбор режима запуска для задачи обновления.....	79
Запуск задачи обновления с правами другого пользователя	80
Настройка обновления модулей программы.....	80
Запуск и остановка задачи обновления.....	81
Откат последнего обновления.....	82
Настройка использования прокси-сервера	82
Обновление антивирусных баз в ручном режиме	84
Устранение уязвимостей и установка критических обновлений в программе	85
Kaspersky Security Network.....	86
Включение и выключение использования Kaspersky Security Network.....	87
Включение и выключение облачного режима для компонентов защиты	88
Проверка подключения к Kaspersky Security Network	89
Проверка репутации файла в Kaspersky Security Network.....	90

Анализ поведения.....	92
Включение и выключение Анализа поведения.....	92
Выбор действия при обнаружении вредоносной активности программы.....	93
Защита папок общего доступа от внешнего шифрования.....	93
Включение и выключение защиты папок общего доступа от внешнего шифрования.....	94
Выбор действия при обнаружении внешнего шифрования папок общего доступа.....	94
Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования.....	95
Защита от эксплойтов.....	97
Включение и выключение Защиты от эксплойтов.....	97
Выбор действия при обнаружении эксплойта.....	98
Включение и выключение защиты памяти системных процессов.....	98
Предотвращение вторжений.....	99
Ограничения контроля аудио и видео устройств.....	100
Включение и выключение Предотвращения вторжений.....	102
Работа с группами доверия программ.....	102
Настройка параметров распределения программ по группам доверия.....	104
Изменение группы доверия.....	104
Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security.....	105
Работа с правами программ.....	105
Изменение прав программ для групп доверия и для групп программ.....	106
Изменение прав программы.....	107
Выключение загрузки и обновления прав программ из базы Kaspersky Security Network.....	108
Выключение наследования ограничений родительского процесса.....	108
Исключение некоторых действий программ из прав программ.....	109
Удаление информации о неиспользуемых программах.....	109
Защита ресурсов операционной системы и персональных данных.....	110
Добавление категории защищаемых ресурсов.....	111
Добавление защищаемого ресурса.....	111
Выключение защиты ресурса.....	112
Откат вредоносных действий.....	113
Ограничения функциональности восстановления файлов.....	114
Включение и выключение Отката вредоносных действий.....	114
Защита от файловых угроз.....	115
Включение и выключение Защиты от файловых угроз.....	115
Автоматическая приостановка Защиты от файловых угроз.....	116
Изменение уровня безопасности.....	117
Изменение действия компонента Защита от файловых угроз над зараженными файлами.....	118
Формирование области защиты компонента Защита от файловых угроз.....	118
Использование эвристического анализа в работе компонента Защита от файловых угроз.....	120
Использование технологий проверки в работе компонента Защита от файловых угроз.....	120
Оптимизация проверки файлов.....	121

Проверка составных файлов	121
Изменение режима проверки файлов.....	123
Защита от веб-угроз.....	124
Включение и выключение Защиты от веб-угроз	125
Изменение уровня безопасности веб-трафика	125
Изменение действия над вредоносными объектами веб-трафика	126
Проверка компонентом Защита от веб-угроз ссылок по базам фишинговых и вредоносных веб-адресов	127
Использование эвристического анализа в работе компонента Защита от веб-угроз	128
Формирование списка доверенных веб-адресов	128
Защита от почтовых угроз	130
Включение и выключение Защиты от почтовых угроз	131
Изменение уровня безопасности почты	131
Изменение действия над зараженными сообщениями электронной почты	132
Формирование области защиты компонента Защита от почтовых угроз	132
Проверка составных файлов, вложенных в сообщения электронной почты	134
Фильтрация вложений в сообщениях электронной почты	134
Защита от сетевых угроз	136
Включение и выключение Защиты от сетевых угроз	136
Изменение параметров блокирования атакующего компьютера	136
Настройка адресов исключений из блокирования.....	137
Защита от атак типа MAC-спуфинг	137
Защита от атак BadUSB	139
Включение и выключение Защиты от атак BadUSB	139
Разрешение и запрещение использования экранной клавиатуры при авторизации	139
Авторизация клавиатуры	140
Поставщик AMSI-защиты	141
Включение и выключение Поставщика AMSI-защиты.....	142
Проверка составных файлов Поставщиком AMSI-защиты	142
Контроль программ	144
Ограничения функциональности Контроля программ.....	147
Включение и выключение Контроля программ	149
Действия с правилами Контроля программ	149
Добавление и изменение правила Контроля программ.....	152
Добавление условия срабатывания в правило Контроля программ	153
Изменение статуса правила Контроля программ	157
Тестирование правил Контроля программ	157
Изменение шаблонов сообщений Контроля программ	158
О режимах работы Контроля программ.....	159
Выбор режима Контроля программ.....	159

Адаптивный контроль аномалий	162
Включение и выключение Адаптивного контроля аномалий	165
Включение и выключение правила Адаптивного контроля аномалий	165
Изменение действия при срабатывании правила Адаптивного контроля аномалий	166
Создание и изменение исключения для правила Адаптивного контроля аномалий	167
Удаление исключения для правила Адаптивного контроля аномалий	168
Импорт исключений для правил Адаптивного контроля аномалий	169
Экспорт исключений для правил Адаптивного контроля аномалий	169
Применение обновлений для правил Адаптивного контроля аномалий	170
Изменение шаблонов сообщений Адаптивного контроля аномалий	170
Просмотр отчетов Адаптивного контроля аномалий	171
Веб-Контроль	172
Включение и выключение Веб-Контроля	174
Правила формирования масок адресов веб-ресурсов	174
Действия с правилами доступа к веб-ресурсам	177
Добавление и изменение правила доступа к веб-ресурсам	178
Назначение приоритета правилам доступа к веб-ресурсам	180
Проверка работы правил доступа к веб-ресурсам	180
Включение и выключение правила доступа к веб-ресурсам	181
Экспорт и импорт списка адресов веб-ресурсов	181
Мониторинг активности пользователей в интернете	183
Изменение шаблонов сообщений Веб-Контроля	184
Контроль сетевого трафика	186
Контроль сетевых портов	187
Включение контроля всех сетевых портов	187
Включение контроля портов для программ из списка, сформированного специалистами "Лаборатории Касперского"	187
Формирование списка контролируемых сетевых портов	189
Формирование списка программ, для которых контролируются все сетевые порты	190
Проверка защищенных соединений	191
Включение и выключение проверки защищенных соединений	191
Настройка параметров проверки защищенных соединений	191
Создание исключения из проверки защищенных соединений	193
Просмотр глобальных исключений из проверки защищенного трафика	193
Проверка целостности модулей программы	195
Запуск и остановка задачи проверки целостности	195
Выбор режима запуска для задачи проверки целостности	196
Защита паролем	197
Включение Защиты паролем	200
Предоставление разрешений для отдельных пользователей или групп	201
Использование временного пароля для предоставления разрешений	202

Особенности разрешений Защиты паролем	203
Шифрование данных	205
Ограничения функциональности шифрования	208
Смена длины ключа шифрования (AES56 / AES256).....	209
Полнодисковое шифрование	210
Полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky	213
Полнодисковое шифрование с помощью технологии Шифрование диска BitLocker	214
Формирование списка жестких дисков для исключения из шифрования.....	216
Расшифровка жестких дисков	217
Восстановление доступа к диску, защищенному технологией Шифрование диска Kaspersky	218
Восстановление доступа к диску, зашифрованному BitLocker	221
Обновление операционной системы	223
Устранение ошибок при обновлении функциональности шифрования	224
Шифрование файлов на локальных дисках компьютера	225
Запуск шифрования файлов на локальных дисках компьютера.....	226
Формирование правил доступа программ к зашифрованным файлам	228
Шифрование файлов, создаваемых и изменяемых отдельными программами	229
Формирование правила расшифровки	230
Расшифровка файлов на локальных дисках компьютера	231
Создание зашифрованных архивов.....	232
Восстановление доступа к зашифрованным файлам.....	233
Восстановление доступа к зашифрованным данным в случае выхода из строя операционной системы	235
Изменение шаблонов сообщений для получения доступа к зашифрованным файлам.....	235
Шифрование съемных дисков	236
Запуск шифрования съемных дисков	238
Добавление правила шифрования для съемных дисков.....	240
Изменение правила шифрования для съемных дисков	241
Портативный режим для работы с зашифрованными файлами на съемных дисках	242
Расшифровка съемных дисков.....	246
Работа с Агентом аутентификации	247
Включение использования технологии единого входа (SSO)	247
Управление учетными записями Агента аутентификации.....	248
Использование токена и смарт-карты при работе с Агентом аутентификации	253
Выбор уровня трассировки Агента аутентификации.....	253
Изменение справочных текстов Агента аутентификации	254
Удаление объектов и данных, оставшихся после тестовой работы Агента аутентификации	256
Просмотр информации о шифровании данных	256
Просмотр статусов шифрования.....	257
Просмотр статистики шифрования на информационных панелях Kaspersky Security Center	258
Просмотр ошибок шифрования файлов на локальных дисках компьютера.....	259

Просмотр отчета о шифровании данных	259
Работа с зашифрованными устройствами при отсутствии доступа к ним	260
Восстановление данных с помощью утилиты восстановления FDERT	261
Создание диска аварийного восстановления операционной системы	265
Интеграция с другими решениями "Лаборатории Касперского"	266
Kaspersky Anti Targeted Attack Platform (KATA)	266
Kaspersky Sandbox	268
Служба уведомлений	269
Настройка параметров журналов событий	269
Настройка отображения и доставки уведомлений	270
Настройка отображения предупреждений о состоянии программы в области уведомлений	271
Работа с отчетами	272
Просмотр отчетов	273
Просмотр информации о событии в отчете	274
Настройка максимального срока хранения отчетов	274
Настройка максимального размера файла отчета	275
Сохранение отчета в файл	275
Удаление информации из отчетов	276
Работа с резервным хранилищем	278
Настройка максимального срока хранения файлов в резервном хранилище	278
Настройка максимального размера резервного хранилища	279
Восстановление и удаление файлов из резервного хранилища	279
Восстановление файлов из резервного хранилища	281
Удаление резервных копий файлов из резервного хранилища	281
Самозащита Kaspersky Endpoint Security	283
Включение и выключение механизма самозащиты	283
Включение и выключение поддержки AM-PPL	284
Включение и выключение механизма защиты от внешнего управления	285
Обеспечение работы программ удаленного администрирования	285
Производительность Kaspersky Endpoint Security и совместимость с другими программами	287
Выбор типов обнаруживаемых объектов	288
Включение и выключение технологии лечения активного заражения	289
Включение и выключение режима энергосбережения	290
Включение и выключение режима передачи ресурсов другим программам	291
Создание и использование конфигурационного файла	292
Работа с программой из командной строки	293
Команды	293
SCAN. Антивирусная проверка	294
UPDATE. Обновление баз и модулей программы	299
ROLLBACK. Откат последнего обновления	300
TRACES. Трассировка	300

START. Запуск профиля.....	302
STOP. Остановка профиля.....	303
STATUS. Статус профиля.....	303
STATISTICS. Статистика выполнения профиля.....	304
RESTORE. Восстановление файлов.....	304
EXPORT. Экспорт параметров программы.....	305
IMPORT. Импорт параметров программы.....	306
ADDKEY. Применение файла ключа.....	307
LICENSE. Лицензирование.....	307
RENEW. Покупка лицензии.....	309
PBATESTRESET. Сбросить результаты проверки перед шифрованием.....	309
EXIT. Завершение работы программы.....	309
EXITPOLICY. Выключение политики.....	309
STARTPOLICY. Включение политики.....	310
DISABLE. Выключение защиты.....	310
SPYWARE. Обнаружение шпионского ПО.....	310
Сообщения об ошибках.....	311
Коды возврата.....	314
Использование профилей задач.....	320
Профили программы.....	322
Действия после сбоя или неустранимой ошибки в работе программы.....	323
Способы получения технической поддержки.....	324
Техническая поддержка по телефону.....	324
Техническая поддержка через Kaspersky CompanyAccount.....	324
Получение информации для Службы технической поддержки.....	325
Трассировка работы программы.....	326
О составе и хранении файлов трассировки.....	327
О составе и хранении файлов дампов.....	330
Запись дампов.....	330
Защита файлов дампов и трассировок.....	331
Глоссарий.....	332
Информация о стороннем коде.....	338
Соответствие терминов.....	339
Приложение 1. Значения параметров программы в сертифицированной конфигурации.....	340
Приложение 2. Категории содержания веб-ресурсов.....	344

Об этом документе

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

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

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

В документе также содержатся разделы с дополнительной информацией о программе.

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

Источники информации о программе

Указанные источники информации о программе (в частности, электронная справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Endpoint Security:

- страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Endpoint Security в Базе знаний;
- электронная справка.

Страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security (<http://www.kaspersky.ru/business-security/endpoint-windows>) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.


Страница Kaspersky Endpoint Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Endpoint Security в Базе знаний (<https://support.kaspersky.ru/kes11.1>) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

Электронная справка входит в состав программы Kaspersky Endpoint Security. Вы можете открыть справку по кнопке  или по клавише **F1**. В электронной справке вы можете найти описание параметров Kaspersky Endpoint Security.

О программе

Программное изделие "Kaspersky Endpoint Security для Windows" представляет собой САВЗ типов "Б", "В", "Г" второго класса защиты, с функциями аутентификации администратора безопасности и ограничения программной среды.

Объект оценки представляет собой программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации, предназначенное для применения на серверах или АРМ информационных систем, а также на автономных АРМ.

Основными угрозами, для противостояния которым используется Kaspersky Endpoint Security, являются:

- угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и / или съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ);
- угрозы, связанные с установкой на узлы информационной системы внутренними и внешними нарушителями незарегистрированного (неучтенного) потенциально вредоносного программного обеспечения.

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению ОО;
- управление работой ОО;
- управление параметрами ОО;
- управление установкой обновлений (актуализации) БД ПКВ ОО;
- аудит безопасности ОО;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация ОО;
- идентификация и аутентификация администратора безопасности;
- ограничение программной среды (управление запуском компонентов ПО, контроль доступа к веб-ресурсам).

Требования

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

В этом разделе

Аппаратные и программные требования.....	14
Указания по эксплуатации и требования к среде	15

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Минимальные общие требования:

- 2 ГБ свободного места на жестком диске;
- Процессор 1 ГГц (с поддержкой инструкций SSE2);
- Оперативная память:
 - для 32-разрядной операционной системы – 1 ГБ;
 - для 64-разрядной операционной системы – 2 ГБ.

Поддерживаемые операционные системы для рабочих станций (32- и 64-разрядные версии):

- Microsoft Windows 7 SP1 Home / Professional / Enterprise;
- Microsoft Windows 8 Pro / Enterprise;
- Microsoft Windows 8.1 Pro / Enterprise;
- Microsoft Windows 10 Home / Pro / Education / Enterprise (TH1, TH2, RS1, RS2, RS3, RS4, RS5, RS6, 19H1, 20H1).

Поддерживаемые операционные системы для серверов (64-разрядные версии):

- Microsoft Windows Small Business Server 2011 Essentials / Standard;
- Microsoft Windows MultiPoint Server 2011;
- Microsoft Windows Server 2008 R2 SP1 Standard / Foundation / Enterprise;
- Microsoft Windows Server 2012 Standard / Foundation / Essentials;
- Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials;
- Microsoft Windows Server 2016 Essentials / Standard;
- Microsoft Windows Server 2019 Essentials / Standard.

Особенности поддержки операционных систем Microsoft Windows 10, Microsoft Windows Server 2016 и Microsoft Windows Server 2019 вы можете узнать в базе знаний Службы технической поддержки: <https://support.kaspersky.ru/kes11/13036>.

Поддерживаемые виртуальные платформы:

- VMware Workstation 15;
- VMware ESXi 6.7 U2;

- Microsoft Hyper-V Server 2019;
- Citrix XenDesktop 7.18;
- Citrix XenApp 7.18;
- Citrix Provisioning Services 7.18;
- Citrix Hypervisor 8.

Указания по эксплуатации и требования к среде

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

Установка программы с помощью мастера

Интерфейс мастера установки программы состоит из последовательности окон, соответствующих шагам установки программы.

- ▶ *Чтобы установить программу или обновить предыдущую версию программы с помощью мастера установки программы,*

скопируйте файл `setup_ks.exe`, входящий в комплект поставки, на компьютер пользователя и запустите его.

Запустится мастер установки программы.

Подготовка к установке

Перед установкой Kaspersky Endpoint Security на компьютер или обновлением предыдущей версии программы проверяются следующие условия:

- наличие несовместимого программного обеспечения (список несовместимого ПО приведен в файле `incompatible.txt` в комплекте поставки);
- выполнение аппаратных и программных требований;
- наличие прав на установку программного обеспечения.

Если какое-либо из перечисленных условий не выполнено, на экран выводится соответствующее уведомление.

Если компьютер соответствует предъявляемым требованиям, мастер установки программы выполняет поиск программ "Лаборатории Касперского", одновременная работа которых может привести к возникновению конфликтов. Если такие программы найдены, вам предлагается удалить их вручную.

Если в числе обнаруженных программ есть предыдущие версии Kaspersky Endpoint Security, то все данные, которые могут быть мигрированы (например, информация об активации, параметры программы), сохраняются и используются при установке Kaspersky Endpoint Security 11.3.0 для Windows, а предыдущая версия программы автоматически удаляется. Это относится к следующим версиям программы:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 для Windows (сборка 10.2.5.3201).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 для Windows (сборка 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 для Windows (сборка 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 для Windows (сборка 10.3.3.275).
- Kaspersky Endpoint Security для Windows 11.0.0 (сборка 11.0.0.6499).

- Kaspersky Endpoint Security для Windows 11.0.1 (сборка 11.0.1.90).
- Kaspersky Endpoint Security для Windows 11.1.0 (сборка 11.1.0.15919).
- Kaspersky Endpoint Security для Windows 11.1.1 (сборка 11.1.1.126).
- Kaspersky Endpoint Security для Windows 11.2.0 (сборка 11.2.0.2254).

Компоненты Kaspersky Endpoint Security

В процессе установки вы можете выбрать компоненты Kaspersky Endpoint Security, которые вы хотите установить.

Для установки сертифицированной конфигурации программы Kaspersky Endpoint Security необходимо исключить установку компонентов Сетевой экран и Контроль устройств (см. рис. ниже).

Выберите следующие компоненты для установки:

- Ядро программы, включая задачи проверки;
- Продвинутая защита:
 - Анализ поведения;
 - Защита от эксплойтов;
 - Отказ вредоносных действий;
 - Предотвращение вторжений.
- Базовая защита:
 - Защита от файловых угроз;
 - Защита от почтовых угроз;
 - Защита от веб-угроз;
 - Защита от сетевых угроз;
 - Защита от атак BadUSB;
 - Поставщик AMSI-защиты.
- Контроль безопасности:
 - Веб-Контроль;
 - Контроль программ;
 - Адаптивный контроль аномалий.
- Шифрование данных:
 - Шифрование файлов;
 - Полнодисковое шифрование;
 - Управление BitLocker.
- Коннектор к Агенту администрирования.

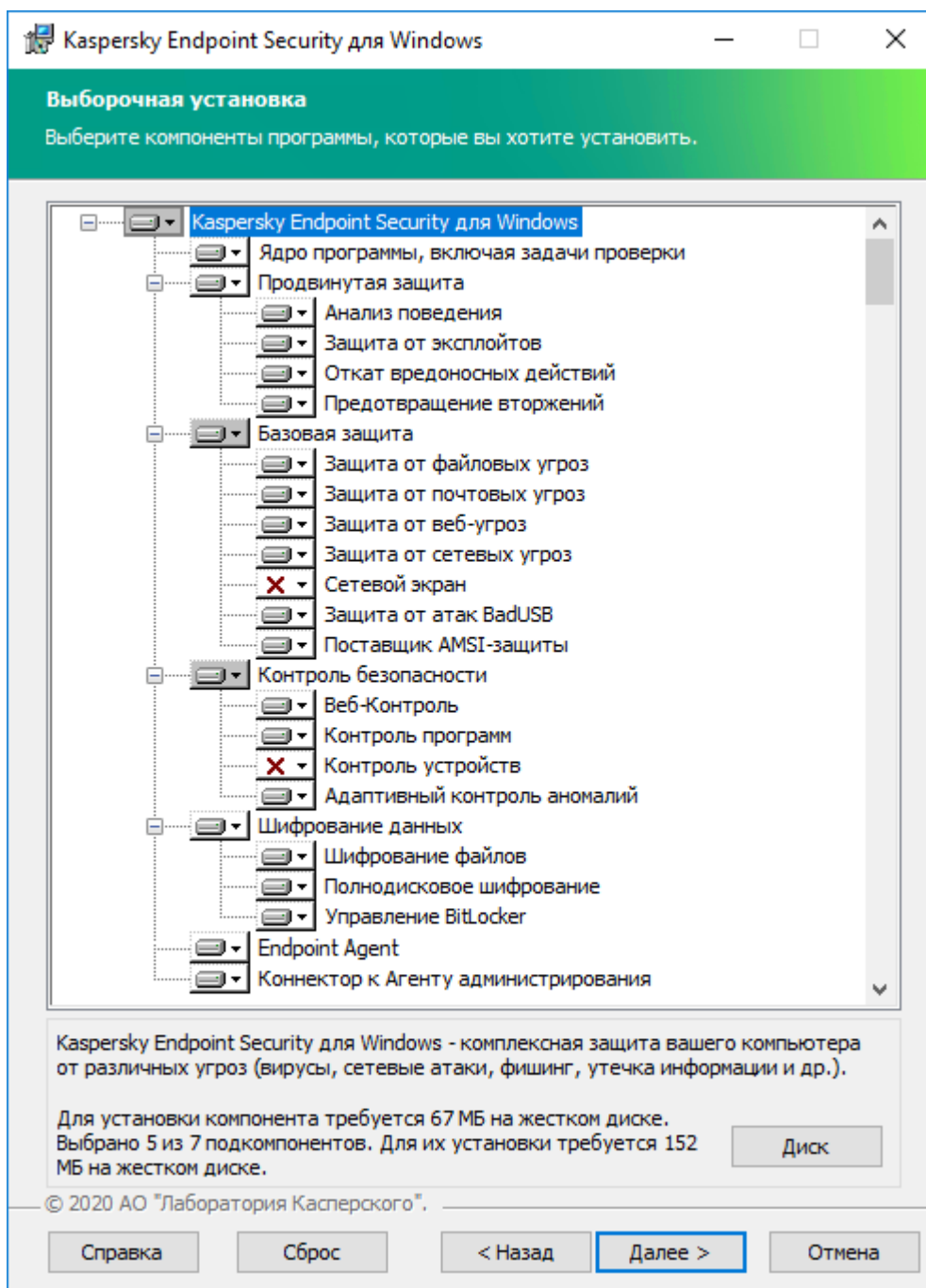


Рисунок 1. Сертификационная конфигурация программы

Чтобы выбрать компонент для последующей установки, по левой клавише мыши откройте контекстное меню значка рядом с названием компонента и выберите пункт **Компонент будет установлен на локальный жесткий диск**. Подробную информацию о том, какие задачи выполняет выбранный компонент и сколько места на жестком диске требуется для установки компонента, вы можете посмотреть в нижней части текущего окна мастера установки программы.

Чтобы узнать подробную информацию о свободном месте на жестких дисках компьютера, нажмите на кнопку **Диск**. Информация будет отображена в открывшемся окне **Доступное дисковое пространство**.

Для отказа от установки компонента в контекстном меню выберите пункт **Компонент будет недоступен**. Чтобы вернуться к списку компонентов, устанавливаемых по умолчанию, нажмите на кнопку **Сброс**.

Вы можете изменить состав компонентов после установки программы. Для этого вам нужно запустить мастер установки повторно и выбрать операцию изменения состава компонентов.

Дополнительные параметры

Защитить процесс установки программы. Защита установки включает в себя защиту от подмены дистрибутива вредоносными программами, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами программы. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку программы (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).



Обеспечить совместимость с Citrix PVS. Вы можете включить поддержку Citrix Provisioning Services для установки Kaspersky Endpoint Security на виртуальную машину.

Добавить путь к программе в переменную окружения %PATH%. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки.

Активация программы с помощью мастера активации программы

Активация программы должна быть выполнена на компьютере с актуальными системными датой и временем. При изменении системных даты и времени после активации программы ключ становится неработоспособным. Программа переходит к режиму работы без обновлений, и Kaspersky Security Network недоступен. Восстановить работоспособность ключа можно только переустановкой операционной системы.

► Чтобы активировать Kaspersky Endpoint Security с помощью мастера активации программы, выполните следующие действия:

1. Нажмите на кнопку  / , расположенную в нижней части главного окна программы.
2. В открывшемся окне нажмите на кнопку **Активировать программу по коммерческой лицензии**.
Запустится мастер активации программы. Следуйте указаниям мастера активации программы.

В сертифицированной версии программы Kaspersky Endpoint Security допускается только активация файлом ключа. Другие способы активации ведут к выходу из безопасного состояния программы.

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу. Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Удаление программы

► Чтобы удалить *Kaspersky Endpoint Security* с помощью мастера установки программы, выполните следующие действия:

1. Откройте окно **Панель управления** одним из следующих способов:
 - Если вы используете Windows 7, то в меню **Пуск** выберите пункт **Панель управления**.
 - Если вы используете Windows 8 или Windows 8.1, то нажмите сочетание клавиш **WIN+I** и выберите пункт **Панель управления**.
 - Если вы используете Windows 10, то нажмите сочетание клавиш **WIN+X** и выберите пункт **Панель управления**.
2. В окне **Панель управления** выберите пункт **Программы и компоненты**.
3. В списке установленных программ выберите элемент **Kaspersky Endpoint Security для Windows**.
4. Нажмите на кнопку **Удалить/Изменить**.
Запустится мастер установки программы.
5. В окне мастера установки программы **Изменение, восстановление или удаление программы** нажмите на кнопку **Удаление**.
6. Следуйте указаниям мастера установки программы.

Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

Безопасное состояние	22
Проверка работоспособности. Тестовый файл EICAR	22

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если параметры программы находятся в рамках допустимых значений, приведенных в приложении 1 к этому документу.

Проверка работоспособности. Тестовый файл EICAR

Чтобы проверить работоспособность программы, вы можете использовать тестовый файл EICAR.

Тестовый файл EICAR предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый файл EICAR не является вирусом и не содержит программного кода, который может нанести вред вашему компьютеру, но антивирусные программы большинства производителей идентифицируют в нем угрозу.

Вы можете загрузить тестовый файл EICAR со страницы веб-сайта организации EICAR.

Проверка работоспособности Защиты от веб-угроз

Проверку работоспособности Защиты от веб-угроз не рекомендуется выполнять в браузере Edge. У браузера Edge есть встроенная система безопасности. Браузер Edge блокирует тестовый вредоносный веб-сайт раньше Kaspersky Endpoint Security. Для проверки работоспособности Защиты от веб-угроз используйте браузер Explorer.

► Чтобы проверить работоспособность Защиты от веб-угроз, выполните следующие действия:

1. Включите защиту виртуальной машины от веб-угроз.
 - a. В главном окне программы нажмите на кнопку **Настройка**.
 - b. В левой части окна выберите **Базовая защита** → **Защита от веб-угроз**.

- c. В правой части окна настройки программы убедитесь, что флажок **Включить Защиту от веб-угроз** установлен.
 - d. Нажмите на кнопку **Сохранить**.
2. В окне браузера перейдите по ссылке на тестовый вредоносный веб-сайт.
Kaspersky Endpoint Security сообщает о запрете доступа, отобразив уведомление в окне браузера (см. рис. ниже).



Рисунок 2. Сообщение о запрете доступа к веб-сайту

3. Проверьте информацию в отчете об обнаруженных вирусах:
 - a. В главном окне программы нажмите на кнопку **Отчеты** и перейдите в раздел **Защита от веб-угроз**.
 - b. Убедитесь, что в отчете присутствует сообщение об обнаружении вируса и информация об этом событии верна.

Проверка работоспособности Защиты от файловых угроз

► Чтобы проверить работоспособность Защиты от файловых угроз, выполните следующие действия:

1. Отключите защиту виртуальной машины от веб-угроз:

Этот шаг необходим для успешного размещения на виртуальной машине тестового файла, иначе он будет мгновенно удален программой.

- a. В главном окне программы нажмите на кнопку **Настройка**.

- b. В левой части окна выберите **Базовая защита** → **Защита от веб-угроз**.
 - c. В правой части окна настройки программы снимите флажок **Включить Защиту от веб-угроз**.
 - d. Нажмите на кнопку **Сохранить**.
2. Загрузите тестовый файл EICAR и разместите его в новую папку на системном диске виртуальной машины.
3. Перейдите в папку с тестовым файлом, загруженным на шаге, и запустите его.
Kaspersky Endpoint Security удаляет тестовый файл с виртуальной машины.
4. Проверьте информацию в отчете об обнаруженных вирусах:
 - a. В главном окне программы нажмите на кнопку **Отчеты** и перейдите в раздел **Защита от файловых угроз**.
 - b. Убедитесь, что в отчете отображается верная информация об обнаружении зараженного файла (время события, путь к файлу).

Проверка работоспособности антивирусной проверки

► *Что проверить работоспособность функции антивирусной проверки, выполните следующие действия:*

1. Отключите защиту виртуальной машины:

Этот шаг необходим для успешного размещения на виртуальной машине тестового файла, иначе он будет мгновенно удален программой.

- a. В главном окне программы нажмите на кнопку **Настройка**.
 - b. В левой части окна выберите **Базовая защита** → **Защита от веб-угроз**.
 - c. В правой части окна настройки программы снимите флажок **Включить Защиту от веб-угроз**.
 - d. Нажмите на кнопку **Сохранить**.
2. Загрузите тестовый файл EICAR и разместите его в новую папку на системном диске виртуальной машины.
3. Добавьте в область проверки папку с тестовым файлом EICAR:
 - a. В главном окне программы нажмите на кнопку **Настройка**.
 - b. В левой части окна выберите **Задачи** → **Выборочная проверка**.
 - c. В правой части окна настройки программы нажмите на кнопку **Область проверки**.
 - d. Добавьте в область проверки папку с тестовым файлом EICAR.
 - e. Сохраните изменения.
4. В главном окне программы перейдите в раздел **Задачи**.
5. Выберите задачу **Выборочная проверка** и нажмите на кнопку **Запустить**.
6. По окончании выполнения задачи проверки проверьте информацию в отчете об обнаруженных вирусах:
 - a. В главном окне программы нажмите на кнопку **Отчеты** и перейдите в раздел **Задачи проверки**.
 - b. Убедитесь, что в отчете отображается верная информация об обнаружении зараженного файла (время события, путь к файлу).

Проверка работоспособности функции контроля программ

Перед проверкой работоспособности функции контроля запуска программ установите программу для тестирования, например, Notepad++. Контроль программ по умолчанию разрешает запуск программ для правила *Операционная система и ее компоненты*. Это правило включает в себя программы, такие как Блокнот, Explorer, WordPad и другие. Специалисты "Лаборатории Касперского" не рекомендует выключать правило *Операционная система и ее компоненты*, так как возможна некорректная работа операционной системы и пользовательских программ.

- ▶ *Чтобы проверить работоспособность функции контроля запуска программ, выполните следующие действия:*
 1. В главном окне программы нажмите на кнопку **Настройка**.
 2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Контроль программ**.
 3. В правой части окна настройки программы установите флажок **Включить Контроль программ**.
 4. Для параметра **Режим контроля программ** выберите значение **Черный список**.
 5. Для параметра **Действие** выберите значение **Блокировать**.
 6. Нажмите на кнопку **Добавить**.
Откроется окно для добавления условий контроля программы.
 7. В открывшемся окне выполните следующие действия:
 - a. В поле **Название правила** укажите произвольное имя.
 - b. В блоке **Включающие условия** нажмите на кнопку **Добавить** → **Условие вручную**.
Откроется окно **Пользовательское условие**.
 - c. В открывшемся окне выберите вариант **Метаданные**, установите флажок **Название файла**, в поле ввода введите `Notepad++.exe` и нажмите на кнопку **ОК**.
 - d. Установите флажок **Запретить остальным пользователям**.
 - e. Сохраните изменения.
 8. Запустите программу Notepad++.
 9. Убедитесь, что запуск программы запрещен (см. рис. ниже).

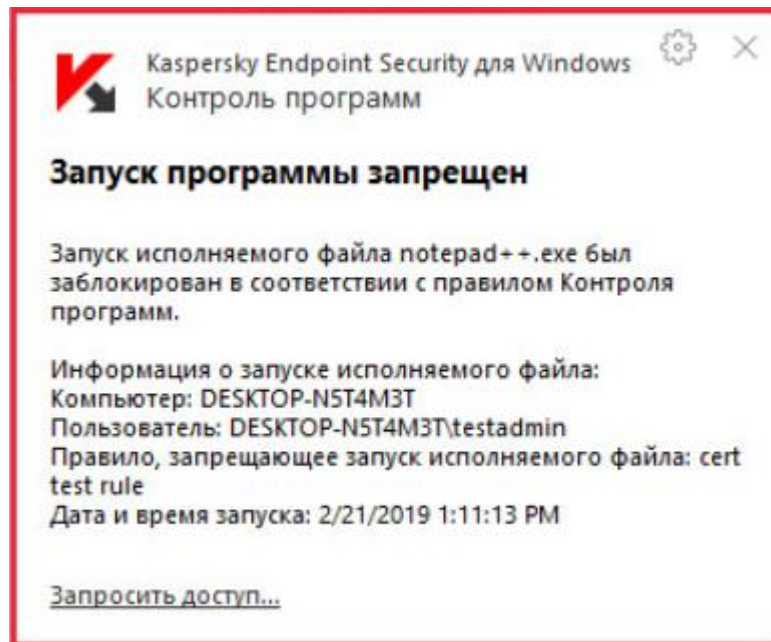


Рисунок 3. Сообщение о запрете запуска программы

10. Проверьте информацию в отчете:

- a. В главном окне программы нажмите на кнопку **Отчеты** и перейдите в раздел **Контроль программ**.
- b. Убедитесь, что в отчете присутствует сообщение о запрете запуска программы Notepad++ и информация об этом событии верна.

Разделение доступа к функциям программы по пользовательским ролям

По умолчанию пользователи, входящие в группу "Администраторы" на защищаемом сервере, имеют доступ ко всем функциям Kaspersky Endpoint Security.

Пользователи, которые имеют доступ к функции **Изменение прав** Kaspersky Endpoint Security, могут предоставлять доступ к функциям Kaspersky Endpoint Security другим пользователям, зарегистрированным на защищаемом сервере или входящим в домен.

Если пользователь не зарегистрирован в списке пользователей Kaspersky Endpoint Security, он не может открыть Консоль Kaspersky Endpoint Security.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Endpoint Security один из следующих предустановленных уровней доступа к функциям Kaspersky Endpoint Security:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры работы Kaspersky Endpoint Security, параметры работы компонентов Kaspersky Endpoint Security, права пользователей Kaspersky Endpoint Security, а также просматривать статистику работы Kaspersky Endpoint Security.
- **Изменение** – доступ ко всем функциям программы, кроме изменения прав пользователей: возможность просматривать и изменять общие параметры работы Kaspersky Endpoint Security, параметры работы компонентов Kaspersky Endpoint Security, а также просматривать статистику работы Kaspersky Endpoint Security и права пользователей Kaspersky Endpoint Security.
- **Чтение** – возможность просматривать общие параметры работы Kaspersky Endpoint Security, параметры работы компонентов Kaspersky Endpoint Security, статистику работы Kaspersky Endpoint Security и права пользователей Kaspersky Endpoint Security.

Также вы можете выполнять расширенную настройку прав доступа: разрешать или запрещать доступ к отдельным функциям Kaspersky Endpoint Security.

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы установлен уровень доступа **Особые разрешения**.

Таблица 1. Права доступа к функциям Kaspersky Endpoint Security

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Endpoint Security.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможности: <ul style="list-style-type: none"> • просматривать и изменять общие параметры работы Kaspersky Endpoint Security; • импортировать из конфигурационного файла и экспортировать в конфигурационный файл параметры работы Kaspersky Endpoint Security; • просматривать и изменять параметры задач; • просматривать и изменять параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Чтение параметров	Возможности: <ul style="list-style-type: none"> • просматривать общие параметры работы Kaspersky Endpoint Security и параметры задач; • экспортировать в конфигурационный файл параметры работы Kaspersky Endpoint Security; • просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: <ul style="list-style-type: none"> • помещать объекты на карантин; • удалять объекты из карантина и резервного хранилища; • восстанавливать объекты из карантина и резервного хранилища.
Управление журналами	Возможность удалять журналы выполнения задач и очищать журнал системного аудита.
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Endpoint Security.
Лицензирование программы	Возможность активировать и деактивировать Kaspersky Endpoint Security.
Чтение прав	Возможность просматривать список пользователей Kaspersky Endpoint Security и права доступа каждого пользователя.
Изменение прав	Возможности: <ul style="list-style-type: none"> • изменять список пользователей, имеющих доступ к управлению программой; • изменять права доступа пользователей к функциям Kaspersky Endpoint Security.

Управление программой через Консоль администрирования Kaspersky Security Center

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Security, настраивать параметры работы программы, изменять состав компонентов программы, добавлять ключи, запускать и останавливать задачи обновления и проверки.

В разделе о Контроле программ вы можете найти информацию об управлении правилами Контроля программ с помощью Kaspersky Security Center.

Подробнее об управлении программой через Kaspersky Security Center см. в справке Kaspersky Security Center <https://help.kaspersky.com/KSC/11/ru-RU/>.

Управление программой через Kaspersky Security Center осуществляется с помощью плагина управления Kaspersky Endpoint Security.

Версия плагина управления может отличаться от версии Kaspersky Endpoint Security, установленной на клиентском компьютере. Если в установленной версии плагина управления предусмотрено меньше функций, чем в установленной версии Kaspersky Endpoint Security, то параметры недостающих функций не регулируются плагином управления. Такие параметры могут быть изменены пользователем в локальном интерфейсе Kaspersky Endpoint Security.

В этом разделе



Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере.....	29
Настройка параметров Kaspersky Endpoint Security	30
Управление задачами	31
Управление политиками	39

Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере

► *Чтобы запустить или остановить программу на клиентском компьютере, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, на котором вы хотите запустить или остановить программу.
5. По правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.

Откроется окно свойств клиентского компьютера.

6. В окне свойств клиентского компьютера выберите раздел **Программы**.
Справа в окне свойств клиентского компьютера отобразится список программ "Лаборатории Касперского", установленных на клиентском компьютере.
7. Выберите программу Kaspersky Endpoint Security.
8. Выполните следующие действия:
 - Если вы хотите запустить программу, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  или выполните следующие действия:
 - a. Выберите пункт **Свойства** в контекстном меню программы Kaspersky Endpoint Security или нажмите на кнопку **Свойства**, расположенную под списком программ «Лаборатории Касперского».
Откроется окно **Параметры Kaspersky Endpoint Security для Windows**.
 - b. В разделе **Общие** нажмите на кнопку **Запустить** в правой части окна.
 - Если вы хотите остановить работу программы, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  или выполните следующие действия:
 - a. Выберите пункт **Свойства** в контекстном меню программы Kaspersky Endpoint Security или нажмите на кнопку **Свойства**, расположенную под списком программ «Лаборатории Касперского».
Откроется окно **Параметры Kaspersky Endpoint Security для Windows**.
 - b. В разделе **Общие** нажмите на кнопку **Остановить** в правой части окна.

Настройка параметров Kaspersky Endpoint Security

- *Чтобы настроить параметры Kaspersky Endpoint Security, выполните следующие действия:*
1. Откройте Консоль администрирования Kaspersky Security Center.
 2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
 3. В рабочей области выберите закладку **Устройства**.
 4. Выберите компьютер, для которого вы хотите настроить параметры Kaspersky Endpoint Security.
 5. В контекстном меню клиентского компьютера выберите пункт **Свойства**.
Откроется окно свойств клиентского компьютера.
 6. В окне свойств клиентского компьютера выберите раздел **Программы**.
Справа в окне свойств клиентского компьютера отобразится список программ "Лаборатории Касперского", установленных на клиентском компьютере.
 7. Выберите программу Kaspersky Endpoint Security.
 8. Выполните одно из следующих действий:
 - В контекстном меню программы Kaspersky Endpoint Security выберите пункт **Свойства**.
 - Нажмите на кнопку **Свойства** под списком программ "Лаборатории Касперского".Откроется окно **Параметры программы "Kaspersky Endpoint Security для Windows"**.

9. В разделе **Общие параметры** настройте параметры работы Kaspersky Endpoint Security, а также параметры отчетов и хранилищ.

Остальные разделы окна **Параметры программы "Kaspersky Endpoint Security для Windows"** стандартны для программы Kaspersky Security Center. Описание этих разделов вы можете прочитать в справке для Kaspersky Security Center.

Если для программы создана политика, в которой запрещено изменение некоторых параметров, то во время настройки параметров программы в разделе **Общие параметры** их изменение недоступно.

10. В окне **Параметры программы "Kaspersky Endpoint Security для Windows"** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Управление задачами

Kaspersky Security Center управляет работой программ "Лаборатории Касперского", установленных на клиентских компьютерах, с помощью задач. Задачи реализуют основные функции управления, например, добавление ключа, проверку компьютера, обновление баз и модулей программы.

Для работы с Kaspersky Endpoint Security через Kaspersky Security Center вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного клиентского компьютера;
- групповые задачи, определенные для клиентских компьютеров, входящих в группы администрирования;
- задачи для выборки компьютеров, не входящих в группы администрирования.

Задачи для выборки компьютеров, не входящих в группы администрирования, выполняются только для клиентских компьютеров, указанных в параметрах задачи. Если в выборку компьютеров, для которой сформирована задача, добавлены новые клиентские компьютеры, то для них эта задача не выполняется. В этом случае требуется создать новую задачу или изменить параметры уже существующей задачи.

Для удаленного управления программой Kaspersky Endpoint Security вы можете работать со следующими задачами любого из перечисленных типов:

- **Добавление ключа.** Kaspersky Endpoint Security добавляет ключ, в том числе дополнительный, для активации программы.
- **Изменение состава компонентов программы.** Kaspersky Endpoint Security устанавливает или удаляет на клиентских компьютерах компоненты согласно списку компонентов, указанному в параметрах задачи.
- **Инвентаризация.** Kaspersky Endpoint Security получает информацию обо всех исполняемых файлах программ, хранящихся на компьютерах.

Вы можете включить инвентаризацию DLL-модулей и файлов скриптов. В этом случае Kaspersky Security Center будет получать информацию о DLL-модулях, загружаемых на компьютере с установленной программой Kaspersky Endpoint Security, и о файлах, содержащих скрипты.

Включение инвентаризации DLL-модулей и файлов скриптов значительно увеличивает время выполнения задачи инвентаризации и размер базы данных.

Если на компьютере с установленной программой Kaspersky Endpoint Security не установлен компонент Контроль программ, то задача инвентаризации на этом компьютере завершится с ошибкой.

- **Обновление.** Kaspersky Endpoint Security обновляет базы и модули программы в соответствии с установленными параметрами обновления.
- **Удаление данных.** Kaspersky Endpoint Security удаляет файлы и папки с компьютеров пользователей немедленно или при длительном отсутствии связи с Kaspersky Security Center.
- **Откат последнего обновления.** Kaspersky Endpoint Security откатывает последнее обновление баз и модулей.
- **Поиск вирусов.** Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи.
- **Проверка целостности.** Kaspersky Endpoint Security получает данные о составе модулей программы, установленных на клиентском компьютере, и проверяет цифровую подпись каждого из модулей.
- **Управление учетными записями Агента аутентификации.** В процессе выполнения задачи Kaspersky Endpoint Security создает команды для удаления, добавления или изменения учетных записей Агента аутентификации.

Вы можете выполнять следующие действия над задачами:

- запускать, останавливать, приостанавливать и возобновлять выполнение задач;
- создавать новые задачи;
- изменять параметры задач.

Права на доступ к задачам Kaspersky Endpoint Security (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через параметры доступа к функциональным областям Kaspersky Endpoint Security. Для настройки доступа к функциональным областям Kaspersky Endpoint Security перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center.

Подробнее о концепции управления задачами через Kaspersky Security Center см. в справке Kaspersky Security Center <https://help.kaspersky.com/KSC/11/ru-RU/>.

В этом разделе

Настройка режима работы с задачами	33
Создание локальной задачи	34
Создание групповой задачи	34
Создание задачи для выборки устройств	34
Запуск, остановка, приостановка и возобновление выполнения задачи	35
Изменение параметров задачи	37
Параметры задачи инвентаризации	38

Настройка режима работы с задачами

► Чтобы настроить режим работы с задачами в локальном интерфейсе Kaspersky Endpoint Security, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, для которой вы хотите настроить режим работы с задачами в локальном интерфейсе Kaspersky Endpoint Security.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную вам политику.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
 - В контекстном меню политики выберите пункт **Свойства**.
 - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.
6. В разделе **Локальные задачи** выберите подраздел **Управление задачами**.
7. В блоке **Управление задачами** выполните следующие действия:
 - Если вы хотите разрешить пользователям работу с локальными задачами в интерфейсе и командной строке Kaspersky Endpoint Security, установите флажок **Разрешить использование локальных задач**.

Если флажок снят, функционирование локальных задач прекращается. В этом режиме локальные задачи не запускаются по расписанию. Также локальные задачи недоступны для запуска и редактирования в локальном интерфейсе Kaspersky Endpoint Security и при работе с командной строкой.

- Если вы хотите разрешить пользователям просматривать список групповых задач, установите флажок **Разрешить отображение групповых задач**.
 - Если вы хотите разрешить пользователям изменять параметры групповых задач, установите флажок **Разрешить управление групповыми задачами**.
8. Сохраните внесенные изменения.

Создание локальной задачи

► Чтобы создать локальную задачу, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, для которого вы хотите создать локальную задачу.
5. Выполните одно из следующих действий:
 - В контекстном меню клиентского компьютера выберите пункт **Все задачи** → **Создать задачу**.
 - В контекстном меню клиентского компьютера выберите пункт **Свойства** и в открывшемся окне **Свойства: <Название компьютера>** на закладке **Задачи** нажмите на кнопку **Добавить**.
 - В раскрывающемся списке **Выполнить действие** выберите элемент **Создать задачу**.Запустится мастер создания задачи.
6. Следуйте указаниям мастера создания задачи.

Создание групповой задачи

► Чтобы создать групповую задачу, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
 - Выберите папку **Управляемые устройства** дерева Консоли администрирования, если вы хотите создать групповую задачу для всех компьютеров, управляемых через программу Kaspersky Security Center.
 - В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.
Запустится мастер создания задачи.
5. Следуйте указаниям мастера создания задачи.

Создание задачи для выборки устройств



► Чтобы создать задачу для выборки устройств, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** дерева Консоли администрирования.
3. Нажмите на кнопку **Создать задачу**.
Запустится мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.



Запуск, остановка, приостановка и возобновление выполнения задачи

Если на клиентском компьютере запущена программа (см. раздел "Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере" на стр. 29) Kaspersky Endpoint Security, вы можете запустить / остановить / приостановить / возобновить выполнение задачи на этом клиентском компьютере через Kaspersky Security Center. Если программа Kaspersky Endpoint Security остановлена, выполнение запущенных задач прекращается, а управлять запуском, остановкой, приостановкой и возобновлением задач через Kaspersky Security Center становится невозможным.


► Чтобы запустить / остановить / приостановить / возобновить выполнение локальной задачи, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, на котором вы хотите запустить / остановить / приостановить / возобновить выполнение локальной задачи.
5. По правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.
Откроется окно свойств клиентского компьютера.
6. Выберите раздел **Задачи**.
В правой части окна отобразится список локальных задач.
7. Выберите локальную задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
8. Выполните необходимое действие с задачей одним из следующих способов:
 - По правой клавише мыши откройте контекстное меню локальной задачи и выберите пункт **Запустить / Остановить / Приостановить / Возобновить**.
 - Нажмите на кнопку  /  справа от списка локальных задач, чтобы запустить или остановить локальную задачу.
 - Выполните следующие действия:
 - a. Нажмите на кнопку **Свойства** под списком локальных задач или выберите пункт **Свойства** в контекстном меню задачи.
Откроется окно **Свойства <Название задачи>**.
 - b. На закладке **Общие** нажмите на кнопку **Запустить / Остановить / Приостановить / Возобновить**.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение групповой задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, для которой вы хотите запустить / остановить / приостановить / возобновить выполнение групповой задачи.
3. В рабочей области выберите закладку **Задачи**.
В правой части окна отобразятся групповые задачи.
4. Выберите групповую задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
5. Выполните необходимое действие с задачей одним из следующих способов:
 - В контекстном меню групповой задачи выберите пункт **Запустить / Остановить / Приостановить / Возобновить**.
 - Нажмите на кнопку  /  в правой части окна, чтобы запустить или остановить групповую задачу.
 - Выполните следующие действия:
 - a. Перейдите по ссылке **Настроить параметры задачи** в правой части рабочей области Консоли администрирования или выберите пункт **Свойства** в контекстном меню задачи.
Откроется окно **Свойства <Название задачи>**.
 - b. На закладке **Общие** нажмите на кнопку **Запустить / Остановить / Приостановить / Возобновить**.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение задачи для выборки компьютеров, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Задачи** дерева Консоли администрирования выберите задачу для выборки компьютеров, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
3. Выполните одно из следующих действий:
 - В контекстном меню задачи выберите пункт **Запустить / Остановить / Приостановить / Возобновить**.
 - Нажмите на кнопку  /  в правой части окна, чтобы запустить или остановить задачу для набора компьютеров.
 - Выполните следующие действия:
 - a. Перейдите по ссылке **Настроить параметры задачи** в правой части рабочей области Консоли администрирования или выберите пункт **Свойства** в контекстном меню задачи.
Откроется окно **Свойства <Название задачи>**.
 - b. На закладке **Общие** нажмите на кнопку **Запустить / Остановить / Приостановить / Возобновить**.

Изменение параметров задачи

► *Чтобы изменить параметры локальной задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, для которого вы хотите настроить параметры программы.
5. По правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.
Откроется окно свойств клиентского компьютера.
6. Выберите раздел **Задачи**.
В правой части окна отобразится список локальных задач.
7. Выберите в списке локальных задач нужную локальную задачу.
8. Нажмите на кнопку **Свойства**.
Откроется окно **Свойства: <Название локальной задачи>**.
9. В окне **Свойства: <Название локальной задачи>** выберите раздел **Параметры**.
10. Измените параметры локальной задачи.
11. Сохраните внесенные изменения.

► *Чтобы изменить параметры групповой задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием нужной группы администрирования.
3. В рабочей области выберите закладку **Задачи**.
В рабочей области Консоли администрирования отобразятся групповые задачи.
4. Выберите нужную групповую задачу.
5. По правой клавише мыши откройте контекстное меню групповой задачи и выберите пункт **Свойства**.
Откроется окно **Свойства: <Название групповой задачи>**.
6. В окне **Свойства: <Название групповой задачи>** выберите раздел **Параметры**.
7. Измените параметры групповой задачи.
8. Сохраните внесенные изменения.

► *Чтобы изменить параметры задачи для выборки компьютеров, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Задачи** дерева Консоли администрирования выберите задачу для выборки компьютеров, параметры которой вы хотите изменить.

3. По правой клавише мыши откройте контекстное меню задачи для выборки компьютеров и выберите пункт **Свойства**.

Откроется окно **Свойства: <Название задачи для выборки компьютеров>**.

4. В окне **Свойства: <Название задачи для выборки компьютеров>** выберите раздел **Параметры**.
5. Измените параметры задачи для выборки компьютеров.
6. Сохраните внесенные изменения.

Все разделы окна свойств задач, кроме раздела **Параметры**, стандартны для программы Kaspersky Security Center. Их подробное описание вы можете прочитать в справке для Kaspersky Security Center. Раздел **Параметры** содержит специфические параметры Kaspersky Endpoint Security для Windows. Его содержимое зависит от выбранной задачи и от ее типа.

Параметры задачи инвентаризации

Kaspersky Endpoint Security не осуществляет инвентаризацию файлов, содержимое которых расположено в облачном хранилище OneDrive.

Вы можете настроить следующие параметры для задачи инвентаризации:

- **Область инвентаризации.** В этом блоке вы можете указать объекты файловой системы, которые будут проверены в ходе инвентаризации. В качестве объектов могут выступать локальные и сетевые папки, съемные и жесткие диски или весь компьютер целиком.
- **Параметры задачи инвентаризации.** В этом блоке вы можете настроить следующие параметры:
 - **Выполнять проверку во время простоя компьютера.** Флажок включает / выключает функцию, которая приостанавливает задачу инвентаризации, если ресурсы компьютера заняты. Kaspersky Endpoint Security приостанавливает задачу инвентаризации, если не включена экранная заставка и разблокирован компьютер.
 - **Инвентаризация DLL-модулей.** Флажок включает / выключает функцию, которая анализирует данные о DLL-модулях и передает результаты анализа на Сервер администрирования.
 - **Инвентаризация файлов скриптов.** Флажок включает / выключает функцию, которая анализирует данные о файлах, содержащих скрипты, и передает результаты анализа на Сервер администрирования.
 - **Дополнительно.** По этой кнопке открывается окно **Дополнительные параметры**, в котором вы можете настроить следующие параметры:
 - **Проверять только новые и измененные файлы.** Флажок включает / выключает режим проверки только новых файлов и тех файлов, которые изменились после предыдущей инвентаризации.
 - **Пропускать файлы, если их проверка длится более.** Флажок включает / выключает ограничение длительности проверки одного файла. По истечении заданного в поле справа периода времени Kaspersky Endpoint Security прекращает проверку файла.
 - **Проверять архивы.** Флажок включает / выключает проверку архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE на наличие исполняемых файлов.
 - **Проверять дистрибутивы.** Флажок включает / выключает проверку дистрибутивов в процессе выполнения задачи инвентаризации.

- **Не распаковывать составные файлы большого размера.**

Если флажок установлен, то Kaspersky Endpoint Security не проверяет составные файлы, размеры которых больше заданного в поле **Максимальный размер файла** значения.

Если флажок снят, Kaspersky Endpoint Security проверяет составные файлы любого размера.

Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.



- **Максимальный размер файла.** Kaspersky Endpoint Security не распаковывает только те файлы, размер которых больше указанного в этом поле значения. Значение задается в мегабайтах.

Управление политиками

При помощи политик вы можете установить одинаковые значения параметров работы программы Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования.

Вы можете локально изменять значения параметров, заданные политикой, для отдельных компьютеров в группе администрирования при помощи Kaspersky Endpoint Security. Вы можете изменять локально только те параметры, изменение которых не запрещено политикой.

Возможность изменять параметры программы на клиентском компьютере определяется статусом относящегося к этим параметрам «замка» в свойствах политики:

- **Закрытый "замок"** () означает следующее:
 - Kaspersky Security Center накладывает запрет на изменение параметров, к которым относится этот замок, из интерфейса Kaspersky Endpoint Security на клиентских компьютерах. На всех клиентских компьютерах Kaspersky Endpoint Security использует одинаковые значения этих параметров – те, которые заданы в свойствах политики.
 - Kaspersky Security Center накладывает запрет на изменение параметров, к которым относится этот замок, в свойствах тех политик для вложенных групп администрирования и подчиненных Серверов администрирования, в которых включена функция **Наследовать параметры родительской политики**. Используются те значения этих параметров, которые заданы в свойствах политики верхнего уровня иерархии.
- **Открытый "замок"** () означает следующее:
 - Kaspersky Security Center снимает запрет на изменение параметров, к которым относится этот замок, из интерфейса Kaspersky Endpoint Security на клиентских компьютерах. На каждом клиентском компьютере Kaspersky Endpoint Security работает согласно локальному значению этих параметров, если компонент включен.
 - Kaspersky Security Center снимает запрет на изменение параметров, к которым относится этот замок, в свойствах тех политик для вложенных групп администрирования и подчиненных Серверов администрирования, в которых включена функция **Наследовать параметры родительской политики**. Значения этих параметров не зависят от того, что указано в свойствах политики верхнего уровня иерархии.

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

Права на доступ к параметрам политики (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, и отдельно для каждой функциональной области Kaspersky Endpoint Security. Для настройки прав доступа к параметрам политики перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center.

Выделены следующие функциональные области Kaspersky Endpoint Security:

- Базовая защита. Функциональная область включает компоненты Защита от файловых угроз, Защита от почтовых угроз, Защита от веб-угроз, Защита от сетевых угроз, Сетевой экран, задачи проверки.
- Контроль программ. Функциональная область включает компонент Контроль программ.
- Контроль устройств. Функциональная область включает компонент Контроль устройств.
- Шифрование. Функциональная область включает компоненты полнодискового шифрования, шифрования файлов.
- Доверенная зона. Функциональная область включает Доверенную зону.
- Веб-Контроль. Функциональная область включает компонент Веб-Контроль.
- Продвинутая защита. Функциональная область включает параметры KSN, компоненты Анализ поведения, Защита от эксплойтов, Предотвращение вторжений, Откат вредоносных действий.

Базовая функциональность. Функциональная область включает общие параметры программы, не указанные в других функциональных областях, в том числе: лицензирование, задачи инвентаризации и обновления баз и модулей программы, самозащита, дополнительные параметры программы, отчеты и хранилища, параметры защиты паролем и интерфейса программы.

В этом разделе

Создание политики	40
Изменение параметров политики.....	41
Индикатор уровня защиты в окне свойств политики	41

Создание политики

► *Чтобы создать политику, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
 - Выберите папку **Управляемые устройства** дерева Консоли администрирования, если вы хотите создать политику для всех управляемых программой Kaspersky Security Center компьютеров.
 - В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят интересующие вас клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.

4. Выполните одно из следующих действий:
 - Нажмите на кнопку **Новая политика**.
 - По правой клавише мыши откройте контекстное меню и выберите пункт **Создать** → **Политику**.
Запустится мастер создания политики.
5. Следуйте указаниям мастера создания политики.

В результате параметры Kaspersky Endpoint Security будут настроены на клиентских компьютерах при следующей синхронизации. Вы можете просмотреть информацию о политике, которая применена к компьютеру, в интерфейсе Kaspersky Endpoint Security по кнопке **Поддержка** на главном экране (например, имя политики). Для этого в параметрах политики Агента администрирования нужно включить получение расширенных данных политики. Подробнее о политике Агента администрирования см. в справке Kaspersky Security Center <https://help.kaspersky.com/KSC/11/ru-RU/>.

Изменение параметров политики

► Чтобы изменить параметры политики, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием нужной группы администрирования, для которой вы хотите изменить параметры политики.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
 - В контекстном меню политики выберите пункт **Свойства**.
 - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.

Параметры политики для Kaspersky Endpoint Security включают в себя параметры компонентов и параметры программы (см. раздел "Настройка параметров Kaspersky Endpoint Security" на стр. 30). В разделах **Продвинутая защита**, **Базовая защита** и **Контроль безопасности** окна **Свойства: <Название политики>** представлены параметры компонентов защиты и контроля, в разделе **Шифрование данных** представлены параметры полнодискового шифрования, шифрования файлов, шифрования съемных дисков, в разделе **Endpoint Sensor** приведены параметры компонента Endpoint Sensor, в разделе **Локальные задачи** приведены параметры локальных и групповых задач, а в разделе **Общие параметры** представлены параметры программы.

Параметры шифрования данных и компонентов контроля в параметрах политики отображаются, если установлены соответствующие флажки в окне Kaspersky Security Center **Настройка интерфейса**. По умолчанию эти флажки установлены.

6. Измените параметры политики.
7. Сохраните внесенные изменения.

Индикатор уровня защиты в окне свойств политики

В верхней части окна **Свойства: <Название политики>** отображается индикатор уровня защиты. Индикатор может принимать одно из следующих значений:


- **Уровень защиты высокий.** Индикатор принимает это значение и цвет индикатора изменяется на зеленый, если включены все компоненты, относящиеся к следующим категориям:
 - **Критические.** Категория включает следующие компоненты:
 - Защита от файловых угроз.
 - Анализ поведения.
 - Защита от эксплойтов.
 - Откат вредоносных действий.
 - **Важные.** Категория включает следующие компоненты:
 - Kaspersky Security Network.
 - Защита от веб-угроз.
 - Защита от почтовых угроз.
 - Предотвращение вторжений.
- **Уровень защиты средний.** Индикатор принимает это значение и цвет индикатора изменяется на желтый, если отключен один важный компонент.
- **Уровень защиты низкий.** Индикатор принимает это значение и цвет индикатора изменяется на красный в одном из следующих случаев:
 - отключены один или несколько критических компонентов;
 - отключены два или более важных компонента.




Если отображается индикатор со значением **Уровень защиты средний** или **Уровень защиты низкий**, то справа от индикатора доступна ссылка **Подробнее**, по которой открывается окно **Рекомендованные компоненты защиты**. В этом окне вы можете включить любой из рекомендованных компонентов защиты.

Интерфейс программы

В главном окне Kaspersky Endpoint Security находятся элементы интерфейса, предоставляющие вам доступ к основным функциям программы.

Главное окно программы содержит следующие элементы:

- Ссылка **Kaspersky Endpoint Security для Windows**. При нажатии на ссылку открывается окно **О программе** со сведениями о версии программы.
- Кнопка . При нажатии на кнопку осуществляется переход к справочной системе Kaspersky Endpoint Security.
- Блок **Технологии обнаружения угроз**. Блок содержит следующую информацию:
 - В левой части блока отображается список технологий обнаружения угроз. Справа от названия каждой из технологий обнаружения угроз отображается количество угроз, обнаруженных с помощью этой технологии.
 - В центре блока в зависимости от наличия активных угроз отображается одна из следующих надписей:
 - **Нет угроз**. Если отображается эта надпись, то при нажатии на блок **Технологии обнаружения угроз** открывается окно **Технологии обнаружения угроз**, в котором приведено краткое описание технологий обнаружения угроз, а также статус и глобальная статистика инфраструктуры облачных служб Kaspersky Security Network.
 - **N активных угроз**. Если отображается эта надпись, то при нажатии на блок **Технологии обнаружения угроз** открывается окно **Активные угрозы**, в котором приведен список событий, связанных с зараженными файлами, которые по каким-либо причинам не были обработаны.
- Блок **Компоненты защиты**. При нажатии на блок открывается окно **Компоненты защиты**. В этом окне вы можете посмотреть статус работы установленных компонентов. Также из этого окна вы можете для любого из установленных компонентов, кроме компонентов шифрования, открыть подраздел в окне **Настройка**, содержащий параметры этого компонента.
- Блок **Задачи**. При нажатии на блок открывается окно **Задачи**. В этом окне вы можете управлять работой задач Kaspersky Endpoint Security, посредством которых обеспечивается актуальность баз и модулей программы, выполняется проверка на присутствие вирусов или других программ, представляющих угрозу, а также выполняется проверка целостности.
- Кнопка **Отчеты**. При нажатии на кнопку открывается окно **Отчеты**, содержащее информацию о событиях, произошедших в ходе работы программы в целом, работы отдельных компонентов и выполнения задач.
- Кнопка **Хранилища**. При нажатии на кнопку открывается окно **Резервное хранилище**. В этом окне вы можете просмотреть список копий зараженных файлов, которые были удалены в ходе работы программы.
- Кнопка **Поддержка**. При нажатии на кнопку открывается окно **Поддержка** с информацией об операционной системе, текущей версии Kaspersky Endpoint Security и ссылками на информационные ресурсы "Лаборатории Касперского".
- Кнопка **Настройка**. При нажатии на кнопку открывается окно **Настройка**, в котором вы можете изменять параметры программы, установленные по умолчанию.

- Кнопка  /  / . При нажатии на кнопку открывается окно **События** с информацией о доступных обновлениях, а также с запросами доступа к зашифрованным файлам и устройствам.
- Ссылка **Лицензия**. При нажатии на ссылку открывается окно **Лицензирование** с информацией о действующей лицензии.

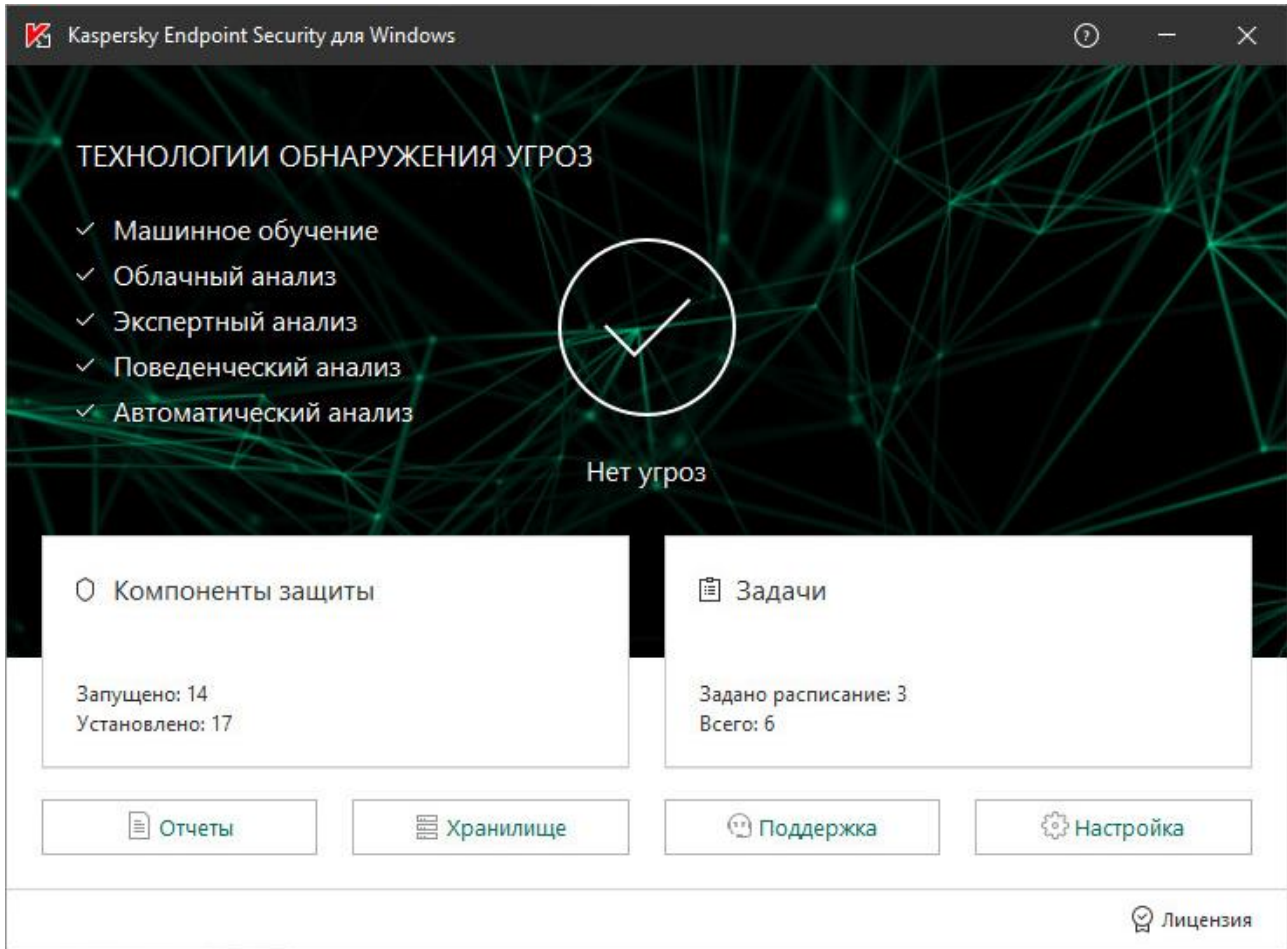


Рисунок 4. Главное окно программы

В этом разделе

Значок программы в области уведомлений	44
Главное окно программы	46
Упрощенный интерфейс программы.....	46
Настройка отображения интерфейса программы.....	47




Значок программы в области уведомлений

Сразу после установки Kaspersky Endpoint Security значок программы появляется в области уведомлений панели задач Microsoft Windows.

Значок программы выполняет следующие функции:

- служит индикатором работы программы;
- обеспечивает доступ к контекстному меню значка программы и главному окну программы.

Для отображения информации о работе программы предназначены следующие статусы значка программы:

- Значок  означает, что работа всех компонентов защиты программы включена.
- Значок  означает, что в работе Kaspersky Endpoint Security произошли события с уровнем важности Предупреждение. Например, выключен компонент Защита от файловых угроз, базы программы устарели.
- Значок  означает, что в работе Kaspersky Endpoint Security произошли события критической важности. Например, сбой в работе компонента, повреждение баз программы.

Контекстное меню значка программы содержит следующие пункты:

- **Kaspersky Endpoint Security для Windows.** Открывает главное окно программы. В этом окне вы можете регулировать работу компонентов и задач программы, просматривать статистику об обработанных файлах и обнаруженных угрозах.
- **Настройка.** Открывает окно настройки параметров программы.
- **Приостановка защиты и контроля / Возобновление защиты и контроля.** Приостановка работы всех компонентов защиты и контроля, не отмеченных в политике замком (🔒). Перед выполнением этой операции рекомендуется выключить политику Kaspersky Security Center.

Перед приостановкой работы компонентов защиты и контроля программа запрашивает пароль доступа к Kaspersky Endpoint Security (см. раздел "Защита паролем" на стр. [197](#)) (пароль учетной записи или временный пароль). Далее вы можете выбрать период приостановки: на указанное время, до перезагрузки или по требованию пользователя.

Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. [200](#)). Для возобновления работы компонентов защиты и контроля выберите пункт **Возобновление защиты и контроля** в контекстном меню программы.

Приостановка работы компонентов защиты и контроля не влияет на выполнение задач обновления и проверки. Также программа продолжает использование Kaspersky Security Network.

- **Выключение политики / Включение политики.** Выключает политику Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком (🔒). При выключении политики программа запрашивает пароль доступа к Kaspersky Endpoint Security (см. раздел "Защита паролем" на стр. [197](#)) (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. [200](#)). Для включения политики выберите пункт **Включение политики** в контекстном меню программы.

- **Поддержка.** Вызов окна **Поддержка**, содержащего информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".
- **О программе.** Открывает информационное окно со сведениями о программе.
- **Выход.** Завершает работу Kaspersky Endpoint Security. Если вы выбрали этот пункт контекстного меню, программа выгружается из оперативной памяти компьютера.



Рисунок 5. Контекстное меню значка программы

Упрощенный интерфейс программы

Если к клиентскому компьютеру, на котором установлена программа Kaspersky Endpoint Security, применена политика Kaspersky Security Center, в которой настроено отображение упрощенного интерфейса программы (см. раздел "Настройка отображения интерфейса программы" на стр. [47](#)), то на этом клиентском компьютере недоступно главное окно программы. По правой клавише мыши пользователь может открыть контекстное меню значка Kaspersky Endpoint Security (см. рис. ниже), содержащее следующие пункты:

- **Выключение политики / Включение политики.** Выключает политику Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком (🔒). При выключении политики программа запрашивает пароль доступа к Kaspersky Endpoint Security (см. раздел "Защита паролем" на стр. [197](#)) (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. [200](#)). Для включения политики выберите пункт **Включение политики** в контекстном меню программы.
- **Задачи.** Раскрывающийся список, содержащий следующие элементы:
 - **Обновление.**
 - **Откат последнего обновления.**
 - **Полная проверка.**
 - **Выборочная проверка.**
 - **Проверка важных областей.**
 - **Проверка целостности.**

- **Поддержка.** Вызов окна **Поддержка**, содержащего информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".
- **Выход.** Завершает работу Kaspersky Endpoint Security. Если вы выбрали этот пункт контекстного меню, программа выгружается из оперативной памяти компьютера.

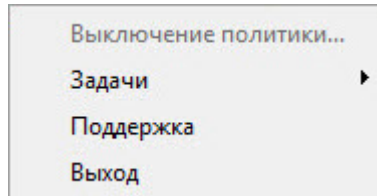


Рисунок 7. Контекстное меню значка программы при отображении упрощенного интерфейса программы

Настройка отображения интерфейса программы

► Чтобы настроить отображение интерфейса программы, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В разделе **Общие параметры** выберите подраздел **Интерфейс**.
6. В блоке **Взаимодействие с пользователем** выполните одно из следующих действий:
 - Установите флажок **Отображать интерфейс программы**, если вы хотите, чтобы на клиентском компьютере отображались следующие элементы интерфейса:
 - папка с названием программы в меню **Пуск**;
 - значок Kaspersky Endpoint Security (см. раздел "Значок программы в области уведомлений" на стр. [44](#)) в области уведомлений панели задач Microsoft Windows;
 - всплывающие уведомления.

Если установлен этот флажок, пользователь может просматривать и, при наличии прав, изменять параметры программы из интерфейса программы.
 - Снимите флажок **Отображать интерфейс программы**, если вы хотите скрыть все признаки работы Kaspersky Endpoint Security на клиентском компьютере.
7. В блоке **Взаимодействие с пользователем** установите флажок **Упрощенный интерфейс программы**, если вы хотите, чтобы на клиентском компьютере с установленной программой Kaspersky Endpoint Security отображался упрощенный интерфейс программы (на стр. [46](#)).

Запуск и остановка программы

Запуск и остановка программы вручную

Специалисты "Лаборатории Касперского" рекомендуют не завершать работу Kaspersky Endpoint Security, поскольку в этом случае защита компьютера и ваших данных окажется под угрозой. Если требуется, вы можете приостановить защиту компьютера (см. раздел "Приостановка и возобновление защиты и контроля компьютера" на стр. [49](#)) на необходимый срок, не завершая работу программы.

Запускать Kaspersky Endpoint Security вручную требуется в том случае, если вы выключили автоматический запуск программы (на стр. [49](#)).

► *Чтобы запустить программу вручную,*

в меню **Пуск** выберите пункт **Программы** → **Kaspersky Endpoint Security для Windows**.

► *Чтобы завершить работу программы вручную, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню выберите пункт **Выход**.

Запуск и остановка программы из командной строки

Специалисты "Лаборатории Касперского" рекомендуют не завершать работу Kaspersky Endpoint Security, поскольку в этом случае защита компьютера и ваших данных окажется под угрозой. Если требуется, вы можете приостановить защиту компьютера (см. раздел "Приостановка и возобновление защиты и контроля компьютера" на стр. [49](#)) на необходимый срок, не завершая работу программы.

Для завершения работы программы из командной строки необходимо, чтобы флажок **Выключить внешнее управление системными службами** (см. раздел "Включение и выключение механизма защиты от внешнего управления" на стр. [285](#)) был снят.

Вы можете запустить или завершить работу программы из командной строки.

Для запуска или завершения работы программы из командной строки используется файл `klpsm.exe`, входящий в комплект поставки Kaspersky Endpoint Security.

► *Чтобы запустить программу, выполните следующие действия:*

1. Запустите интерпретатор командной строки `cmd` от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. В командной строке введите `klpsm.exe start_avp_service`.

► *Чтобы завершить работу программы, выполните следующие действия:*

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

В командной строке введите `klpsm.exe stop_avp_service`.

В этом разделе

Автоматический запуск программы.....	49
Приостановка и возобновление защиты и контроля компьютера.....	49

Автоматический запуск программы

Под автоматическим запуском программы подразумевается запуск Kaspersky Endpoint Security, который выполняется без участия пользователя после загрузки операционной системы. Этот вариант запуска программы установлен по умолчанию.

В первый раз программа Kaspersky Endpoint Security запускается автоматически после ее установки.

Загрузка антивирусных баз Kaspersky Endpoint Security после загрузки операционной системы занимает до двух минут, в зависимости от производительности (технических возможностей) компьютера. В течение этого времени уровень защиты компьютера снижен. Загрузка антивирусных баз при запуске программы Kaspersky Endpoint Security в уже запущенной операционной системе не вызывает снижения уровня защиты компьютера.

Настроить автоматический запуск программы в параметрах операционной системы невозможно. По умолчанию автоматический запуск программы включен.



► *Чтобы выключить автоматический запуск программы, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры программы**.
3. Снимите флажок **Запускать Kaspersky Endpoint Security для Windows при включении компьютера**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Приостановка и возобновление защиты и контроля компьютера

Приостановка защиты и контроля компьютера означает выключение на некоторое время всех компонентов защиты и всех компонентов контроля Kaspersky Endpoint Security.

Состояние программы отображается с помощью значка программы в области уведомлений панели задач (см. раздел «Значок программы в области уведомлений» на стр. [44](#)):

- значок  свидетельствует о приостановке защиты и контроля компьютера;
- значок  свидетельствует о том, что защита и контроль компьютера включены.

Приостановка и возобновление защиты и контроля компьютера не оказывает влияния на выполнение задач проверки и задачи обновления.

Если в момент приостановки и возобновления защиты и контроля компьютера были установлены сетевые соединения, на экран выводится уведомление о разрыве этих сетевых соединений.

► *Чтобы приостановить защиту и контроль компьютера, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню выберите пункт **Приостановка защиты и контроля**.
Откроется окно **Приостановка защиты**.
3. Выберите один из следующих вариантов:
 - **Приостановить на указанное время** – защита и контроль компьютера включатся через интервал времени, указанный в раскрывающемся списке ниже.
 - **Приостановить до перезагрузки** – защита и контроль компьютера включатся после перезапуска программы или перезагрузки операционной системы. Для использования этой возможности должен быть включен автоматический запуск программы.
 - **Приостановить** – защита и контроль компьютера включатся тогда, когда вы решите возобновить их.
4. Если на предыдущем шаге вы выбрали вариант **Приостановить на указанное время**, выберите нужный интервал в раскрывающемся списке.

► *Чтобы возобновить защиту и контроль компьютера, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню выберите пункт **Возобновление защиты и контроля**.

Вы можете возобновить защиту и контроль компьютера в любой момент, независимо от того, какой вариант приостановки защиты и контроля компьютера вы выбрали ранее.

Проверка компьютера

Антивирусная проверка является важным фактором для обеспечения безопасности компьютера. Требуется регулярно выполнять антивирусную проверку, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам.

Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive, и создает в журнале записи о том, что эти файлы не были проверены.

Полная проверка

Тщательная проверка всей системы. Kaspersky Endpoint Security проверяет следующие объекты:

- память ядра;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- загрузочные секторы;
- резервное хранилище операционной системы;
- все жесткие и съемные диски.

Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задачи *Полная проверка*.

Для экономии ресурсов компьютера рекомендуется вместо задачи полной проверки запускать задачу фоновой проверки. Уровень защиты компьютера при этом не изменится.

Проверка важных областей

По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задачи *Проверка важных областей*.

Выборочная проверка

Kaspersky Endpoint Security проверяет объекты, выбранные пользователем. Вы можете проверить любой объект из следующего списка:

- память ядра;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- резервное хранилище операционной системы;
- почтовый ящик Outlook;
- жесткие, съемные и сетевые диски;
- любой выбранный файл.

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security проверяет объекты автозапуска, памяти ядра и системного раздела.

Проверка целостности

Kaspersky Endpoint Security проверяет модули программы на наличие повреждений или изменений.

В этом разделе

Запуск и остановка задачи проверки	52
Изменение уровня безопасности	53
Изменение действия над зараженными файлами.....	53
Формирование списка проверяемых объектов	54
Выбор типа проверяемых файлов	55
Оптимизация проверки файлов.....	56
Проверка составных файлов	57
Использование методов проверки	57
Использование технологий проверки	58
Выбор режима запуска для задачи проверки.....	59
Настройка запуска задачи проверки с правами другого пользователя	59
Проверка съемных дисков при подключении к компьютеру	60
Фоновая проверка.....	61

Запуск и остановка задачи проверки

Независимо от выбранного режима запуска задачи проверки вы можете запустить или остановить задачу проверки в любой момент.

► *Чтобы запустить или остановить задачу проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки.
3. Выполните одно из следующих действий:
 - Нажмите на кнопку **Запустить**, если вы хотите запустить задачу проверки.
Статус выполнения задачи, отображающийся под названием задачи проверки, изменится на *Выполняется*.
 - Выберите в контекстном меню пункт **Остановить**, если вы хотите остановить задачу проверки.
Статус выполнения задачи, отображающийся под названием задачи проверки, изменится на *Остановлена*.

► Чтобы запустить или остановить задачу проверки при отображении упрощенного интерфейса программы, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:
 - выберите незапущенную задачу проверки, чтобы запустить ее;
 - выберите запущенную задачу проверки, чтобы остановить ее;
 - выберите остановленную задачу проверки, чтобы возобновить ее или запустить ее заново.

Изменение уровня безопасности

Для выполнения задач проверки Kaspersky Endpoint Security применяет разные наборы параметров. Наборы параметров, сохраненные в программе, называются *уровнями безопасности*. Предусмотрены три уровня безопасности: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными. Они рекомендованы специалистами "Лаборатории Касперского". Вы можете выбрать один из предусмотренных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

► Чтобы изменить уровень безопасности, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Полная проверка, Проверка важных областей** или **Выборочная проверка**.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
 - Если вы хотите применить один из предусмотренных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
 - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне с названием задачи проверки.
После того как вы самостоятельно настроили уровень безопасности, название уровня безопасности в блоке **Уровень безопасности** изменится на **Другой**.
 - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия над зараженными файлами

По умолчанию при обнаружении зараженных файлов Kaspersky Endpoint Security пытается вылечить их или удаляет их, если лечение невозможно.

► Чтобы изменить действие над зараженными файлами, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Полная проверка, Проверка важных областей, Выборочная проверка** или **Проверка из контекстного меню**.
3. В блоке **Действие при обнаружении угрозы**, выберите один из следующих вариантов:
 - Установите флажок **Лечить; удалять, если лечение невозможно**, если вы хотите, чтобы при обнаружении зараженных файлов Kaspersky Endpoint Security пытался вылечить их или удалял их, если лечение невозможно.
 - Установите флажок **Лечить; информировать, если лечение невозможно**, если вы хотите, чтобы при обнаружении зараженных файлов Kaspersky Endpoint Security пытался вылечить их и информировал вас, если лечение невозможно.
 - Установите флажок **Информировать**, если вы хотите, чтобы при обнаружении зараженных файлов Kaspersky Endpoint Security информировал вас об этом.

При обнаружении зараженных файлов, являющихся частью приложения Windows Store, Kaspersky Endpoint Security выполняет действие **Удалить**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка проверяемых объектов

► Чтобы сформировать список проверяемых объектов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Полная проверка, Проверка важных областей, Выборочная проверка** или **Проверка из контекстного меню**.
3. Нажмите на кнопку **Область проверки**.
Откроется окно **Область проверки**.
4. Если вы хотите добавить новый объект в область проверки, выполните следующие действия:
 - a. Нажмите на кнопку **Добавить**.
Откроется окно **Выбор области проверки**.
 - b. Выберите объект и нажмите на кнопку **Добавить**.
Все объекты, выбранные в окне **Выбор области проверки**, отобразятся в списке **Область проверки**.
 - c. Нажмите на кнопку **ОК**.

5. Если вы хотите изменить путь к объекту области проверки, выполните следующие действия:
 - a. Выберите объект из области проверки.
 - b. Нажмите на кнопку **Изменить**.
Откроется окно **Выбор области проверки**.
 - c. Введите новый путь к объекту области проверки.
 - d. Нажмите на кнопку **ОК**.

Вы не можете удалить или изменить объекты, включенные в область проверки по умолчанию.

6. Если вы хотите удалить объект из области проверки, выполните следующие действия:
 - a. Выберите объект, который вы хотите удалить из области проверки.
Чтобы выбрать несколько объектов, выделяйте их, удерживая клавишу **CTRL**.
 - b. Нажмите на кнопку **Удалить**.
Откроется окно подтверждения удаления.
 - c. Нажмите на кнопку **Да** в окне подтверждения удаления.

Вы не можете удалить или изменить объекты, включенные в область проверки по умолчанию.

7. Чтобы исключить объект из области проверки, в окне **Область проверки** снимите флажок рядом с ним.
Объект остается в списке объектов области проверки, но не проверяется во время выполнения задачи проверки.
8. Сохраните внесенные изменения.

Выбор типа проверяемых файлов

Выбирая тип проверяемых файлов, нужно учитывать следующее:

1. Вероятность внедрения вредоносного кода в файлы некоторых форматов и его последующей активации низка (например, формат TXT). В то же время существуют форматы файлов, которые содержат исполняемый код (например, форматы EXE, DLL). Также исполняемый код могут содержать форматы файлов, которые для этого не предназначены (например, формат DOC). Риск внедрения в такие файлы вредоносного кода и его активации высок.
2. Злоумышленник может отправить вирус или другую программу, представляющую угрозу, на ваш компьютер в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки программа пропускает такой файл. Если же выбрана проверка файлов по формату, то вне зависимости от расширения компонент Защита от файловых угроз анализирует заголовок файла. Если в результате выясняется, что файл имеет формат исполняемого файла (например, EXE), то программа проверяет его.

► *Чтобы выбрать тип проверяемых файлов выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Полная проверка, Проверка важных областей, Выборочная проверка** или **Проверка из контекстного меню**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно с названием выбранной задачи проверки.
4. В окне с названием выбранной задачи проверки выберите закладку **Область действия**.
5. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять во время выполнения выбранной задачи проверки:
 - Выберите **Все файлы**, если вы хотите проверять все файлы.
 - Выберите **Файлы, проверяемые по формату**, если вы хотите проверять файлы тех форматов, которые наиболее подвержены заражению.
 - Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, типичными для файлов, которые наиболее подвержены заражению.
6. Сохраните внесенные изменения.

Оптимизация проверки файлов

Вы можете оптимизировать проверку файлов: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security. Этого можно достичь, если проверять только новые файлы и те файлы, что изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы. Вы можете также ограничить длительность проверки одного файла. По истечении заданного времени Kaspersky Endpoint Security исключает файл из текущей проверки (кроме архивов и объектов, в состав которых входит несколько файлов).

Вы также можете включить использование технологий iChecker и iSwift. Технологии iChecker и iSwift позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

► *Чтобы оптимизировать проверку файлов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Полная проверка, Проверка важных областей, Выборочная проверка** или **Проверка из контекстного меню**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне выберите закладку **Область действия**.
5. В блоке **Оптимизация проверки** выполните следующие действия:
 - Установите флажок **Проверять только новые и измененные файлы**.
 - Установите флажок **Пропускать файлы, если их проверка длится более** и задайте длительность проверки одного файла (в секундах).
6. Сохраните внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие программы, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить типы проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Чтобы настроить проверку составных файлов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Полная проверка, Проверка важных областей** или **Выборочная проверка**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне выберите закладку **Область действия**.
5. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты, файлы офисных форматов, файлы почтовых форматов, защищенные паролем архивы.
6. Если в блоке **Оптимизация проверки** снят флажок **Проверять только новые и измененные файлы**, нажмите на ссылку **все / новые**, расположенную рядом с названием типа составного файла, чтобы выбрать, следует ли проверять все файлы этого типа или только новые файлы этого типа.

Ссылка меняет свое значение при нажатии.

Если флажок **Проверять только новые и измененные файлы** установлен, то проверяются только новые файлы.

7. Нажмите на кнопку **Дополнительно**.
Откроется окно **Составные файлы**.
8. В блоке **Ограничение по размеру** выполните одно из следующих действий:
 - Если вы не хотите распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.
 - Если вы хотите распаковывать составные файлы независимо от размера, снимите флажок **Не распаковывать составные файлы большого размера**.

Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

9. Сохраните внесенные изменения.

Использование методов проверки

Во время своей работы Kaspersky Endpoint Security использует метод проверки Машинное обучение и сигнатурный анализ. В процессе сигнатурного анализа Kaspersky Endpoint Security сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Endpoint Security анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать вредоносные объекты, записей о которых еще нет в базах Kaspersky Endpoint Security.

► *Чтобы использовать методы проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Полная проверка, Проверка важных областей, Выборочная проверка** или **Проверка из контекстного меню**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне выберите закладку **Дополнительно**.
5. В блоке **Методы проверки** установите флажок **Эвристический анализ**, если вы хотите, чтобы программа использовала эвристический анализ во время выполнения задачи проверки. Далее при помощи ползунка задайте уровень эвристического анализа: **поверхностный, средний** или **глубокий**.
6. Сохраните внесенные изменения.

Использование технологий проверки

► *Чтобы использовать технологии проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Полная проверка, Проверка важных областей, Выборочная проверка** или **Проверка из контекстного меню**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне выберите закладку **Дополнительно**.
5. В блоке **Технологии проверки** установите флажки около названий технологий, которые вы хотите использовать во время проверки.
6. Сохраните внесенные изменения.

Выбор режима запуска для задачи проверки

Если по каким-либо причинам запуск задачи проверки невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи проверки, как только это станет возможным.

Вы можете отложить запуск задачи проверки после старта программы для случаев, если вы выбрали режим запуска задачи проверки **По расписанию** и время запуска Kaspersky Endpoint Security совпадает с расписанием запуска задачи проверки. Задача проверки запускается только по истечении указанного времени после старта Kaspersky Endpoint Security.

► *Чтобы выбрать режим запуска для задачи проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Полная проверка, Проверка важных областей** или **Выборочная проверка**.
3. Нажмите на кнопку **Режим запуска**.
Откроется окно свойств выбранной задачи на закладке **Режим запуска**.
4. В блоке **Режим запуска** выберите режим запуска задачи: **Вручную** или **По расписанию**.
5. Если вы выбрали вариант **По расписанию**, задайте параметры расписания. Для этого выполните следующие действия:
 - a. В раскрывающемся списке **Периодичность** выберите периодичность запуска задачи (**Минуты, Часы, Дни, Каждую неделю, В указанное время, Каждый месяц, После запуска программы, После каждого обновления**).
 - b. В зависимости от выбранной периодичности настройте дополнительные параметры, которые уточняют расписание запуска задачи.
 - c. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенные вовремя задачи проверки.

Если в раскрывающемся списке **Периодичность** выбран элемент **Минуты, Часы, После запуска программы** или **После каждого обновления**, то флажок **Запускать пропущенные задачи** недоступен.

- d. Установите флажок **Выполнять только во время простоя компьютера**, если вы хотите, чтобы Kaspersky Endpoint Security приостанавливал задачу, когда ресурсы компьютера заняты.
Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.
6. Сохраните внесенные изменения.

Настройка запуска задачи проверки с правами другого пользователя

По умолчанию задача проверки запускается с правами учетной записи, под которой пользователь зарегистрирован в операционной системе. Однако может возникнуть необходимость запустить задачу проверки с правами другого пользователя. Вы можете указать пользователя, обладающего этими правами, в параметрах задачи проверки и запускать задачу проверки от имени этого пользователя.

► *Чтобы настроить запуск задачи проверки с правами другого пользователя, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Полная проверка, Проверка важных областей** или **Выборочная проверка**.
3. Нажмите на кнопку **Режим запуска**.
Откроется окно свойств выбранной задачи на закладке **Режим запуска**.
4. На закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами пользователя**.
5. В поле **Имя** введите имя пользователя, права которого требуется использовать для запуска задачи проверки.
6. В поле **Пароль** введите пароль пользователя, права которого требуется использовать для запуска задачи проверки.
7. Сохраните внесенные изменения.

Проверка съемных дисков при подключении к компьютеру

Некоторые вредоносные программы используют уязвимости операционной системы для распространения через локальные сети и съемные диски. Kaspersky Endpoint Security позволяет проверять на вирусы и другие программы, представляющие угрозу, съемные диски при их подключении к компьютеру.

► *Чтобы настроить проверку съемных дисков при их подключении к компьютеру, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Проверка съемных дисков**.
3. В раскрывающемся списке **Действие при подключении съемного диска** выберите нужное действие:
 - **Не проверять.**
 - **Подробная проверка.**

В этом режиме Kaspersky Endpoint Security проверяет все файлы, расположенные на съемном диске, в том числе вложенные файлы внутри составных объектов.

- **Быстрая проверка.**

В этом режиме Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы, а также не распаковывает составные объекты.

4. Выполните одно из следующих действий:

- Если вы хотите, чтобы Kaspersky Endpoint Security проверял только те съемные диски, размер которых не превышает указанного значения, установите флажок **Максимальный размер съемного диска** и укажите в соседнем поле значение в мегабайтах.
- Если вы хотите, чтобы Kaspersky Endpoint Security проверял все съемные диски, снимите флажок **Максимальный размер съемного диска**.

5. Выполните одно из следующих действий:

- Если вы хотите, чтобы программа Kaspersky Endpoint Security отображала ход проверки съемных дисков в отдельном окне, установите флажок **Отображать ход проверки**.

В окне проверки съемного диска пользователь может остановить проверку. Чтобы сделать проверку съемных дисков обязательной и запретить пользователю останавливать проверку, установите флажок **Запретить остановку задачи проверки**.

- Если вы хотите, чтобы программа Kaspersky Endpoint Security запускала проверку съемных дисков в фоновом режиме, снимите флажок **Отображать ход проверки**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security проверяет объекты автозапуска, памяти ядра и системного раздела. Фоновая проверка запускается в следующих случаях:

- после обновления антивирусных баз;
- через 30 минут после запуска Kaspersky Endpoint Security;
- каждые шесть часов;
- при простое компьютера в течение пяти и более минут.

Фоновая проверка при простое компьютера прерывается при выполнении любого из следующих условий:

- Компьютер перешел в активный режим.

Если фоновая проверка не выполнялась более десяти дней, проверка не прерывается.

- Компьютер (ноутбук) перешел в режим питания от батареи.

При выполнении фоновой проверки Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

► *Чтобы включить фоновую проверку компьютера, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Фоновая проверка**.
3. Установите флажок **Выполнять проверку во время простоя компьютера**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Доверенная зона

Доверенная зона – это сформированный администратором системы список объектов и программ, которые Kaspersky Endpoint Security не контролирует в процессе работы. Иначе говоря, это набор исключений из проверки.

Доверенную зону администратор системы формирует самостоятельно в зависимости от особенностей объектов, с которыми требуется работать, а также от программ, установленных на компьютере. Включение объектов и программ в доверенную зону может потребоваться, например, если Kaspersky Endpoint Security блокирует доступ к какому-либо объекту или программе, в то время как вы уверены, что этот объект или программа безвредны.

Вы можете исключать из проверки объекты следующими способами:

- укажите путь к файлу или папке;
- введите хеш объекта;
- используйте маски:
 - Символ *, который заменяет любой набор символов, в том числе пустой, кроме символов \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:**.txt будет включать все пути к файлам с расширением txt, расположенным в папках на диске C, но не в подпапках.
 - Два введенных подряд символа * заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:\Folder***.txt будет включать все пути к файлам с расширением txt в папке Folder и вложенных папках. Маска должна включать хотя бы один уровень вложенности. Маска C:***.txt не работает.
 - Символ ?, который заменяет любой один символ, кроме символов \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:\Folder\???.txt будет включать пути ко всем расположенным в папке Folder файлам с расширением txt и именем, состоящим из трех символов.
- введите название объекта по классификации Вирусной энциклопедии "Лаборатории Касперского" <https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/> (например, Email-Worm, Rootkit или RemoteAdmin).

Исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security не проверяет объект на вирусы и другие программы, представляющие угрозу.

Исключения из проверки позволяют работать с легальными программами, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы злоумышленниками. Подробную информацию о легальных программах, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского" <https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/>.

В результате работы Kaspersky Endpoint Security такие программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ вы можете настроить исключения из проверки. Для этого нужно добавить в доверенную зону название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского". Например, вы часто используете в своей работе программу Radmin, предназначенную для удаленного управления компьютерами. Такая активность программы

рассматривается Kaspersky Endpoint Security как подозрительная и может быть заблокирована. Чтобы исключить блокировку программы, нужно сформировать исключение из проверки, где указать название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского".

Если у вас на компьютере установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Endpoint Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из проверки, настроив Kaspersky Endpoint Security способом, описанным в этом документе.

Исключения из проверки могут использоваться в ходе работы следующих компонентов и задач программы, заданных администратором системы:

- Анализ поведения.
- Защита от эксплойтов.
- Предотвращение вторжений.
- Защита от файловых угроз.
- Защита от веб-угроз.
- Защита от почтовых угроз.
- Задачи проверки.

Список доверенных программ

Список доверенных программ – это список программ, у которых Kaspersky Endpoint Security не контролирует файловую и сетевую активность (в том числе и вредоносную), а также обращения этих программ к системному реестру. По умолчанию Kaspersky Endpoint Security проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и создаваемый ими сетевой трафик. Kaspersky Endpoint Security исключает из проверки программу, добавленную в список доверенных программ (см. раздел "Формирование списка доверенных программ" на стр. [69](#)).

Например, если вы считаете объекты, используемые программой Microsoft Windows Блокнот, безопасными и не требующими проверки, то есть доверяете этой программе, вам следует добавить программу Microsoft Windows Блокнот в список доверенных программ, чтобы не проверять объекты, используемые этой программой.

Кроме того, некоторые действия, которые Kaspersky Endpoint Security классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда программ. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием программ автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких программ и отключить контроль их активности, рекомендуется добавить их в список доверенных программ.

Исключение доверенных программ из проверки позволяет избежать проблемы совместимости Kaspersky Endpoint Security с другими программами (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Endpoint Security и другой антивирусной программой), а также увеличить производительность компьютера, что особенно важно при использовании серверных программ.

В то же время исполняемый файл и процесс доверенной программы по-прежнему проверяются на наличие в них вирусов и других программ, представляющих угрозу. Для полного исключения программы из проверки Kaspersky Endpoint Security следует пользоваться исключениями из проверки.

В этом разделе

Создание исключения из проверки	65
Изменение исключения из проверки	67
Удаление исключения из проверки	68
Запуск и остановка работы исключения из проверки	68
Формирование списка доверенных программ	69
Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ	70
Использование доверенного системного хранилища сертификатов	71

Создание исключения из проверки

Kaspersky Endpoint Security не проверяет объект, если при запуске одной из задач проверки в область проверки включен диск, на котором находится объект, или папка, в которой находится объект. Однако при запуске задачи выборочной проверки именно для этого объекта исключение из проверки не применяется.

► Чтобы создать исключение из проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Исключения**.
3. В блоке **Исключения из проверки и доверенные программы** нажмите на кнопку **Настройка**.
Откроется окно **Доверенная зона** на закладке **Исключения из проверки**.
4. Нажмите на кнопку **Добавить**.
Откроется окно **Исключение из проверки**. В этом окне вы можете сформировать исключение из проверки, используя один или оба критерия из блока **Свойства**.
5. Если вы хотите исключить из проверки файл или папку, выполните следующие действия:
 - a. В блоке **Свойства** установите флажок **Файл или папка**.
 - b. По ссылке **выберите файл или папку**, расположенной в блоке **Описание исключения из проверки**, откройте окно **Имя файла или папки**.
 - c. Введите имя файла или папки, маску имени файла или папки или выберите файл или папку в дереве папок, нажав на кнопку **Обзор**.

Используйте маски:

- Символ *, который заменяет любой набор символов, в том числе пустой, кроме символов \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:**.txt будет включать все пути к файлам с расширением txt, расположенным в папках на диске C, но не в подпапках.

- Два введенных подряд символа * заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:\Folder***.txt будет включать все пути к файлам с расширением txt в папке Folder и вложенных папках. Маска должна включать хотя бы один уровень вложенности. Маска C:***.txt не работает.
- Символ ?, который заменяет любой один символ, кроме символов \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:\Folder\???.txt будет включать пути ко всем расположенным в папке Folder файлам с расширением txt и именем, состоящим из трех символов.

В маске имени файла или папки вы можете использовать символ *, который заменяет любой набор символов в имени файла.

Например, вы можете использовать маски для добавления следующих путей:

- Пути к файлам, расположенным в любой из папок:
 - Маска *.exe будет включать все пути к файлам с расширением exe.
 - Маска example* будет включать все пути к файлам с именем EXAMPLE.
 - Пути к файлам, расположенным в указанной папке:
 - маска C:\dir*. * будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\;
 - маска C:\dir* будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\;
 - маска C:\dir\ будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\;
 - маска C:\dir*.exe будет включать все пути к файлам с расширением exe в папке C:\dir\, но не в подпапках папки C:\dir\;
 - маска C:\dir\test будет включать все пути к файлам с именем test в папке C:\dir\, но не в подпапках папки C:\dir\;
 - маска C:\dir*\test будет включать все пути к файлам с именем test в папке C:\dir\ и в подпапках папки C:\dir\.
 - Пути к файлам, расположенным во всех папках с указанным именем:
 - маска dir*. * будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
 - маска dir* будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
 - маска dir\ будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
 - маска dir*.exe будет включать все пути к файлам с расширением exe в папках с именем dir, но не в подпапках этих папок;
 - маска dir\test будет включать все пути к файлам с именем test в папках с именем dir, но не в подпапках этих папок.
- d. Нажмите на кнопку **ОК** в окне **Имя файла или папки**.

Ссылка на добавленный файл или папку появится в блоке **Описание исключения из проверки** окна **Исключение из проверки**.

6. Если вы хотите исключить из проверки объекты с определенным названием, выполните следующие действия:
 - a. В блоке **Свойства** установите флажок **Название объекта**.
 - b. По ссылке **введите название объекта**, расположенной в блоке **Описание исключения из проверки**, откройте окно **Название объекта**.
 - c. Введите название или маску названия объекта согласно классификации Вирусной энциклопедии "Лаборатории Касперского".
 - d. Нажмите на кнопку **ОК** в окне **Название объекта**.

Ссылка на добавленное название объекта появится в блоке **Описание исключения из проверки** окна **Исключение из проверки**.
7. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.
8. Определите компоненты Kaspersky Endpoint Security, в работе которых должно быть использовано исключение из проверки:
 - a. По ссылке **любые**, расположенной в блоке **Описание исключения из проверки**, активируйте ссылку **выберите компоненты**.
 - b. По ссылке **выберите компоненты** откройте окно **Компоненты защиты**.
 - c. Установите флажки напротив тех компонентов, на работу которых должно распространяться исключение из проверки.
 - d. Нажмите на кнопку **ОК** в окне **Компоненты защиты**.

Если компоненты указаны в параметрах исключения из проверки, то исключение применяется при проверке только этими компонентами Kaspersky Endpoint Security.

Если компоненты не указаны в параметрах исключения из проверки, то исключение применяется при проверке всеми компонентами Kaspersky Endpoint Security.
9. Нажмите на кнопку **ОК** в окне **Исключение из проверки**.

Добавленное исключение из проверки появится в таблице на закладке **Исключения из проверки** окна **Доверенная зона**. В блоке **Описание исключения из проверки** отобразятся заданные параметры этого исключения из проверки.
10. Сохраните внесенные изменения.

Изменение исключения из проверки

► *Чтобы изменить исключение из проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Исключения**.
3. В блоке **Исключения из проверки и доверенные программы** нажмите на кнопку **Настройка**.

Откроется окно **Доверенная зона** на закладке **Исключения из проверки**.
4. В списке выберите нужное исключение из проверки.

5. Измените параметры исключения из проверки одним из следующих способов:
 - Нажмите на кнопку **Изменить**.
Откроется окно **Исключения из проверки**.
 - Откройте окно для изменения нужного параметра по ссылке в поле **Описание исключения из проверки**.
6. Если на предыдущем шаге вы нажали на кнопку **Изменить**, нажмите на кнопку **ОК** в окне **Исключение из проверки**.
В блоке **Описание исключения из проверки** отобразятся измененные параметры исключения из проверки.
7. Сохраните внесенные изменения.

Удаление исключения из проверки

► *Чтобы удалить исключение из проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Исключения**.
3. В блоке **Исключения из проверки и доверенные программы** нажмите на кнопку **Настройка**.
Откроется окно **Доверенная зона** на закладке **Исключения из проверки**.
4. В списке исключений из проверки выберите нужное исключение из проверки.
5. Нажмите на кнопку **Удалить**.
Удаленное исключение из проверки исчезнет из списка.
6. Сохраните внесенные изменения.

Запуск и остановка работы исключения из проверки

► *Чтобы запустить или остановить работу исключения из проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Исключения**.
3. В блоке **Исключения из проверки и доверенные программы** нажмите на кнопку **Настройка**.
Откроется окно **Доверенная зона** на закладке **Исключения из проверки**.
4. В списке исключений из проверки выберите нужное исключение.
5. Выполните одно из следующих действий:
 - Установите флажок рядом с названием исключения из проверки, если вы хотите запустить работу этого исключения.
 - Снимите флажок рядом с названием исключения из проверки, если вы хотите временно приостановить работу этого исключения.
6. Сохраните внесенные изменения.

Формирование списка доверенных программ

► Чтобы сформировать список доверенных программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Исключения**.
3. В блоке **Исключения из проверки и доверенные программы** нажмите на кнопку **Настройка**.
Откроется окно **Доверенная зона**.
4. В окне **Доверенная зона** выберите закладку **Доверенные программы**.
5. Если вы хотите добавить программу в список доверенных программ, выполните следующие действия:

- a. Нажмите на кнопку **Добавить**.
- b. В раскрывшемся контекстном меню выполните одно из следующих действий:
 - Выберите пункт **Программы**, если вы хотите найти программу в списке установленных на компьютере программ.
Откроется окно **Выбор программы**.
 - Выберите пункт **Обзор**, если вы хотите указать путь к исполняемому файлу нужной программы.
Откроется стандартное окно Microsoft Windows **Открыть**.
- c. Выберите программу одним из следующих способов:
 - Если на предыдущем шаге вы выбрали пункт **Программы**, выберите программу в списке установленных на компьютере программ и нажмите на кнопку **ОК** в окне **Выбор программы**.
 - Если на предыдущем шаге вы выбрали пункт **Обзор**, укажите путь к исполняемому файлу нужной программы и нажмите на кнопку **Открыть** в стандартном окне Microsoft Windows **Открыть**.

В результате выполненных действий откроется окно **Исключения из проверки для программы**.

- d. Установите флажки напротив нужных правил доверенной зоны для выбранной программы:
 - **Не проверять открываемые файлы.**
 - **Не контролировать активность программы.**
 - **Не наследовать ограничения родительского процесса (программы).**
 - **Не контролировать активность дочерних программ.**
 - **Не блокировать взаимодействие с интерфейсом программы.**
 - **Не блокировать взаимодействие с Поставщиком AMSI-защиты.**
 - **Не проверять сетевой трафик.**
- e. Нажмите на кнопку **ОК** в окне **Исключения из проверки для программы**.
В списке доверенных программ появится добавленная доверенная программа.

6. Если вы хотите изменить параметры доверенной программы, выполните следующие действия:
 - a. Выберите доверенную программу из списка доверенных программ.
 - b. Нажмите на кнопку **Изменить**.
 - c. Откроется окно **Исключения из проверки для программы**.
 - d. Установите или снимите флажки напротив нужных правил доверенной зоны для выбранной программы.

Если в окне **Исключения из проверки для программы** не выбрано ни одно из правил доверенной зоны для программы, то происходит включение доверенной программы в проверку (см. раздел "Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ" на стр. 70). Доверенная программа не удаляется из списка доверенных программ, но флажок для нее снимается.

- e. Нажмите на кнопку **ОК** в окне **Исключения из проверки для программы**.
7. Если вы хотите удалить доверенную программу из списка доверенных программ, выполните следующие действия:
 - a. Выберите доверенную программу из списка доверенных программ.
 - b. Нажмите на кнопку **Удалить**.
8. Сохраните внесенные изменения.

Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ

► Чтобы включить или выключить действие правил доверенной зоны на программу из списка доверенных программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Исключения**.
3. В блоке **Исключения из проверки и доверенные программы** нажмите на кнопку **Настройка**.
Откроется окно **Доверенная зона**.
4. В окне **Доверенная зона** выберите закладку **Доверенные программы**.
5. В списке доверенных программ выберите нужную доверенную программу.
6. Выполните одно из следующих действий:
 - Установите флажок рядом с названием доверенной программы, если хотите выключить ее из проверки Kaspersky Endpoint Security.
 - Снимите флажок рядом с названием доверенной программы, если хотите включить ее в проверку Kaspersky Endpoint Security.
7. Сохраните внесенные изменения.

Использование доверенного системного хранилища сертификатов

Использование системного хранилища сертификатов позволяет исключать из антивирусной проверки программы, подписанные доверенной цифровой подписью.

► *Чтобы начать использовать доверенное системное хранилище сертификатов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Исключения**.
3. В блоке **Исключения из проверки и доверенные программы** нажмите на кнопку **Настройка**.
Откроется окно **Доверенная зона**.
4. В окне **Доверенная зона** выберите закладку **Доверенное системное хранилище сертификатов**.
5. Установите флажок **Использовать доверенное системное хранилище сертификатов**.
6. В раскрывающемся списке **Доверенное системное хранилище сертификатов** выберите, какое системное хранилище Kaspersky Endpoint Security должен считать доверенным.
7. Сохраните внесенные изменения.

Работа с активными угрозами

Программа Kaspersky Endpoint Security фиксирует информацию о файлах, которые она по каким-либо причинам не обработала. Эта информация записывается в виде событий в список активных угроз.

Зараженный файл считается *обработанным*, если Kaspersky Endpoint Security в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу, совершил одно из следующих действий с этим файлом согласно заданным настройкам программы:

- Лечить.
- Удалять.
- Удалять, если лечение невозможно.

Kaspersky Endpoint Security помещает файл в список активных угроз, если в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу, Kaspersky Endpoint Security по каким-либо причинам не совершил действие с этим файлом согласно заданным настройкам программы.

Такая ситуация возможна в следующих случаях:

- Проверяемый файл недоступен (например, находится на сетевом диске или внешнем диске без прав на запись данных).
- В настройках программы для задач проверки в блоке **Действие при обнаружении угрозы** выбрано действие **Информировать**, и когда на экране отобразилось уведомление о зараженном файле, пользователь выбрал вариант **Пропустить**.

Вы можете выполнить одно из следующих действий:

- Вручную запустить задачу выборочной проверки файлов из списка активных угроз после обновления баз и модулей программы. После проверки статус файлов может измениться.
- Удалить записи из списка активных угроз (см. раздел "Удаление записей из списка активных угроз" на стр. [73](#)).

В этом разделе

Работа со списком активных угроз	72
Запуск задачи выборочной проверки файлов из списка активных угроз	73
Удаление записей из списка активных угроз.....	73

Работа со списком активных угроз

Список активных угроз представлен в виде таблицы событий, связанных с зараженными файлами, которые по каким-либо причинам не были обработаны.

Вы можете выполнять следующие действия с файлами из списка активных угроз:

- просматривать список активных угроз;
- проверять из списка активных угроз, используя текущую версию баз и модулей Kaspersky Endpoint Security;

- восстанавливать файлы из списка активных угроз в исходные папки или в другую выбранную вами папку (в случае, если исходная папка размещения файла недоступна для записи);
- удалять файлы из списка активных угроз;
- открыть папку исходного размещения файла из списка активных угроз.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать активные угрозы по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска активных угроз;
- сортировать активные угрозы;
- изменять порядок и набор граф, отображаемых в списке активных угроз;
- группировать активные угрозы.

Если требуется, вы можете скопировать информацию о выбранных активных угрозах в буфер обмена.

Запуск задачи выборочной проверки файлов из списка активных угроз

Вы можете вручную запустить задачу выборочной проверки зараженных файлов, которые по каким-либо причинам не были обработаны. Проверку можно запустить, например, если по какой-либо причине последняя проверка была прервана или если вы хотите повторно проверить файлы из списка активных угроз после очередного обновления баз и модулей программы.

► *Чтобы запустить задачу выборочной проверки файлов из списка активных угроз, выполните следующие действия:*

1. В главном окне программы нажмите на блок **<...> активных угроз**.
Откроется окно **Активные угрозы**.
2. В таблице в окне **Активные угрозы** выберите одну или несколько записей, относящихся к файлам, которые вы хотите проверить.
Чтобы выбрать несколько записей, выделяйте их, удерживая клавишу **CTRL**.
3. Запустите задачу выборочной проверки файлов одним из следующих способов:
 - Нажмите на кнопку **Перепроверить**.
 - По правой клавише мыши откройте контекстное меню и выберите пункт **Перепроверить**.

Удаление записей из списка активных угроз

► *Чтобы удалить записи из списка активных угроз, выполните следующие действия:*

1. В главном окне программы нажмите на блок **<...> активных угроз**.
Откроется окно **Активные угрозы**.
2. В таблице в окне **Активные угрозы** выберите одну или несколько записей, которые вы хотите удалить из списка активных угроз.
Чтобы выбрать несколько записей, выделяйте их, удерживая клавишу **CTRL**.

3. Удалите записи одним из следующих способов:

- Нажмите на кнопку **Удалить**.
- По правой клавише мыши откройте контекстное меню и выберите пункт **Удалить**.

Обновление баз и модулей программы

В сертифицированной конфигурации не допускается загружать и устанавливать обновления модулей программы. Изменение модулей программы может привести к выходу из безопасного состояния.

Обновление баз и модулей программы Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули программы.

Для регулярного обновления требуется действующая лицензия на использование программы. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

Основным источником обновлений Kaspersky Endpoint Security служат серверы обновлений "Лаборатории Касперского".

Для успешной загрузки пакета обновлений с серверов обновлений "Лаборатории Касперского" компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, требуется настроить параметры прокси-сервера (см. раздел "Настройка использования прокси-сервера" на стр. [82](#)).

Загрузка обновлений осуществляется по протоколу HTTPS. Загрузка по протоколу HTTP может осуществляться в случае, когда загрузка обновлений по протоколу HTTPS невозможна.

В процессе обновления на ваш компьютер загружаются и устанавливаются следующие объекты:

- Базы Kaspersky Endpoint Security. Защита компьютера обеспечивается на основании баз данных, содержащих сигнатуры вирусов и других программ, представляющих угрозу, и информацию о способах борьбы с ними. Компоненты защиты используют эту информацию при поиске и обезвреживании зараженных файлов на компьютере. Базы регулярно пополняются записями о появляющихся угрозах и способах борьбы с ними. Поэтому рекомендуется регулярно обновлять базы.
Наряду с базами Kaspersky Endpoint Security обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.
- Модули программы. Помимо баз Kaspersky Endpoint Security, можно обновлять и модули программы. Обновления модулей программы устраняют уязвимости Kaspersky Endpoint Security, добавляют новые функции или улучшают существующие.

В процессе обновления базы и модули программы на вашем компьютере сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули программы отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Вместе с обновлением модулей программы может быть обновлена и контекстная справка программы.

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Информация о текущем состоянии баз Kaspersky Endpoint Security отображается в блоке **Обновление** в окне **Задачи**.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в отчет Kaspersky Endpoint Security (см. раздел "Работа с отчетами" на стр. [272](#)).

В этом разделе

Добавление источника обновлений	76
Выбор региона сервера обновлений	77
Настройка обновления из папки общего доступа	78
Выбор режима запуска для задачи обновления	79
Запуск задачи обновления с правами другого пользователя.....	80
Настройка обновления модулей программы.....	80
Запуск и остановка задачи обновления	81
Откат последнего обновления	82
Настройка использования прокси-сервера	82
Обновление антивирусных баз в ручном режиме	84
Устранение уязвимостей и установка критических обновлений в программе	85

Добавление источника обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей программы Kaspersky Endpoint Security.

Источником обновлений может быть FTP-, HTTP-сервер (например, Kaspersky Security Center, серверы обновлений "Лаборатории Касперского"), сетевая или локальная папка.

Если серверы обновлений "Лаборатории Касперского" вам недоступны (например, ограничен доступ в интернет), вы можете обратиться в центральный офис "Лаборатории Касперского" (<https://www.kaspersky.ru/about/contact>) и узнать адреса партнеров "Лаборатории Касперского". Партнеры "Лаборатории Касперского" предоставят вам обновления на съемном диске.

Заказывая обновления на съемном диске, вам следует уточнить, хотите ли вы получить обновления модулей программы.

По умолчанию список источников обновлений содержит сервер Kaspersky Security Center и серверы обновлений "Лаборатории Касперского". Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений можно указывать HTTP- или FTP-серверы, папки общего доступа.

Если в качестве источников обновлений выбрано несколько ресурсов, в процессе обновления Kaspersky Endpoint Security обращается к ним строго по списку и выполняет задачу обновления, используя пакет обновлений первого доступного источника обновлений.

► *Чтобы добавить источник обновлений, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Обновление**.
3. В блоке **Режим запуска и источник обновлений** нажмите на кнопку **Источник обновлений**.
4. На закладке **Источник** нажмите на кнопку **Добавить**.
5. В открывшемся окне укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, которая содержит пакет обновлений.

Формат пути для источника обновлений следующий:

- Для FTP- или HTTP-сервера введите веб-адрес или IP-адрес сайта.
Например, `http://dn1-01.geo.kaspersky.com/` или `93.191.13.103`.
Для FTP-сервера в адресе можно указывать параметры аутентификации в формате `ftp://<имя пользователя>:<пароль>@<узел>:<порт>`.
- Для сетевой папки введите UNC-путь.
Например, `\\Server\Share\Update distribution`.
- Для локальной папки введите полный путь к папке.
Например, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Сохраните внесенные изменения.

Выбор региона сервера обновлений

Если в качестве источника обновлений вы используете серверы "Лаборатории Касперского", вы можете выбрать местоположение сервера обновлений "Лаборатории Касперского" для загрузки пакета обновлений. Серверы обновлений "Лаборатории Касперского" расположены в нескольких странах мира. Использование географически ближайшего к вам сервера обновлений "Лаборатории Касперского" поможет сократить время получения пакета обновлений.

По умолчанию в параметрах обновления используется информация о текущем регионе из реестра операционной системы.

► *Чтобы выбрать регион сервера обновлений, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Обновление**.
3. В блоке **Режим запуска и источник обновлений** нажмите на кнопку **Источник обновлений**.

Откроется закладка **Источник** окна **Обновление**.

4. На закладке **Источник** в блоке **Региональные параметры** выберите **Выбрать из списка**.
5. В раскрывающемся списке выберите ближайшую к вашему текущему местонахождению страну.
6. Сохраните внесенные изменения.

Настройка обновления из папки общего доступа

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы на компьютерах локальной сети организации из папки общего доступа. Для этого один из компьютеров локальной сети организации должен получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или серверов обновлений "Лаборатории Касперского" и копировать полученный пакет обновлений в папку общего доступа. В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений из папки общего доступа.

Настройка обновления баз и модулей программы из папки общего доступа состоит из следующих этапов:

1. Включение режима копирования пакета обновлений в папку общего доступа на одном из компьютеров локальной сети организации.
2. Настройка обновления баз и модулей программы из указанной папки общего доступа на остальных компьютерах локальной сети организации.

► *Чтобы включить режим копирования пакета обновлений в папку общего доступа, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Обновление**.
3. В блоке **Дополнительно** установите флажок **Копировать обновления в папку**.
4. Введите UNC-путь к папке общего доступа (например, `\\Server\Share\Update distribution`).
5. Нажмите на кнопку **Сохранить**.

► *Чтобы настроить обновление из папки общего доступа, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Обновление**.
3. В блоке **Режим запуска и источник обновлений** нажмите на кнопку **Источник обновлений**.
4. На закладке **Источник** нажмите на кнопку **Добавить**.
5. В открывшемся окне укажите путь к папке общего доступа.

Адрес источника должен совпадать с адресом, указанным ранее при настройке режима копирования пакета обновлений в папку общего доступа (см. инструкцию выше).

6. Нажмите на кнопку **ОК**.
7. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.
8. Сохраните внесенные изменения.

Выбор режима запуска для задачи обновления

Если по каким-либо причинам запуск задачи обновления невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи обновления, как только это станет возможным.

Вы можете отложить запуск задачи обновления после старта программы для случаев, если вы выбрали режим запуска задачи обновления **По расписанию** и время запуска Kaspersky Endpoint Security совпадает с расписанием запуска задачи обновления. Задача обновления запускается только по истечении указанного времени после старта Kaspersky Endpoint Security.

► Чтобы выбрать режим запуска для задачи обновления, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Обновление**.
3. Нажмите на кнопку **Режим запуска**.
Откроется закладка **Режим запуска** окна **Обновление**.
4. В блоке **Режим запуска** выберите один из следующих вариантов режима запуска задачи обновления:
 - Выберите вариант **Автоматически**, если вы хотите, чтобы Kaspersky Endpoint Security запускал задачу обновления в зависимости от наличия пакета обновлений в источнике обновления. Частота проверки Kaspersky Endpoint Security наличия пакета обновлений увеличивается во время вирусных эпидемий и сокращается при их отсутствии.
 - Выберите вариант **Вручную**, если вы хотите запускать задачу обновления вручную.
 - Выберите вариант **По расписанию**, если вы хотите настроить расписание запуска задачи обновления.
5. Выполните одно из следующих действий:
 - Если вы выбрали вариант **Автоматически** или **Вручную**, перейдите к пункту 6 инструкции.
 - Если вы выбрали вариант **По расписанию**, задайте параметры расписания запуска задачи обновления. Для этого выполните следующие действия:
 - a. В раскрывающемся списке **Периодичность** укажите, когда следует запускать задачу обновления. Выберите один из следующих вариантов: **Минуты**, **Часы**, **Дни**, **Каждую неделю**, **В указанное время**, **Каждый месяц**, **После запуска программы**.
 - b. В зависимости от выбранного в раскрывающемся списке **Периодичность** элемента задайте значения параметров, которые уточняют время запуска задачи обновления.
 - c. В поле **Отложить запуск после старта программы на** укажите время, на которое следует отложить запуск задачи обновления после старта Kaspersky Endpoint Security.

Если в раскрывающемся списке **Периодичность** выбран элемент **После запуска программы**, поле **Отложить запуск после старта программы на** недоступно.
 - d. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенные вовремя задачи обновления.

Если в раскрывающемся списке **Периодичность** выбран элемент **Часы**, **Минуты** или **После запуска программы**, то флажок **Запускать пропущенные задачи** недоступен.
6. Сохраните внесенные изменения.

Запуск задачи обновления с правами другого пользователя

По умолчанию задача обновления Kaspersky Endpoint Security запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление Kaspersky Endpoint Security может производиться из источника обновления, к которому у пользователя нет прав доступа (например, из папки общего доступа, содержащей пакет обновлений) или для которого не настроено использование аутентификации на прокси-сервере. Вы можете указать пользователя, обладающего этими правами, в параметрах Kaspersky Endpoint Security и запускать задачу обновления Kaspersky Endpoint Security от имени этого пользователя.

► *Чтобы запускать задачу обновления с правами другого пользователя, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Обновление**.
3. В блоке **Режим запуска и источник обновлений** нажмите на кнопку **Режим запуска**.
Откроется закладка **Режим запуска** окна **Обновление**.
4. На закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами пользователя**.
5. В поле **Имя** введите имя учетной записи пользователя, права которого требуется использовать для доступа к источнику обновлений.
6. В поле **Пароль** введите пароль пользователя, права которого требуется использовать для доступа к источнику обновлений.
7. Сохраните внесенные изменения.

Настройка обновления модулей программы

► *Чтобы настроить обновление модулей программы, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Обновление**.
3. В блоке **Дополнительно** выполните одно из следующих действий:
 - Установите флажок **Загружать обновления модулей программы**, если вы хотите, чтобы программа включала обновления модулей программы в пакеты обновлений.
 - В противном случае снимите флажок **Загружать обновления модулей программы**.

4. Если на предыдущем шаге установлен флажок **Загружать обновления модулей программы**, укажите, при каких условиях программа будет устанавливать обновления модулей программы:
 - Выберите вариант **Устанавливать критические и одобренные обновления**, если вы хотите, чтобы программа устанавливала критические обновления модулей программы автоматически, а остальные обновления модулей программы – после одобрения их установки, локально через интерфейс программы или с помощью Kaspersky Security Center.
 - Выберите вариант **Устанавливать только одобренные обновления**, если вы хотите, чтобы программа устанавливала обновления модулей программы только после одобрения их установки, локально через интерфейс программы или с помощью Kaspersky Security Center.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск и остановка задачи обновления

Независимо от выбранного режима запуска задачи обновления вы можете запустить или остановить задачу обновления Kaspersky Endpoint Security в любой момент.

► *Чтобы запустить или остановить задачу обновления, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. По левой клавише мыши выберите блок с названием задачи обновления.
Раскроется выбранный блок.
3. Выполните одно из следующих действий:
 - Выберите в меню пункт **Запустить**, если вы хотите запустить задачу обновления.
Статус выполнения задачи, отображающийся под названием задачи обновления, изменится на *Выполняется*.
 - Выберите в меню пункт **Остановить**, если вы хотите остановить задачу обновления.
Статус выполнения задачи, отображающийся под названием задачи обновления, изменится на *Остановлена*.

► *Чтобы запустить или остановить задачу обновления при отображении упрощенного интерфейса программы (см. раздел "Упрощенный интерфейс программы" на стр. 46), выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:
 - выберите незапущенную задачу обновления, чтобы запустить ее;
 - выберите запущенную задачу обновления, чтобы остановить ее;
 - выберите остановленную задачу обновления, чтобы возобновить ее или запустить ее заново.

Откат последнего обновления

После первого обновления баз и модулей программы становится доступна функция отката к предыдущим базам и модулям программы.

Каждый раз, когда пользователь запускает обновление, Kaspersky Endpoint Security создает резервную копию используемых баз и модулей программы и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущих баз и модулей программы при необходимости. Возможность отката последнего обновления полезна, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

► *Чтобы откатить последнее обновление, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**, расположенную в нижней части главного окна программы.
Откроется окно **Задачи**.
2. По левой клавише мыши выберите блок с названием задачи отката обновления.
Раскроется выбранный блок.
3. Нажмите на кнопку **Запустить**.
Запустится задача отката обновления.
Статус выполнения задачи, отображающийся под названием задачи отката обновления, изменится на *Выполняется*.

► *Чтобы запустить или остановить задачу отката обновления при отображении упрощенного интерфейса программы (см. раздел "Упрощенный интерфейс программы" на стр. [46](#)), выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:
 - Выберите незапущенную задачу отката обновления, чтобы запустить ее.
 - Выберите запущенную задачу отката обновления, чтобы остановить ее.
 - Выберите остановленную задачу отката обновления, чтобы возобновить ее или запустить ее заново.

Настройка использования прокси-сервера

► *Чтобы настроить параметры прокси-сервера, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры сети**.
3. В блоке **Прокси-сервер** нажмите на кнопку **Настройка**.
Откроется окно **Параметры прокси-сервера**.
4. В окне **Параметры прокси-сервера** установите флажок **Использовать прокси-сервер**.

5. Выберите один из следующих вариантов определения адреса прокси-сервера:
 - **Автоматически определять адрес прокси-сервера.**
Этот вариант выбран по умолчанию.
 - **Использовать указанные адрес и порт прокси-сервера.**
6. Если вы выбрали вариант **Использовать указанные адрес и порт прокси-сервера**, укажите значения в полях **Адрес** и **Порт**.
7. Если вы хотите включить использование аутентификации на прокси-сервере, установите флажок **Задать имя пользователя и пароль для аутентификации** и укажите значения в следующих полях:
 - **Имя пользователя.**
Поле для ввода имени пользователя, которое используется при аутентификации на прокси-сервере.
 - **Пароль.**
Поле для ввода пароля пользователя, который используется при аутентификации на прокси-сервере.
8. Если вы хотите выключить использование прокси-сервера при обновлении баз и модулей программы из папки общего доступа (см. раздел "Настройка обновления из папки общего доступа" на стр. [78](#)), установите флажок **Не использовать прокси-сервер для локальных адресов**.
9. Сохраните внесенные изменения.

Обновление антивирусных баз в ручном режиме

Для обновления антивирусных баз, находящихся в изолированном сегменте сети, рекомендуется использовать следующий порядок действий:

1. В программе Kaspersky Security Center, находящейся в открытом сегменте сети, настроить задачу загрузки обновлений в хранилище.
2. Убедиться в том, что под управлением Kaspersky Security Center в открытом сегменте есть управляемые машины с установленными программами, базы для которых необходимо обновить.
3. Запустить задачу. В процессе загрузки обновлений с открытых серверов «Лаборатории Касперского» Kaspersky Security Center проведет проверку контроля целостности обновлений, прежде чем добавит их в свое хранилище.
4. Удобным вам способом перенесите содержимое хранилища Kaspersky Security Center в изолированный сегмент сети.

Запустите на средствах антивирусной защиты внутри изолированного сегмента сети задачу обновления с указанием перенесенного хранилища как источника обновлений. При загрузке обновлений из хранилища, программы еще раз проведут контроль целостности загружаемых обновлений.

Если вам недоступны серверы обновлений "Лаборатории Касперского" (например, нет доступа к интернету), обратитесь в Службу технической поддержки "Лаборатории Касперского" для получения обновлений программы на дисках.

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программного обеспечения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (<https://support.kaspersky.ru/general/certificates>) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: <http://support.kaspersky.ru/subscribe>). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (<http://www.bdu.fstec.ru>, <https://support.kaspersky.ru/vulnerability>).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (<https://support.kaspersky.ru/vulnerability.aspx?el=12429>).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (<https://community.kaspersky.com/>).

Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

В зависимости от расположения инфраструктуры различают Глобальный KSN (инфраструктура расположена на серверах "Лаборатории Касперского") и Локальный KSN.

В сертифицированной версии программы Kaspersky Endpoint Security используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается.

Участие пользователей в KSN позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках угроз, разрабатывать способы нейтрализации угроз, уменьшать количество ложных срабатываний компонентов программы.

При использовании расширенного режима KSN программа автоматически отправляет в KSN статистическую информацию, полученную в результате своей работы. Также программа может отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или части файлов), которые злоумышленники могут использовать для нанесения вреда компьютеру или данным.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского" (<https://www.kaspersky.ru/products-and-services-privacy-policy>). Файл ksn_<ID языка>.txt с текстом Положения о Kaspersky Security Network входит в комплект поставки программы. Для снижения нагрузки на серверы KSN специалисты "Лаборатории Касперского" могут выпускать антивирусные базы программы, которые временно выключают или частично ограничивают обращения в Kaspersky Security Network. В этом случае статус подключения к KSN – *Включено с ограничениями* (см. раздел "Проверка подключения к Kaspersky Security Network" на стр. 88).

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.
- Служба KSN Proxy кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение компьютером пользователя запрошенной информации.

Подробнее о службе KSN Proxy вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Настройка параметров использования службы KSN Proxy доступна в свойствах политики *Kaspersky Security Center* (см. раздел "*Управление политиками*" на стр. [39](#)).

Использование Kaspersky Security Network является добровольным. Программа предлагает использовать KSN во время первоначальной настройки программы. Начать или прекратить использование KSN можно в любой момент.

В этом разделе

Включение и выключение использования Kaspersky Security Network.....	87
Включение и выключение облачного режима для компонентов защиты	88
Проверка подключения к Kaspersky Security Network.....	88
Проверка репутации файла в Kaspersky Security Network	90

Включение и выключение использования Kaspersky Security Network

► *Чтобы включить или выключить использование Kaspersky Security Network, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Kaspersky Security Network**.
3. Выполните одно из следующих действий:
 - Установите флажок **Kaspersky Security Network**, если вы хотите, чтобы в работе компонентов Kaspersky Endpoint Security использовалась информация о репутации файлов, веб-ресурсов и программ, полученная из баз Kaspersky Security Network.

Для настройки расширенного использования Kaspersky Security Network в работе Kaspersky Endpoint Security выполните следующие действия:

- Установите флажок **Включить расширенный режим KSN**, если вы хотите, чтобы Kaspersky Endpoint Security отправлял на сервер Kaspersky Security Network статистическую информацию, полученную в результате своей работы, а также мог отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или части файлов), которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным.
 - Снимите флажок **Включить расширенный режим KSN**, если вы хотите, чтобы Kaspersky Endpoint Security использовал базовые функции Kaspersky Security Network.
 - Снимите флажок **Kaspersky Security Network**, если вы хотите выключить использование Kaspersky Security Network.
4. Сохраните внесенные изменения.

Включение и выключение облачного режима для компонентов защиты

При использовании Kaspersky Private Security Network функциональность облачного режима доступна начиная с версии Kaspersky Private Security Network 3.0.

► Чтобы включить или выключить облачный режим для компонентов защиты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Kaspersky Security Network**.
3. Выполните одно из следующих действий:

- Установите флажок **Включить облачный режим для компонентов защиты**.

Если флажок установлен, то Kaspersky Endpoint Security использует облегченную версию антивирусных баз, за счет чего снижается нагрузка на ресурсы операционной системы.

Kaspersky Endpoint Security загружает облегченную версию антивирусных баз в ходе ближайшего обновления после того, как флажок был установлен. Если облегченная версия антивирусных баз недоступна для использования, Kaspersky Endpoint Security автоматически переключается на использование полной версии антивирусных баз.

- Снимите флажок **Включить облачный режим для компонентов защиты**.

Если флажок снят, то Kaspersky Endpoint Security использует полную версию антивирусных баз.

Kaspersky Endpoint Security загружает полную версию антивирусных баз в ходе ближайшего обновления после того, как флажок был снят.

Флажок доступен, если установлен флажок **Kaspersky Security Network**.

4. Сохраните внесенные изменения.

Проверка подключения к Kaspersky Security Network

► Чтобы проверить подключение к Kaspersky Security Network, выполните следующие действия:

1. В главном окне программы нажмите на блок **Технологии обнаружения угроз**.

В нижней части окна **Технологии обнаружения угроз** отображается следующая информация о работе Kaspersky Security Network:

- Под строкой **Kaspersky Security Network (KSN)** отображается один из следующих статусов подключения Kaspersky Endpoint Security к Kaspersky Security Network:
 - *Включено. Доступно.*
Статус означает, что Kaspersky Security Network используется в работе Kaspersky Endpoint Security и серверы KSN доступны.
 - *Включено. Недоступно.*
Статус означает, что Kaspersky Security Network используется в работе Kaspersky Endpoint Security и серверы KSN недоступны.
 - *Отключено.*
Статус означает, что Kaspersky Security Network не используется в работе Kaspersky Endpoint Security.
- В строках **Безопасных объектов**, **Опасных объектов**, **Нейтрализованных угроз за сутки** отображается глобальная статистика инфраструктуры облачных служб Kaspersky Security Network.
- В строке **Последняя синхронизация** отображается дата и время последней синхронизации Kaspersky Endpoint Security с серверами KSN.

Получение статистических данных по использованию KSN программа производит при открытии окна **Технологии обнаружения угроз**. Обновление глобальной статистики инфраструктуры облачных служб Kaspersky Security Network, а также строки **Последняя синхронизация** в реальном времени не производится. Если время, прошедшее после последней синхронизации с серверами KSN, превышает 15 минут или отображается статус *Неизвестно*, то статус подключения Kaspersky Endpoint Security к Kaspersky Security Network принимает значение *Включено. Недоступно*.

Связь с серверами Kaspersky Security Network может отсутствовать по следующим причинам:

- Ваш компьютер не подключен к интернету.
- Программа не активирована.
- Срок действия лицензии истек.
- Выявлены проблемы, связанные с лицензионным ключом (например, ключ попал в черный список ключей).

Если восстановить связь с серверами Kaspersky Security Network не удастся, то рекомендуется обратиться в Службу технической поддержки или к поставщику услуг.

Проверка репутации файла в Kaspersky Security Network

Если вы сомневаетесь в безопасности файла, вы можете проверить его репутацию в Kaspersky Security Network.

Проверка репутации файла доступна, если вы приняли условия Положения о Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 87).

► Чтобы проверить репутацию файла в Kaspersky Security Network,

откройте контекстное меню файла и выберите пункт **Проверить репутацию в KSN** (см. рис. ниже).

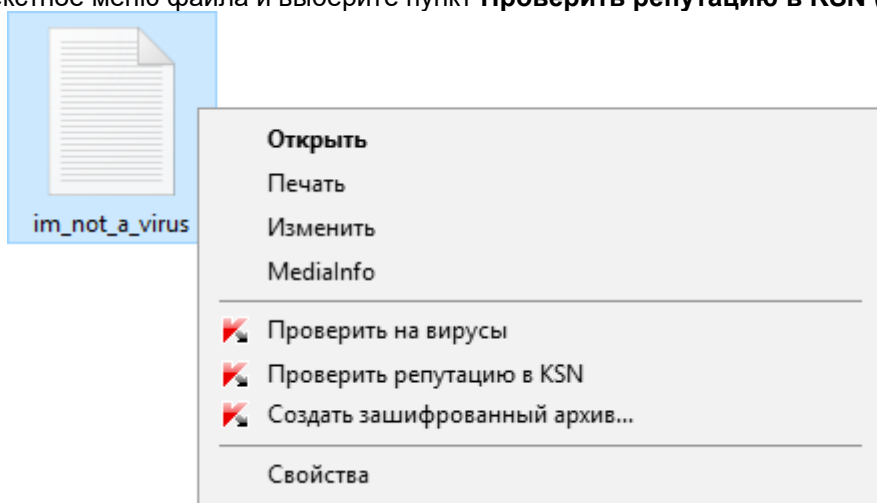


Рисунок 8. Контекстное меню файла

Kaspersky Endpoint Security отображает репутацию файла:



Доверенный. Большинство пользователей Kaspersky Security Network подтвердили, что файл доверенный.



Легальная программа, которая может быть использована для нанесения вреда компьютеру или данным. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы злоумышленниками. Подробную информацию о легальных программах, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского" <https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/>. Вы можете добавить эти программы в список доверенных (см. раздел "Формирование списка доверенных программ" на стр. 69).



Недоверенный. Вирус или другая программа, представляющая угрозу (см. раздел "Работа с активными угрозами" на стр. 63).



Неизвестный. В Kaspersky Security Network отсутствует информация о файле. Вы можете проверить файл с помощью антивирусных баз (пункт контекстного меню **Проверить на вирусы**).

Kaspersky Endpoint Security отображает решение KSN, которое было использовано для определения репутации файла: *Глобальный KSN* или *Локальный KSN*.

Также Kaspersky Endpoint Security отображает дополнительную информацию о файле (см. рис. ниже).

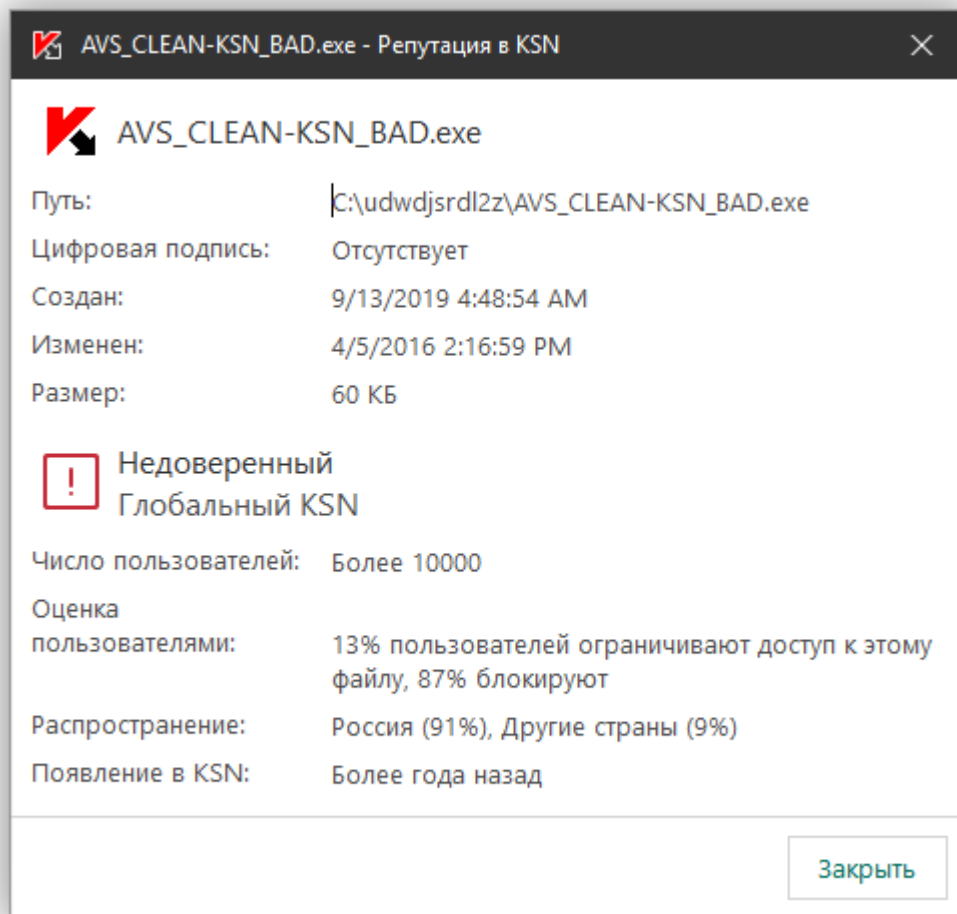


Рисунок 9. Репутация файла в Kaspersky Security Network

Анализ поведения

Компонент Анализ поведения получает данные о действиях программ на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы.

Компонент Анализ поведения использует шаблоны опасного поведения программ. Если активность программы совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security выполняет выбранное ответное действие. Функциональность Kaspersky Endpoint Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

В этом разделе

Включение и выключение Анализа поведения	92
Выбор действия при обнаружении вредоносной активности программы	93
Защита папок общего доступа от внешнего шифрования	93

Включение и выключение Анализа поведения

По умолчанию Анализ поведения включен и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". Вы можете выключить Анализ поведения при необходимости.

Не рекомендуется выключать Анализ поведения без необходимости, так как это снижает эффективность работы компонентов защиты. Компоненты защиты могут запрашивать данные, полученные компонентом Анализ поведения, для обнаружения угроз.

► Чтобы включить или выключить Анализ поведения, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Анализ поведения**.
3. Выполните одно из следующих действий:
 - Установите флажок **Анализ поведения**, если вы хотите, чтобы Kaspersky Endpoint Security анализировал активность программ в операционной системе, используя шаблоны опасного поведения.
 - Снимите флажок **Анализ поведения**, если вы не хотите, чтобы Kaspersky Endpoint Security анализировал активность программ в операционной системе, используя шаблоны опасного поведения.
4. Сохраните внесенные изменения.

Выбор действия при обнаружении вредоносной активности программы

► Чтобы выбрать действие при обнаружении вредоносной активности программы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Анализ поведения**.
3. В раскрывающемся списке **При обнаружении вредоносной активности программы** выберите нужное действие:

- **Удалять файл.**

Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security удаляет исполняемый файл вредоносной программы и создает резервную копию файла в резервном хранилище.

- **Завершать работу программы.**

Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security завершает работу этой программы.

- **Информировать.**

Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security добавляет информацию о вредоносной активности этой программы в список активных угроз.

4. Сохраните внесенные изменения.

Защита папок общего доступа от внешнего шифрования

Компонент обеспечивает отслеживание операций только над теми файлами, которые расположены на запоминающих устройствах с файловой системой NTFS и не зашифрованы системой EFS.

Функция защиты папок общего доступа от внешнего шифрования обеспечивает анализ активности в папках общего доступа. Если активность совпадает с одним из шаблонов поведения, характерного для внешнего шифрования, Kaspersky Endpoint Security выполняет выбранное действие.

По умолчанию защита папок общего доступа от внешнего шифрования выключена.

После установки Kaspersky Endpoint Security функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

В этом разделе

Включение и выключение защиты папок общего доступа от внешнего шифрования	94
Выбор действия при обнаружении внешнего шифрования папок общего доступа	94
Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования	95

Включение и выключение защиты папок общего доступа от внешнего шифрования

После установки Kaspersky Endpoint Security функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

► Чтобы включить или выключить защиту папок общего доступа от внешнего шифрования, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Анализ поведения**.
3. В блоке **Защита папок общего доступа от внешнего шифрования** выполните одно из следующих действий:
 - Установите флажок **Включить защиту папок общего доступа от внешнего шифрования**, если вы хотите, чтобы программа Kaspersky Endpoint Security анализировала активность, характерную для внешнего шифрования.
 - Снимите флажок **Включить защиту папок общего доступа от внешнего шифрования**, если вы не хотите, чтобы программа Kaspersky Endpoint Security анализировала активность, характерную для внешнего шифрования.
4. Сохраните внесенные изменения.

Выбор действия при обнаружении внешнего шифрования папок общего доступа

► Чтобы выбрать действие при обнаружении внешнего шифрования папок общего доступа, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Анализ поведения**.
3. В блоке **Защита папок общего доступа от внешнего шифрования** в раскрывающемся списке **При обнаружении внешнего шифрования папок общего доступа** выберите нужное действие:
 - **Блокировать соединение.**

Если выбран этот вариант, то при обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security выполняет следующие действия:

 - блокирует сетевую активность компьютера, осуществляющего изменение;
 - создает резервные копии подверженных изменению файлов;

- добавляет запись в отчеты локального интерфейса программы (см. раздел "Работа с отчетами" на стр. [272](#));
- отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.

Если при этом включен компонент Откат вредоносных действий (см. раздел "Включение и выключение Отката вредоносных действий" на стр. [114](#)), то выполняется восстановление измененных файлов из резервных копий.

Если вы выбрали элемент **Блокировать соединение**, то вы можете указать время в минутах, на которое будет заблокировано сетевое соединение, в поле **Блокировать соединение на N минут**.

- **Информировать.**

Если выбран этот вариант, то при обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security добавляет запись в отчеты локального интерфейса программы (см. раздел "Работа с отчетами" на стр. [272](#)), добавляет запись в список активных угроз (см. раздел "Работа со списком активных угроз" на стр. [72](#)) и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.

4. Сохраните внесенные изменения.

Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования

Для работы функциональности исключений адресов из защиты папок общего доступа от внешнего шифрования необходимо включить службу Аудит входа в систему. По умолчанию служба Аудит входа в систему выключена (подробную информацию о включении службы Аудит входа в систему см. на сайте корпорации Microsoft).

Функциональность исключений адресов из защиты папок общего доступа не работает на удаленном компьютере, если этот удаленный компьютер был включен до запуска Kaspersky Endpoint Security. Вы можете перезагрузить этот удаленный компьютер после запуска Kaspersky Endpoint Security, чтобы обеспечить работу функциональности исключений адресов из защиты папок общего доступа на этом удаленном компьютере.

► *Чтобы исключить из защиты удаленные компьютеры, осуществляющие внешнее шифрование папок общего доступа, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Анализ поведения**.
3. В блоке **Защита папок общего доступа от внешнего шифрования** нажмите на кнопку **Исключения**.

Откроется окно **Исключения**.

4. Выполните одно из следующих действий:

- Если вы хотите добавить IP-адрес или имя компьютера в список исключений, нажмите на кнопку **Добавить**.
- Если вы хотите изменить IP-адрес или имя компьютера, выберите его в списке исключений и нажмите на кнопку **Изменить**.

Откроется окно **Компьютер**.

5. Введите IP-адрес компьютера или имя компьютера, попытки внешнего шифрования с которого не должны обрабатываться.
6. Сохраните внесенные изменения.

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимую программу. При обработке этих данных уязвимая программа выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО.

Если попытка запустить исполняемый файл из уязвимой программы не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя.

В этом разделе

Включение и выключение Защиты от эксплойтов	97
Выбор действия при обнаружении эксплойта	97
Включение и выключение защиты памяти системных процессов	98

Включение и выключение Защиты от эксплойтов

По умолчанию Защита от эксплойтов включена и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". Вы можете выключить Защиту от эксплойтов при необходимости.

► *Чтобы включить или выключить Защиту от эксплойтов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Защита от эксплойтов**.
3. Выполните одно из следующих действий:
 - Установите флажок **Защита от эксплойтов**, если вы хотите, чтобы Kaspersky Endpoint Security отслеживал исполняемые файлы, запускаемые уязвимыми программами.
Если Kaspersky Endpoint Security обнаруживает, что исполняемый файл из уязвимой программы был запущен не пользователем, то Kaspersky Endpoint Security выполняет действие, выбранное в раскрывающемся списке **При обнаружении эксплойта**.
 - Снимите флажок **Защита от эксплойтов**, если вы не хотите, чтобы Kaspersky Endpoint Security отслеживал исполняемые файлы, запускаемые уязвимыми программами.
4. Сохраните внесенные изменения.

Выбор действия при обнаружении эксплойта

По умолчанию, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта.

► *Чтобы выбрать действие при обнаружении эксплойта, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Защита от эксплойтов**.
3. В раскрывающемся списке **При обнаружении эксплойта** выберите нужное действие:
 - **Блокировать операцию.**
Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта и создает в журнале запись, содержащую информацию об этом эксплойте.
 - **Информировать.**
Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security создает в журнале запись, содержащую информацию об этом эксплойте, и добавляет информацию об этом эксплойте в список активных угроз.
4. Сохраните внесенные изменения.

Включение и выключение защиты памяти системных процессов

По умолчанию защита памяти системных процессов включена.

► *Чтобы включить или выключить защиту памяти системных процессов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Защита от эксплойтов**.
3. Выполните одно из следующих действий:
 - В блоке **Защита памяти системных процессов** установите флажок **Включить защиту памяти системных процессов**, если вы хотите, чтобы Kaspersky Endpoint Security блокировал сторонние процессы, осуществляющие попытки доступа к системным процессам.
 - В блоке **Защита памяти системных процессов** снимите флажок **Включить защиту памяти системных процессов**, если вы не хотите, чтобы Kaspersky Endpoint Security блокировал сторонние процессы, осуществляющие попытки доступа к системным процессам.
4. Сохраните внесенные изменения.

Предотвращение вторжений

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Предотвращение вторжений (англ. HIPS – Host Intrusion Prevention System) предотвращает выполнение программами опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным. Компонент обеспечивает защиту компьютера с помощью антивирусных баз и облачной службы Kaspersky Security Network.

Компонент контролирует работу программ с помощью *прав программ*. Права программ включают в себя следующие параметры доступа:

- доступ к ресурсам операционной системы (например, параметры автозапуска, ключи реестра);
- доступ к персональным данным (например, к файлам, программам).

Сетевую активность программ контролирует Сетевой экран с помощью *сетевых правил*.

Во время первого запуска программы компонент Предотвращение вторжений выполняет следующие действия:

1. Проверяет безопасность программы с помощью загруженных антивирусных баз.
2. Проверяет безопасность программы в Kaspersky Security Network.

Для более эффективной работы компонента Предотвращение вторжений вам рекомендуется принять участие в Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. [87](#)).

3. Помещает программу в одну из *групп доверия*: Доверенные, Слабые ограничения, Сильные ограничения, Недоверенные.

Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля сетевой активности программ. Kaspersky Endpoint Security помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

Kaspersky Endpoint Security помещает программу в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security помещает программу в группу доверия в зависимости от параметров компонента Предотвращение вторжений (см. раздел "Настройка параметров распределения программ по группам доверия" на стр. 103). После получения данных о репутации программы от KSN группа доверия может быть изменена автоматически.

4. Блокирует действия программы в зависимости от группы доверия. Например, программам из группы доверия "Сильные ограничения" запрещен доступ к модулям операционной системы.

При следующем запуске программы Kaspersky Endpoint Security проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие права программ. Если программа была изменена, Kaspersky Endpoint Security исследует программу как при первом запуске.

В этом разделе

Ограничения контроля аудио и видео устройств	100
Включение и выключение Предотвращения вторжений	101
Работа с группами доверия программ	102
Работа с правами программ	105
Защита ресурсов операционной системы и персональных данных	110

Ограничения контроля аудио и видео устройств

О защите аудиосигнала

Функциональность защиты аудиосигнала имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Предотвращение вторжений.
- Если программа начала получать аудиосигнал до запуска компонента Предотвращение вторжений, то Kaspersky Endpoint Security разрешает программе получение аудиосигнала и не показывает никаких уведомлений.
- Если вы поместили программу в группу **Недоверенные** или **Сильные ограничения** после того, как программа начала получать аудиосигнал, то Kaspersky Endpoint Security разрешает программе получение аудиосигнала и не показывает никаких уведомлений.
- При изменении параметров доступа программы к устройствам записи звука (например, программе было запрещено получение аудиосигнала в окне параметров Предотвращение вторжений) требуется перезапуск этой программы, чтобы она перестала получать аудиосигнал.
- Контроль получения аудиосигнала с устройств записи звука не зависит от параметров доступа программ к веб-камере.
- Kaspersky Endpoint Security защищает доступ только к встроенным и внешним микрофонам. Другие устройства передачи звука не поддерживаются.
- Kaspersky Endpoint Security не гарантирует защиту аудиосигнала, передаваемого с таких устройств, как DSLR-камеры, портативные видеокамеры, экшн-камеры.

Особенности работы аудио и видео устройств во время установки и обновления Kaspersky Endpoint Security

При первом запуске программы Kaspersky Endpoint Security с момента ее установки воспроизведение или запись аудио и видео могут быть прерваны в программах записи или воспроизведения аудио и видео. Это необходимо для того, чтобы включилась функциональность контроля доступа программ к устройствам записи звука. Системная служба управления средствами работы со звуком будет перезапущена при первом запуске программы Kaspersky Endpoint Security.

О доступе программ к веб-камерам

Функциональность защиты доступа к веб-камере имеет следующие особенности и ограничения:

- Программа контролирует видео и статические изображения, полученные в результате обработки данных веб-камеры.
- Программа контролирует аудиосигнал, если он является частью видеопотока, получаемого с веб-камеры.
- Программа контролирует только веб-камеры, подключаемые по интерфейсу USB или IEEE1394 и отображаемые в Диспетчере устройств Windows как **Устройства обработки изображений** (Imaging Device).

Поддерживаемые веб-камеры

Kaspersky Endpoint Security поддерживает следующие веб-камеры:

- Logitech HD Webcam C270;
- Logitech HD Webcam C310;
- Logitech Webcam C210;
- Logitech Webcam Pro 9000;
- Logitech HD Webcam C525;
- Microsoft LifeCam VX-1000;
- Microsoft LifeCam VX-2000;
- Microsoft LifeCam VX-3000;
- Microsoft LifeCam VX-800;
- Microsoft LifeCam Cinema.

"Лаборатория Касперского" не гарантирует поддержку веб-камер, не указанных в этом списке.

Включение и выключение Предотвращения вторжений

По умолчанию компонент Предотвращение вторжений включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить компонент Предотвращение вторжений при необходимости.

► *Чтобы включить или выключить компонент Предотвращение вторжений выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. В правой части окна выполните одно из следующих действий:
 - Установите флажок **Предотвращение вторжений**, если вы хотите включить компонент Предотвращение вторжений.
 - Снимите флажок **Предотвращение вторжений**, если вы хотите выключить компонент Предотвращение вторжений.
4. Сохраните внесенные изменения.

Работа с группами доверия программ

Во время первого запуска каждой программы компонент Предотвращение вторжений проверяет безопасность программы и помещает программу в одну из групп доверия.

Вы можете выбрать группу доверия, в которую Kaspersky Endpoint Security должен автоматически помещать все неизвестные программы. Программы, которые были запущены до Kaspersky Endpoint Security, автоматически помещаются в группу доверия, указанную в окне **Выбор группы доверия** (см. раздел "**Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security**" на стр. [105](#)).

Существуют следующие группы доверия:

- **Доверенные.** В группу входят программы, для которых выполняется одно или более следующих условий:
 - программы обладают цифровой подписью доверенных производителей;
 - о программах есть записи в базе доверенных программ Kaspersky Security Network;
 - пользователь поместил программы в группу "Доверенные".Запрещенных операций для таких программ нет.
- **Слабые ограничения.** В группу входят программы, для которых выполняются следующие условия:
 - программы не обладают цифровой подписью доверенных производителей;
 - о программах нет записей в базе доверенных программ Kaspersky Security Network;
 - пользователь поместил программы в группу "Слабые ограничения".

Такие программы имеют минимальные ограничения на работу с ресурсами операционной системы.

- **Сильные ограничения.** В группу входят программы, для которых выполняются следующие условия:

- программы не обладают цифровой подписью доверенных производителей;
- о программах нет записей в базе доверенных программ Kaspersky Security Network;
- пользователь поместил программы в группу "Сильные ограничения".

Такие программы имеют значительные ограничения на работу с ресурсами операционной системы.

- **Недоверенные.** В группу входят программы, для которых выполняются следующие условия:

- программы не обладают цифровой подписью доверенных производителей;
- о программах нет записей в базе доверенных программ Kaspersky Security Network;
- пользователь поместил программы в группу "Недоверенные".

Такие программы имеют значительные ограничения на работу с ресурсами операционной системы.

На первом этапе проверки программы Kaspersky Endpoint Security ищет запись о программе во внутренней базе известных программ и одновременно отправляет запрос в базу Kaspersky Security Network (при наличии подключения к интернету). По результатам проверки по внутренней базе и по базе Kaspersky Security Network программа помещается в группу доверия. При каждом повторном запуске программы Kaspersky Endpoint Security отправляет новый запрос в базу KSN и перемещает программу в другую группу доверия, если репутация программы в базе KSN изменилась.

Вы можете выбрать группу доверия, в которую Kaspersky Endpoint Security должен автоматически помещать все неизвестные программы. Программы, которые были запущены до Kaspersky Endpoint Security, автоматически помещаются в группу доверия, указанную в окне **Выбор группы доверия** (см. раздел **"Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security"** на стр. [105](#)).

Для программ, запущенных до Kaspersky Endpoint Security, контролируется только сетевая активность. Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана.

В этом разделе

Настройка параметров распределения программ по группам доверия	103
Изменение группы доверия	104
Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security	105

Настройка параметров распределения программ по группам доверия

Если участие в Kaspersky Security Network включено, Kaspersky Endpoint Security отправляет запрос о репутации программы в KSN при каждом запуске программы. На основе полученного ответа программа может быть перемещена в группу доверия, отличную от заданной в параметрах компонента Предотвращение вторжений.

Kaspersky Endpoint Security всегда помещает программы, подписанные сертификатами Microsoft или сертификатами "Лаборатории Касперского", в группу доверия "Доверенные".

► Чтобы настроить параметры распределения программ по группам доверия, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. Если вы хотите автоматически помещать программы с цифровой подписью в группу доверия "Доверенные", установите флажок **Доверять программам, имеющим цифровую подпись**.
4. Чтобы помещать все неизвестные программы в указанную группу доверия, выберите нужную группу доверия из раскрывающегося списка **Программы, для которых не удалось определить группу доверия, автоматически помещать в**.

В целях безопасности группа **Доверенные** не включена в значения параметра **Программы, для которых не удалось определить группу доверия, автоматически помещать в**.

5. Сохраните внесенные изменения.

Изменение группы доверия

Во время первого запуска программы Kaspersky Endpoint Security автоматически помещает программу в ту или иную группу доверия. При необходимости вы можете вручную переместить программу в другую группу доверия.

Специалисты "Лаборатории Касперского" не рекомендуют перемещать программы из группы доверия, определенной автоматически, в другую группу доверия. Вместо этого при необходимости измените права отдельной программы (см. раздел "Изменение прав программы" на стр. 107).

► Чтобы изменить группу доверия, в которую Kaspersky Endpoint Security автоматически поместил программу при первом ее запуске, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.

3. Нажмите на кнопку **Программы**.
Откроется закладка **Права программ** окна **Предотвращение вторжений**.
4. На закладке **Права программ** выберите нужную программу.
5. Выполните одно из следующих действий:
 - По правой клавише мыши откройте контекстное меню программы. В контекстном меню программы выберите пункт **Переместить в группу** → <название группы>.
 - По ссылке **Доверенные / Слабые ограничения / Сильные ограничения / Недоверенные** откройте контекстное меню. В контекстном меню выберите нужную группу доверия.
6. Сохраните внесенные изменения.

Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security

Для программ, запущенных до Kaspersky Endpoint Security, контролируется только сетевая активность. Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана. Чтобы указать, какими сетевыми правилами должен регулироваться контроль сетевой активности таких программ, необходимо выбрать группу доверия.

- Чтобы выбрать группу доверия для программ, запускаемых до Kaspersky Endpoint Security, выполните следующие действия:
1. В главном окне программы нажмите на кнопку **Настройка**.
 2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
 3. Нажмите на кнопку **Изменить**.
Откроется окно **Выбор группы доверия**.
 4. Выберите нужную группу доверия.
 5. Сохраните внесенные изменения.

Работа с правами программ

По умолчанию для контроля работы программы применяются права программ, определенные для той группы доверия, в которую Kaspersky Endpoint Security поместил программу при первом ее запуске. При необходимости вы можете изменить права программ для всей группы доверия, для отдельной программы или группы программ внутри группы доверия.

Права программ, определенные для отдельных программ или групп программ внутри группы доверия, имеют более высокий приоритет, чем права программ, определенные для группы доверия. То есть, если параметры прав программ, определенные для отдельной программы или группы программ внутри группы доверия, отличны от параметров прав программ, определенных для группы доверия, то компонент Предотвращение вторжений контролирует работу программы или группы программ внутри группы доверия в соответствии с правами программ, определенными для программы или группы программ.

В этом разделе

Изменение прав программ для групп доверия и для групп программ	106
Изменение прав программы	107
Выключение загрузки и обновления прав программ из базы Kaspersky Security Network	108
Выключение наследования ограничений родительского процесса	108
Исключение некоторых действий программ из прав программ	109
Удаление информации о неиспользуемых программах	109

Изменение прав программ для групп доверия и для групп программ

По умолчанию для разных групп доверия созданы оптимальные права программ. Параметры прав групп программ, входящих в группу доверия, наследуют значения параметров прав групп доверия. Вы можете изменить предустановленные права групп доверия и права групп программ.

► *Чтобы изменить права группы доверия или права группы программ, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Программы**.
Откроется закладка **Права программ** окна **Предотвращение вторжений**.
4. Выберите нужную группу доверия или группу программ.
5. В контекстном меню группы доверия или группы программ выберите пункт **Права группы**.
Откроется окно **Права группы программ**.
6. В окне **Права группы программ** выполните одно из следующих действий:
 - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия или права группы программ, регулирующие права группы доверия или группы программ на операции с реестром операционной системы, файлами пользователя и параметрами программ.
 - Выберите закладку **Права**, если вы хотите изменить права группы доверия или права группы программ, регулирующие права группы доверия или группы программ на доступ к процессам и объектам операционной системы.
7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню.
8. В контекстном меню выберите нужный пункт:
 - **Наследовать**.
 - **Разрешать**.

- **Запрещать.**
- **Записывать в отчет.**

Если вы изменяете правила контроля группы доверия, то пункт **Наследовать** недоступен для выбора.

9. Сохраните внесенные изменения.

Изменение прав программы

По умолчанию параметры прав программ, входящих в группу программ или в группу доверия, наследуют значения параметров прав группы доверия. Вы можете изменить параметры прав программ.

► *Чтобы изменить права программы, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Программы**.
Откроется закладка **Права программ** окна **Предотвращение вторжений**.
4. Выберите нужную программу.
5. Выполните одно из следующих действий:
 - В контекстном меню программы выберите пункт **Права программы**.
 - Нажмите на кнопку **Дополнительно** в правом нижнем углу закладки **Права программ**.
Откроется окно **Права программы**.
6. В окне **Права программы** выполните одно из следующих действий:
 - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить права программы, регулирующие права программы на операции с реестром операционной системы, файлами пользователя и параметрами программ.
 - Выберите закладку **Права**, если вы хотите изменить права программы, регулирующие права программы на доступ к процессам и объектам операционной системы.
7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню.
8. В контекстном меню выберите нужный пункт:
 - **Наследовать.**
 - **Разрешать.**
 - **Запрещать.**
 - **Записывать в отчет.**
9. Сохраните внесенные изменения.

Выключение загрузки и обновления прав программ из базы Kaspersky Security Network

По умолчанию при обнаружении в базе Kaspersky Security Network новой информации о программе Kaspersky Endpoint Security применяется для этой программы права, загруженные из базы KSN. После этого вы можете изменить права программы вручную.

Если на момент первого своего запуска программа отсутствовала в базе Kaspersky Security Network, но затем информация о ней была добавлена в базу Kaspersky Security Network, то по умолчанию Kaspersky Endpoint Security автоматически обновляет права этой программы.

Вы можете выключить загрузку прав программ из базы Kaspersky Security Network и автоматическое обновление прав ранее неизвестных программ.

► *Чтобы выключить загрузку и обновление прав программ из базы Kaspersky Security Network, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. Снимите флажок **Обновлять права для ранее неизвестных программ из базы KSN**.
4. Сохраните внесенные изменения.

Выключение наследования ограничений родительского процесса

Инициатором запуска программы может быть как пользователь, так и другая запущенная программа. Если инициатором запуска программы является другая программа, образуется последовательность запуска, состоящая из родительских и дочерних процессов.

Когда программа пытается получить доступ к защищаемому ресурсу, компонент Предотвращение вторжений анализирует права всех родительских процессов этой программы на доступ к защищаемому ресурсу. При этом применяются права минимального приоритета: при сравнении прав доступа программы и родительского процесса к активности программы применяются права доступа с минимальным приоритетом.

Приоритет прав доступа следующий:

1. **Разрешать**. Это право доступа имеет высший приоритет.
2. **Запрещать**. Это право доступа имеет низший приоритет.

Этот механизм предотвращает использование доверенных программ недоверенными или ограниченными в правах программами с целью выполнения привилегированных действий.

Если действие программы блокируется по причине недостатка прав у одного из родительских процессов, вы можете изменить эти права или выключить наследование ограничений родительского процесса.

► *Чтобы выключить наследование ограничений родительского процесса, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Программы**.

Откроется закладка **Права программ** окна **Предотвращение вторжений**.

4. Выберите нужную программу.
5. В контекстном меню программы выберите пункт **Права программы**.
Откроется окно **Права программы**.
6. В окне **Права программы** выберите закладку **Исключения**.
7. Установите флажок **Не наследовать ограничения родительского процесса (программы)**.
8. Сохраните внесенные изменения.

Исключение некоторых действий программ из прав программ

► *Чтобы исключить некоторые действия программы из прав программы, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Программы**.
Откроется закладка **Права программ** окна **Предотвращение вторжений**.
4. Выберите нужную программу.
5. В контекстном меню программы выберите пункт **Права программы**.
Откроется окно **Права программы**.
6. Выберите закладку **Исключения**.
7. Установите флажки напротив действий программы, которые не нужно контролировать.
8. Сохраните внесенные изменения.

Удаление информации о неиспользуемых программах

Kaspersky Endpoint Security контролирует работу программ с помощью прав программ. Права программы определены группой доверия. Kaspersky Endpoint Security помещает программу в группу доверия при первом запуске. Вы можете изменить группу доверия для программы вручную (см. раздел "Изменение прав программы" на стр. [107](#)). Также вы можете настроить права для отдельной программы вручную (см. раздел "Изменение прав программы" на стр. [107](#)). Таким образом, Kaspersky Endpoint Security хранит следующую информацию о программе: группа доверия и права программы.

Kaspersky Endpoint Security автоматически удаляет информацию о неиспользуемых программах для экономии ресурсов компьютера. Kaspersky Endpoint Security удаляет информацию о программах по следующим правилам:

- Если группа доверия и права программы определены автоматически, Kaspersky Endpoint Security удаляет информацию об этой программе через 30 дней. Изменить время хранения информации о программе или выключить автоматическое удаление невозможно.
- Если вы вручную поместили программу в группу доверия или настроили права доступа, Kaspersky Endpoint Security удаляет информацию об этой программе через 60 дней (значение по умолчанию). Вы можете изменить время хранения информации о программе или выключить автоматическое удаление (см. инструкцию ниже).

При запуске программы, информация о которой была удалена, Kaspersky Endpoint Security исследует программу как при первом запуске.

► Чтобы настроить автоматическое удаление информации о неиспользуемых программах, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. Выполните одно из следующих действий:
 - Если вы хотите настроить автоматическое удаление, установите флажок **Удалять права для программ, не запускавшихся более N дней** и укажите нужное количество дней.
Kaspersky Endpoint Security будет удалять информацию о тех программах, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, через заданное количество дней. Также Kaspersky Endpoint Security будет удалять информацию о программах, для которых группа доверия и права программы определены автоматически, через 30 дней.
 - Если вы хотите выключить автоматическое удаление, снимите флажок **Удалять права для программ, не запускавшихся более N дней**.
Kaspersky Endpoint Security будет хранить информацию о тех программах, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, без ограничений по времени. Kaspersky Endpoint Security будет удалять информацию только о программах, для которых группа доверия и права программы определены автоматически, через 30 дней.
4. Сохраните внесенные изменения.

Защита ресурсов операционной системы и персональных данных

Компонент Предотвращение вторжений управляет правами программ на операции над различными категориями ресурсов операционной системы и персональных данных.

Специалисты "Лаборатории Касперского" выделили предустановленные категории защищаемых ресурсов. Вы не можете изменять или удалять предустановленные категории защищаемых ресурсов и относящиеся к ним защищаемые ресурсы.

Вы можете выполнить следующие действия:

- добавить новую категорию защищаемых ресурсов;
- добавить новый защищаемый ресурс;
- выключить защиту ресурса.

В этом разделе

Добавление категории защищаемых ресурсов.....	111
Добавление защищаемого ресурса	111
Выключение защиты ресурса	112

Добавление категории защищаемых ресурсов

► *Чтобы добавить новую категорию защищаемых ресурсов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Ресурсы**.
Откроется закладка **Защищаемые ресурсы** окна **Предотвращение вторжений**.
4. В левой части закладки **Защищаемые ресурсы** выберите раздел или категорию защищаемых ресурсов, в которые вы хотите добавить новую категорию защищаемых ресурсов.
5. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Категорию**.
Откроется окно **Категория защищаемых ресурсов**.
6. В окне **Категория защищаемых ресурсов** введите название новой категории защищаемых ресурсов.
7. Сохраните внесенные изменения.

Добавление защищаемого ресурса

► *Чтобы добавить защищаемый ресурс, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Ресурсы**.
Откроется закладка **Защищаемые ресурсы** окна **Предотвращение вторжений**.
4. В левой части закладки **Защищаемые ресурсы** выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.
5. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите тип ресурса, который вы хотите добавить:
 - **Файл или папку.**
 - **Ключ реестра.**Откроется окно **Защищаемый ресурс**.
6. В окне **Защищаемый ресурс** в поле **Название** введите название защищаемого ресурса.
7. Нажмите на кнопку **Обзор**.
8. В открывшемся окне задайте необходимые параметры в зависимости от типа добавляемого защищаемого ресурса и нажмите на кнопку **ОК**.
9. Сохраните внесенные изменения.

Выключение защиты ресурса

► Чтобы выключить защиту ресурса, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Продвинутая защита** → **Предотвращение вторжений**.
3. В правой части окна нажмите на кнопку **Ресурсы**.
Откроется закладка **Защищаемые ресурсы** окна **Предотвращение вторжений**.
4. Выполните одно из следующих действий:
 - В левой части закладки в списке защищаемых ресурсов выберите ресурс, защиту которого вы хотите выключить, и снимите флажок рядом с его названием.
 - Нажмите на кнопку **Исключения** и выполните следующие действия:
 - a. В окне **Исключения** нажмите на кнопку **Добавить** и в раскрывающемся списке выберите тип ресурса, который вы хотите добавить в список исключений из защиты компонента **Предотвращение вторжений**: **Файл или папку** или **Ключ реестра**.
Откроется окно **Защищаемый ресурс**.
 - b. В окне **Защищаемый ресурс** в поле **Название** введите название защищаемого ресурса.
 - c. Нажмите на кнопку **Обзор**.
 - d. В открывшемся окне задайте необходимые параметры в зависимости от типа защищаемого ресурса, который вы хотите добавить в список исключений из защиты компонентом **Предотвращение вторжений**.
 - e. Нажмите на кнопку **ОК**.
 - f. В окне **Защищаемый ресурс** нажмите на кнопку **ОК**.
В списке ресурсов, исключенных из защиты компонента **Предотвращение вторжений**, появится новый элемент.
 - g. В окне **Исключения** нажмите на кнопку **ОК**.
5. Сохраните внесенные изменения.

Откат вредоносных действий

Компонент Откат вредоносных действий позволяет Kaspersky Endpoint Security выполнить откат действий, произведенных вредоносными программами в операционной системе.

Во время отката действий вредоносной программы в операционной системе Kaspersky Endpoint Security обрабатывает следующие типы активности вредоносной программы:

- **Файловая активность**

Kaspersky Endpoint Security выполняет следующие действия:

- удаляет исполняемые файлы, созданные вредоносной программой (на всех носителях, кроме сетевых дисков);
- удаляет исполняемые файлы, созданные программами, в которые внедрилась вредоносная программа;
- восстанавливает измененные или удаленные вредоносной программой файлы.

Функциональность восстановления файлов имеет ряд ограничений (см. раздел "Ограничения функциональности восстановления файлов" на стр. [114](#)).

- **Реестровая активность**

Kaspersky Endpoint Security выполняет следующие действия:

- удаляет разделы и ключи реестра, созданные вредоносной программой;
- не восстанавливает измененные или удаленные вредоносной программой разделы и ключи реестра.

- **Системная активность**

Kaspersky Endpoint Security выполняет следующие действия:

- завершает процессы, которые запускала вредоносная программа;
- завершает процессы, в которые внедрялась вредоносная программа;
- не возобновляет процессы, которые остановила вредоносная программа.

- **Сетевая активность**

Kaspersky Endpoint Security выполняет следующие действия:

- запрещает сетевую активность вредоносной программы;
- запрещает сетевую активность тех процессов, в которые внедрялась вредоносная программа.

Откат действий вредоносной программы может быть запущен компонентом Защита от файловых угроз (см. стр. [115](#)), Анализ поведения (см. раздел «Выбор действия при обнаружении внешнего шифрования папок общего доступа» на стр. [94](#)) или при антивирусной проверке (см. раздел «Проверка компьютера» на стр. [51](#)).

Откат действий вредоносной программы затрагивает строго ограниченный набор данных. Откат не оказывает негативного влияния на работу операционной системы и целостность информации на вашем компьютере.

Защита от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. По умолчанию компонент Защита от файловых угроз постоянно находится в оперативной памяти компьютера. Компонент проверяет файлы на всех дисках компьютера, а также на подключенных дисках. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 87) и эвристического анализа.

Компонент проверяет файлы, к которым обращается пользователь или программа. При обнаружении вредоносного файла Kaspersky Endpoint Security блокирует операцию с файлом. Далее программа лечит или удаляет вредоносный файл, в зависимости от настройки компонента Защита от файловых угроз.

При обращении к файлу, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security загружает и проверяет содержимое этого файла.

В этом разделе

Включение и выключение Защиты от файловых угроз	115
Автоматическая приостановка Защиты от файловых угроз	116
Изменение уровня безопасности	117
Изменение действия компонента Защита от файловых угроз над зараженными файлами	117
Формирование области защиты компонента Защита от файловых угроз	118
Использование эвристического анализа в работе компонента Защита от файловых угроз	120
Использование технологий проверки в работе компонента Защита от файловых угроз	120
Оптимизация проверки файлов	121
Проверка составных файлов	121
Изменение режима проверки файлов	122

Включение и выключение Защиты от файловых угроз

По умолчанию компонент Защита от файловых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Защиту от файловых угроз при необходимости.

► *Чтобы включить или выключить Защиту от файловых угроз, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от файловых угроз**.

3. Выполните одно из следующих действий:
 - Установите флажок **Защита от файловых угроз**, если вы хотите включить Защиту от файловых угроз.
 - Снимите флажок **Защита от файловых угроз**, если вы хотите выключить Защиту от файловых угроз.
4. Сохраните внесенные изменения.

Автоматическая приостановка Защиты от файловых угроз

Вы можете настроить автоматическую приостановку Защиты от файловых угроз в указанное время или во время работы с определенными программами.

Приостановка работы Защиты от файловых угроз при конфликте с определенными программами является экстренной мерой. Если во время работы компонента возникают какие-либо конфликты, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (<https://companyaccount.kaspersky.com> <https://companyaccount.kaspersky.com>). Специалисты помогут вам наладить совместную работу компонента Защита от файловых угроз с другими программами на вашем компьютере.

- *Чтобы настроить автоматическую приостановку работы Защиты от файловых угроз, выполните следующие действия:*
1. В главном окне программы нажмите на кнопку **Настройка**.
 2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от файловых угроз**.
 3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно **Защита от файловых угроз**.
 4. В окне **Защита от файловых угроз** выберите закладку **Дополнительно**.
 5. В блоке **Приостановка задачи** выполните следующие действия:
 - Установите флажок **По расписанию** и нажмите на кнопку **Расписание**, если вы хотите настроить автоматическую приостановку работы Защиты от файловых угроз в указанное время.
Откроется окно **Приостановка задачи**.
 - Установите флажок **При запуске программ** и нажмите на кнопку **Выбрать**, если вы хотите настроить автоматическую приостановку Защиты от файловых угроз при запуске указанных программ.
Откроется окно **Программы**.

6. Выполните одно из следующих действий:

- Если вы настраиваете автоматическую приостановку Защиты от файловых угроз в указанное время, то в окне **Приостановка задачи** в полях **Приостановить в** и **Возобновить в** укажите время (в формате ЧЧ:ММ), в течение которого Защиту от файловых угроз следует приостанавливать. Нажмите на кнопку **ОК**.
- Если вы настраиваете автоматическую приостановку Защиты от файловых угроз при запуске указанных программ, то в окне **Программы** с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список программ, во время работы которых Защиту от файловых угроз следует приостанавливать. Нажмите на кнопку **ОК**.

7. Сохраните внесенные изменения.

Изменение уровня безопасности

Для защиты файловой системы компьютера компонент Защита от файловых угроз применяет разные наборы параметров. Такие наборы параметров называют *уровнями безопасности*. Предусмотрены три уровня безопасности: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского". Вы можете выбрать один из предусмотренных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

► *Чтобы изменить уровень безопасности, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от файловых угроз**.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
 - Если вы хотите установить один из предусмотренных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
 - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Защита от файловых угроз**.
После того как вы самостоятельно настроили уровень безопасности, название уровня безопасности в блоке **Уровень безопасности** изменится на **Другой**.
 - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Сохраните внесенные изменения.

Изменение действия компонента Защита от файловых угроз над зараженными файлами

По умолчанию компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз удаляет эти файлы.

► *Чтобы изменить действие компонента Защита от файловых угроз над зараженными файлами, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от файловых угроз**.
3. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:
 - **Лечить; удалять, если лечение невозможно.**
Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз удаляет эти файлы.
 - **Лечить; блокировать, если лечение невозможно.**
Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз блокирует эти файлы.
 - **Блокировать.**
Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически блокирует зараженные файлы без попытки их вылечить.
4. Сохраните внесенные изменения.

Формирование области защиты компонента Защита от файловых угроз

Под областью защиты подразумеваются объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты компонента Защита от файловых угроз являются местоположение и тип проверяемых файлов. По умолчанию компонент Защита от файловых угроз проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков компьютера.

► *Чтобы сформировать область защиты, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от файловых угроз**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Общие**.

5. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять компонентом Защита от файловых угроз:
- Выберите **Все файлы**, если вы хотите проверять все файлы.
 - Выберите **Файлы, проверяемые по формату**, если вы хотите проверять файлы тех форматов, которые наиболее подвержены заражению.
 - Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, наиболее подверженными заражению.

Выбирая тип проверяемых файлов, нужно помнить следующее:

- Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, TXT) и его последующей активации достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, форматы EXE, DLL, DOC). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.
 - Злоумышленник может отправить вирус или другую программу, представляющую угрозу, на ваш компьютер в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки такой файл пропускается. Если же выбрана проверка файлов по формату, то вне зависимости от расширения компонент Защита от файловых угроз проанализирует заголовок файла, в результате чего может выясниться, что файл имеет формат EXE. Такой файл тщательно проверяется на вирусы и другие программы, представляющие угрозу.
6. В списке **Область защиты** выполните одно из следующих действий:
- Нажмите на кнопку **Добавить**, если вы хотите добавить новый объект в область проверки.
 - Если вы хотите изменить местоположение объекта, выберите объект из области проверки и нажмите на кнопку **Изменить**.

Откроется окно **Выбор области проверки**.

- Если вы хотите удалить объект из списка проверяемых объектов, выберите объект в списке проверяемых объектов и нажмите на кнопку **Удалить**.

Откроется окно подтверждения удаления.

7. Выполните одно из следующих действий:
- Если вы хотите добавить новый объект или изменить местоположение объекта из списка проверяемых объектов, в окне **Выбор области проверки** выберите объект и нажмите на кнопку **Добавить**.
Все объекты, выбранные в окне **Выбор области проверки**, отобразятся в списке **Область защиты** в окне **Защита от файловых угроз**.
Нажмите на кнопку **ОК**.
 - Если вы хотите удалить объект, нажмите на кнопку **Да** в окне подтверждения удаления.
8. Чтобы исключить объект из списка проверяемых объектов, в списке **Область защиты** снимите флажок рядом с ним. Объект при этом остается в списке проверяемых объектов, но исключается из проверки компонентом Защита от файловых угроз.
9. Сохраните внесенные изменения.

Использование эвристического анализа в работе компонента Защита от файловых угроз

Во время своей работы компонент Защита от файловых угроз использует метод проверки Машинное обучение и сигнатурный анализ. В процессе сигнатурного анализа компонент Защита от файловых угроз сравнивает найденный объект с записями в антивирусных базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа компонент Защита от файловых угроз анализирует активность, которую объекты производят в системе. Эвристический анализ позволяет обнаруживать вредоносные объекты, записей о которых еще нет в антивирусных базах программы.

► *Чтобы настроить использование эвристического анализа в работе компонента Защита от файловых угроз, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от файловых угроз**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Производительность**.
5. В блоке **Методы проверки** выполните следующие действия:
 - Если вы хотите, чтобы компонент Защита от файловых угроз использовал эвристический анализ, установите флажок **Эвристический анализ** и при помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.
 - Если вы хотите, чтобы компонент Защита от файловых угроз не использовал эвристический анализ, снимите флажок **Эвристический анализ**.
6. Сохраните внесенные изменения.

Использование технологий проверки в работе компонента Защита от файловых угроз

► *Чтобы настроить использование технологий проверки в работе компонента Защита от файловых угроз, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от файловых угроз**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Дополнительно**.

5. В блоке **Технологии проверки** выполните следующие действия:
 - Установите флажки около названий тех технологий, которые вы хотите использовать в работе компонента Защита от файловых угроз.
 - Снимите флажки около названий тех технологий, которые вы не хотите использовать в работе компонента Защита от файловых угроз.
6. Сохраните внесенные изменения.

Оптимизация проверки файлов

Вы можете оптимизировать проверку файлов компонентом Защита от файловых угроз: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Вы также можете включить использование технологий iChecker и iSwift, которые позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

► *Чтобы оптимизировать проверку файлов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от файловых угроз**.
3. Нажмите на кнопку **Настройка**.
Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Производительность**.
5. В блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.
6. Сохраните внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы или почтовые базы. Чтобы обнаружить скрытые таким образом вирусы и другие программы, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить круг проверяемых составных файлов, таким образом увеличив скорость проверки.

Способ обработки зараженного составного файла (лечение или удаление) зависит от типа файла. Компонент Защита от файловых угроз лечит составные файлы форматов RAR, ARJ, ZIP, CAB, LHA и удаляет файлы всех остальных форматов (кроме почтовых баз).

► Чтобы настроить проверку составных файлов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от файловых угроз**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

Откроется окно **Защита от файловых угроз**.

4. В окне **Защита от файловых угроз** выберите закладку **Производительность**.
5. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты или файлы офисных форматов.
6. Чтобы проверять только новые и измененные составные файлы, установите флажок **Проверять только новые и измененные файлы**.

Компонент Защита от файловых угроз будет проверять только новые и измененные составные файлы всех типов.

7. Нажмите на кнопку **Дополнительно**.

Откроется окно **Составные файлы**.

8. В блоке **Фоновая проверка** выполните одно из следующих действий:

- Чтобы запретить компоненту Защита от файловых угроз распаковывать составные файлы в фоновом режиме, снимите флажок **Распаковывать составные файлы в фоновом режиме**.
- Чтобы разрешить компоненту Защита от файловых угроз распаковывать составные файлы при проверке в фоновом режиме, установите флажок **Распаковывать составные файлы в фоновом режиме** и в поле **Минимальный размер файла** укажите нужное значение.

9. В блоке **Ограничение по размеру** выполните одно из следующих действий:

- Чтобы запретить компоненту Защита от файловых угроз распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение. Компонент Защита от файловых угроз не будет распаковывать составные файлы больше указанного размера.
- Чтобы разрешить компоненту Защита от файловых угроз распаковывать составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

Файлом большого размера считается файл, размер которого больше значения в поле **Максимальный размер файла**.

Компонент Защита от файловых угроз проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

10. Сохраните внесенные изменения.

Изменение режима проверки файлов

Под *режимом проверки* подразумевается условие, при котором компонент Защита от файловых угроз начинает проверять файлы. По умолчанию Kaspersky Endpoint Security использует интеллектуальный режим проверки файлов. Работая в этом режиме проверки файлов, компонент Защита от файловых угроз принимает решение о проверке файлов на основании анализа операций, которые пользователь, программа от имени пользователя (под учетными данными которого был осуществлен вход в операционную систему или другого пользователя) или операционная система выполняет над файлами. Например, работая с документом Microsoft Office Word, Kaspersky Endpoint Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

► *Чтобы изменить режим проверки файлов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от файловых угроз**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Дополнительно**.
5. В блоке **Режим проверки** выберите нужный режим:
 - **Интеллектуальный**.
 - **При доступе и изменении**.
 - **При доступе**.
 - **При выполнении**.
6. Сохраните внесенные изменения.

Защита от веб-угроз

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует вредоносные и фишинговые веб-сайты. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. [87](#)) и эвристического анализа.

Kaspersky Endpoint Security проверяет HTTP-, HTTPS- и FTP-трафик. Kaspersky Endpoint Security проверяет URL- и IP-адреса. Вы можете задать порты, которые Kaspersky Endpoint Security будет контролировать, (см. раздел "Контроль сетевых портов" на стр. [187](#)) или выбрать все порты.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений (см. раздел "Включение и выключение проверки защищенных соединений" на стр. [191](#)).

При попытке пользователя открыть вредоносный или фишинговый веб-сайт, Kaspersky Endpoint Security заблокирует доступ и покажет предупреждение (см. рис. ниже).



Рисунок 10. Сообщение о запрете доступа к веб-сайту

В этом разделе

Включение и выключение Защиты от веб-угроз	125
Изменение уровня безопасности веб-трафика	125
Изменение действия над вредоносными объектами веб-трафика	126
Проверка компонентом Защита от веб-угроз ссылок по базам фишинговых и вредоносных веб-адресов	127
Использование эвристического анализа в работе компонента Защита от веб-угроз	128
Формирование списка доверенных веб-адресов	128

Включение и выключение Защиты от веб-угроз

По умолчанию компонент Защита от веб-угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить компонент Защита от веб-угроз при необходимости.

► *Чтобы включить или выключить компонент Защита от веб-угроз выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от веб-угроз**.
3. Выполните одно из следующих действий:
 - Установите флажок **Защита от веб-угроз**, если вы хотите включить компонент Защита от веб-угроз.
 - Снимите флажок **Защита от веб-угроз**, если вы хотите выключить компонент Защита от веб-угроз.
4. Сохраните внесенные изменения.

Изменение уровня безопасности веб-трафика

Для защиты данных, получаемых и передаваемых по протоколам HTTP и FTP, компонент Защита от веб-угроз применяет разные наборы параметров. Такие наборы параметров называются *уровнями безопасности веб-трафика*. Предусмотрены три уровня безопасности веб-трафика: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности веб-трафика **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского". Вы можете выбрать один из предустановленных уровней безопасности веб-трафика, получаемых или передаваемых по протоколам HTTP и FTP, или настроить уровень безопасности веб-трафика самостоятельно. После того как вы изменили параметры уровня безопасности веб-трафика, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности веб-трафика.

► *Чтобы изменить уровень безопасности веб-трафика, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от веб-угроз**.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
 - Если вы хотите установить один из предустановленных уровней безопасности веб-трафика (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
 - Если вы хотите настроить уровень безопасности веб-трафика самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Защита от веб-угроз**.
После того как вы самостоятельно настроили уровень безопасности веб-трафика, название уровня безопасности веб-трафика в блоке **Уровень безопасности** изменится на **Другой**.
 - Если вы хотите изменить настроенный самостоятельно уровень безопасности веб-трафика на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Сохраните внесенные изменения.

Изменение действия над вредоносными объектами веб-трафика

По умолчанию в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и выводит на экран окно уведомления о блокировке.

► *Чтобы изменить действие над вредоносными объектами веб-трафика, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от веб-угроз**.
3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами веб-трафика:
 - **Запрещать загрузку.**
Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и выводит на экран окно уведомления о блокировке, создает в журнале запись, содержащую информацию о зараженном объекте.
 - **Информировать.**
Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз разрешает загрузку этого объекта на компьютер и Kaspersky Endpoint Security создает в журнале запись, содержащую информацию о зараженном объекте, добавляет информацию о зараженном объекте в список активных угроз.
4. Сохраните внесенные изменения.

Проверка компонентом Защита от веб-угроз ссылок по базам фишинговых и вредоносных веб-адресов

Проверка ссылок на принадлежность к фишинговым веб-адресам позволяет избежать *фишинговых атак*. Частным примером фишинговых атак может служить сообщение электронной почты якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт банка в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его веб-адрес в браузере, однако находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия на веб-сайте отслеживаются и могут быть использованы для кражи ваших денежных средств.

Поскольку ссылка на фишинговый веб-сайт может содержаться не только в сообщении электронной почты, но и, например, в тексте ICQ-сообщения, компонент Защита от веб-угроз отслеживает попытки перейти на фишинговый веб-сайт на уровне проверки веб-трафика и блокирует доступ к таким веб-сайтам. Списки фишинговых веб-адресов включены в комплект поставки Kaspersky Endpoint Security.

► *Чтобы настроить проверку компонентом Защита от веб-угроз ссылок по базам фишинговых и вредоносных веб-адресов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от веб-угроз**.
3. Нажмите на кнопку **Настройка**.

Откроется окно **Защита от веб-угроз**.

4. В окне **Защита от веб-угроз** выберите закладку **Общие**.
5. Выполните следующие действия:
 - В блоке **Методы проверки** установите флажок **Проверять ссылки по базе вредоносных веб-адресов**, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам вредоносных веб-адресов.

Kaspersky Endpoint Security проверяет ссылки по базам вредоносных веб-адресов, даже если сетевой трафик передается по защищенному соединению и флажок **Проверять защищенные соединения** (см. раздел "**Включение и выключение проверки защищенных соединений**" на стр. 191) снят.

- В блоке **Параметры антифишинга** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам фишинговых веб-адресов.

Для проверки ссылок вы также можете использовать репутационные базы Kaspersky Security Network.

6. Сохраните внесенные изменения.

Использование эвристического анализа в работе компонента Защита от веб-угроз

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Endpoint Security анализирует активность, которую программы производят в операционной системе. Эвристический анализ позволяет обнаруживать угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security.

► *Чтобы настроить использование эвристического анализа, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от веб-угроз**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно **Защита от веб-угроз**.
4. Выберите закладку **Общие**.
5. Если вы хотите, чтобы компонент Защита от веб-угроз использовал эвристический анализ при проверке веб-трафика на наличие вирусов и других программ, представляющих угрозу, в блоке **Методы проверки** установите флажок **Эвристический анализ для обнаружения вирусов** и при помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.
6. Если вы хотите, чтобы компонент Защита от веб-угроз использовал эвристический анализ при проверке веб-страниц на наличие фишинговых ссылок, в блоке **Параметры антифишинга** установите флажок **Эвристический анализ для обнаружения фишинговых ссылок**.
7. Сохраните внесенные изменения.

Формирование списка доверенных веб-адресов

Вы можете сформировать список веб-адресов, содержанию которых вы доверяете. Компонент Защита от веб-угроз не анализирует информацию, поступающую с доверенных веб-адресов, на присутствие вирусов и других программ, представляющих угрозу. Такая возможность может быть использована, например, в том случае, если компонент Защита от веб-угроз препятствует загрузке файла с известного вам веб-сайта.

Под веб-адресом подразумевается адрес как отдельной веб-страницы, так и веб-сайта.

► *Чтобы сформировать список доверенных веб-адресов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от веб-угроз**.
3. Нажмите на кнопку **Настройка**.
Откроется окно **Защита от веб-угроз**.
4. Выберите закладку **Доверенные веб-адреса**.
5. Установите флажок **Не проверять веб-трафик с доверенных веб-адресов**.

6. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете. Для пополнения списка выполните следующие действия:
 - a. Нажмите на кнопку **Добавить**.
Откроется окно **Веб-адрес / Маска веб-адреса**.
 - b. Введите адрес веб-сайта / веб-страницы или маску адреса веб-сайта / веб-страницы.
 - c. Нажмите на кнопку **ОК**.
В списке доверенных веб-адресов появится новая запись.
7. Сохраните внесенные изменения.

Защита от почтовых угроз

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других программ, представляющих угрозу. Также компонент проверяет сообщения на наличие вредоносных и фишинговых ссылок. По умолчанию компонент Защита от почтовых угроз постоянно находится в оперативной памяти компьютера и проверяет все сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, NNTP или в почтовом клиенте Microsoft Office Outlook (MAPI). Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. [87](#)) и эвристического анализа.

Компонент Защита от почтовых угроз не проверяет сообщения, если почтовый клиент открыт в браузере.

При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security переименовывает тему сообщения: [Сообщение заражено] <тема сообщения> или [Зараженный объект удален] <тема сообщения>.

Компонент взаимодействует с почтовыми клиентами, установленными на компьютере. Для почтового клиента Microsoft Office Outlook предусмотрено расширение с дополнительными параметрами. Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft Office Outlook во время установки Kaspersky Endpoint Security.

В этом разделе

Включение и выключение Защиты от почтовых угроз.....	130
Изменение уровня безопасности почты	131
Изменение действия над зараженными сообщениями электронной почты	132
Формирование области защиты компонента Защита от почтовых угроз	132
Проверка составных файлов, вложенных в сообщения электронной почты	134
Фильтрация вложений в сообщениях электронной почты	134

Включение и выключение Защиты от почтовых угроз

По умолчанию компонент Защита от почтовых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме.

► *Чтобы включить или выключить компонент Защита от почтовых угроз выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от почтовых угроз**.
3. Выполните одно из следующих действий:
 - Установите флажок **Защита от почтовых угроз**, если вы хотите включить компонент Защита от почтовых угроз.
 - Снимите флажок **Защита от почтовых угроз**, если вы хотите выключить компонент Защита от почтовых угроз.
4. Сохраните внесенные изменения.

Изменение уровня безопасности почты

Для защиты почты компонент Защита от почтовых угроз применяет разные наборы параметров. Такие наборы параметров называют *уровнями безопасности почты*. Установлены три уровня безопасности почты: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности почты **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского". Вы можете выбрать один из предустановленных уровней безопасности почты или настроить уровень безопасности почты самостоятельно. После того как вы изменили параметры уровня безопасности почты, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности почты.

► *Чтобы изменить уровень безопасности почты, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от почтовых угроз**.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
 - Если вы хотите установить один из предустановленных уровней безопасности почты (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
 - Если вы хотите настроить уровень безопасности почты самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Защита от почтовых угроз**.
После того как вы самостоятельно настроили уровень безопасности почты, название уровня безопасности почты в блоке **Уровень безопасности** изменится на **Другой**.
 - Если вы хотите изменить настроенный самостоятельно уровень безопасности почты на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Сохраните внесенные изменения.

Изменение действия над зараженными сообщениями электронной почты

По умолчанию компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз удаляет зараженные сообщения электронной почты.

► *Чтобы изменить действие над зараженными сообщениями электронной почты, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от почтовых угроз**.
3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое выполняет Kaspersky Endpoint Security при обнаружении зараженного сообщения:

- **Лечить; удалять, если лечение невозможно.**

Если выбран этот вариант действия, то компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз удаляет зараженные сообщения электронной почты.

- **Лечить; блокировать, если лечение невозможно.**

Если выбран этот вариант действия, то компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз блокирует зараженные сообщения электронной почты.

- **Блокировать.**

Если выбран этот вариант действия, то компонент Защита от почтовых угроз автоматически блокирует зараженные сообщения электронной почты без попытки их вылечить.

4. Сохраните внесенные изменения.

Формирование области защиты компонента Защита от почтовых угроз

Область защиты – это объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты компонента Защита от почтовых угроз являются параметры интеграции компонента Защита от почтовых угроз в почтовые клиенты, тип сообщений электронной почты и почтовые протоколы, трафик которых проверяет компонент Защита от почтовых угроз. По умолчанию Kaspersky Endpoint Security проверяет как входящие, так и исходящие сообщения электронной почты, трафик почтовых протоколов POP3, SMTP, NNTP и IMAP, а также интегрируется в почтовый клиент Microsoft Office Outlook.

► *Чтобы сформировать область защиты компонента Защита от почтовых угроз, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от почтовых угроз**.

3. Нажмите на кнопку **Настройка**.

Откроется окно **Защита от почтовых угроз**.

4. Выберите закладку **Общие**.

5. В блоке **Область защиты** выполните одно из следующих действий:

- Выберите вариант **Входящие и исходящие сообщения**, если вы хотите, чтобы компонент Защита от почтовых угроз проверял все входящие и исходящие сообщения на вашем компьютере.
- Выберите вариант **Только входящие сообщения**, если вы хотите, чтобы компонент Защита от почтовых угроз проверял только входящие сообщения на вашем компьютере.

Если вы выбираете проверку только входящих сообщений, рекомендуется однократно проверить все исходящие сообщения, поскольку существует вероятность того, что на вашем компьютере есть почтовые черви, которые используют электронную почту в качестве канала распространения. Это позволит избежать проблем, связанных с неконтролируемой рассылкой зараженных сообщений с вашего компьютера.

6. В блоке **Встраивание в систему** выполните следующие действия:

- Установите флажок **Трафик POP3 / SMTP / NNTP / IMAP**, если вы хотите, чтобы компонент Защита от почтовых угроз проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя.

Снимите флажок **Трафик POP3 / SMTP / NNTP / IMAP**, если вы хотите, чтобы компонент Защита от почтовых угроз не проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя. В этом случае сообщения проверяет расширение компонента Защита от почтовых угроз, встроенное в почтовый клиент Microsoft Office Outlook, после их получения на компьютере пользователя, если установлен флажок **Дополнительно: расширение в Microsoft Office Outlook**.

Если вы используете почтовый клиент, отличный от Microsoft Office Outlook, то при снятом флажке **Трафик POP3 / SMTP / NNTP / IMAP** компонент Защита от почтовых угроз не проверяет сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP.

- Установите флажок **Дополнительно: расширение в Microsoft Office Outlook**, если вы хотите открыть доступ к настройке параметров компонента Защита от почтовых угроз из программы Microsoft Office Outlook и включить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя с помощью расширения, интегрированного в программу Microsoft Office Outlook.

Снимите флажок **Дополнительно: расширение в Microsoft Office Outlook**, если вы хотите закрыть доступ к настройке параметров компонента Защита от почтовых угроз из программы Microsoft Office Outlook и выключить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя с помощью расширения, интегрированного в программу Microsoft Office Outlook.

Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft Office Outlook во время установки Kaspersky Endpoint Security.

7. Сохраните внесенные изменения.

Проверка составных файлов, вложенных в сообщения электронной почты

Вы можете включить или выключить проверку объектов, вложенных в сообщения, ограничить максимальный размер проверяемых объектов, вложенных в сообщения, и максимальную длительность проверки объектов, вложенных в сообщения.

► *Чтобы настроить проверку составных файлов, вложенных в сообщения электронной почты, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от почтовых угроз**.
3. Нажмите на кнопку **Настройка**.
Откроется окно **Защита от почтовых угроз**.
4. Выберите закладку **Общие**.
5. В блоке **Проверка составных файлов** выполните следующие действия:
 - Снимите флажок **Проверять вложенные архивы**, если вы хотите, чтобы компонент Защита от почтовых угроз не выполнял проверку вложенных в сообщения архивов.
 - Снимите флажок **Проверять вложенные файлы офисных форматов**, если вы хотите, чтобы компонент Защита от почтовых угроз не выполнял проверку вложенных в сообщения файлов офисных форматов.
 - Установите флажок **Не проверять архивы размером более N МБ**, если вы хотите, чтобы компонент Защита от почтовых угроз не проверял вложенные в сообщения архивы размером более N мегабайт. Если вы установили этот флажок, укажите максимальный размер архивов в поле рядом с названием флажка.
 - Снимите флажок **Не проверять архивы более N с**, если вы хотите, чтобы компонент Защита от почтовых угроз проверял вложенные в сообщения архивы, если на их проверку затрачивается более N секунд.
6. Сохраните внесенные изменения.

Фильтрация вложений в сообщениях электронной почты

Функциональность фильтрации вложений не применяется для исходящих сообщений электронной почты.

Вредоносные программы могут распространяться в виде вложений в сообщениях электронной почты. Вы можете настроить фильтрацию по типу вложений в сообщениях, чтобы автоматически переименовывать или удалять файлы указанных типов. Переименовав вложение определенного типа, Kaspersky Endpoint Security может защитить ваш компьютер от автоматического запуска вредоносной программы.

► Чтобы настроить фильтрацию вложений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от почтовых угроз**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
Откроется окно **Защита от почтовых угроз**.
4. В окне **Защита от почтовых угроз** выберите закладку **Фильтр вложений**.
5. Выполните одно из следующих действий:
 - Выберите вариант **Не применять фильтр**, если вы хотите, чтобы компонент Защита от почтовых угроз не фильтровал вложения в сообщениях.
 - Выберите вариант **Переименовывать вложения указанных типов**, если вы хотите, чтобы компонент Защита от почтовых угроз изменял названия вложенных в сообщения файлы указанных типов.
 - Выберите вариант **Удалять вложения указанных типов**, если вы хотите, чтобы компонент Защита от почтовых угроз удалял вложенные в сообщения файлы указанных типов.
6. Если на предыдущем шаге инструкции вы выбрали вариант **Переименовывать вложения указанных типов** или вариант **Удалять вложения указанных типов**, установите флажки напротив нужных типов файлов.
7. Сохраните внесенные изменения.

Защита от сетевых угроз

Компонент Защита от сетевых угроз (англ. IDS – Intrusion Detection System) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security блокирует сетевое соединение с атакующим компьютером.

Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах Kaspersky Endpoint Security. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей программы.

В этом разделе

Включение и выключение Защиты от сетевых угроз.....	136
Изменение параметров блокирования атакующего компьютера.....	136
Настройка адресов исключений из блокирования.....	137
Защита от атак типа MAC-спуфинг	137

Включение и выключение Защиты от сетевых угроз

По умолчанию Защита от сетевых угроз включена и работает в оптимальном режиме. При необходимости вы можете выключить Защиту от сетевых угроз.

► *Чтобы включить или выключить Защиту от сетевых угроз выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от сетевых угроз**.
3. Выполните следующие действия:
 - Установите флажок **Защита от сетевых угроз**, если вы хотите включить Защиту от сетевых угроз.
 - Снимите флажок **Защита от сетевых угроз**, если вы хотите выключить Защиту от сетевых угроз.
4. Сохраните внесенные изменения.

Изменение параметров блокирования атакующего компьютера

► *Чтобы изменить параметры блокирования атакующего компьютера, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от сетевых угроз**.

3. Установите флажок **Добавить атакующий компьютер в список блокирования на**.

Если этот флажок установлен, то, обнаружив попытку сетевой атаки, компонент Защита от сетевых угроз блокирует сетевую активность атакующего компьютера в течение заданного времени, чтобы автоматически защитить компьютер от возможных будущих сетевых атак с этого адреса.

Если этот флажок снят, то, обнаружив попытку сетевой атаки, компонент Защита от сетевых угроз не включает автоматическую защиту от возможных будущих сетевых атак с этого адреса.

4. Измените время блокирования атакующего компьютера в поле, расположенном справа от флажка **Добавить атакующий компьютер в список блокирования на**.
5. Сохраните внесенные изменения.

Настройка адресов исключений из блокирования

► *Чтобы настроить адреса исключений из блокирования, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от сетевых угроз**.
3. Нажмите на кнопку **Исключения**.

Откроется окно **Исключения**.

4. Выполните одно из следующих действий:

- Если хотите добавить новый IP-адрес, нажмите на кнопку **Добавить**.
- Если хотите изменить добавленный ранее IP-адрес, выберите его в списке адресов и нажмите на кнопку **Изменить**.

Откроется окно **IP-адрес**.

5. Введите IP-адрес компьютера, сетевые атаки с которого не должны блокироваться.
6. Сохраните внесенные изменения.

Защита от атак типа MAC-спуфинг

Компонент Защита от сетевых угроз отслеживает уязвимости в протоколе определения адреса (англ. Address Resolution Protocol – ARP). Таким образом компонент защищает компьютер от *атак типа MAC-спуфинг*. Атака типа MAC-спуфинг заключается в изменении MAC-адреса сетевого устройства (сетевой карты). В результате злоумышленник может перенаправить данные, отправленные на устройство, на другое устройство и получить доступ к этим данным.

По умолчанию Kaspersky Endpoint Security не отслеживает атаки типа MAC-спуфинг.

► *Чтобы изменить режим работы защиты от атак типа MAC-спуфинг, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от сетевых угроз**.

3. В блоке **Режим работы защиты от атак типа MAC-спуфинг** выберите один из следующих вариантов:
- **Не отслеживать атаки типа MAC-спуфинг.**
 - **Уведомлять обо всех признаках атак типа MAC-спуфинг.**
 - **Блокировать все признаки атак типа MAC-спуфинг.**

Защита от атак BadUSB

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру.

Компонент Защита от атак BadUSB позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.

Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, программа предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный программой. Эта процедура называется авторизацией клавиатуры. Программа разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

Компонент Защита от атак BadUSB не устанавливается по умолчанию. Если вам нужен компонент Защита от атак BadUSB, вы можете добавить компонент в свойствах инсталляционного пакета перед установкой программы или измените состав компонентов программы после установки программы.

В этом разделе

Включение и выключение Защиты от атак BadUSB	139
Разрешение и запрещение использования экранной клавиатуры при авторизации	139
Авторизация клавиатуры.....	140

Включение и выключение Защиты от атак BadUSB

► *Чтобы включить или выключить Защиту от атак BadUSB, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от атак BadUSB**.
3. Выполните одно из следующих действий:
 - Установите флажок **Защита от атак BadUSB**, если вы хотите включить Защиту от атак BadUSB.
 - Снимите флажок **Защита от атак BadUSB**, если вы хотите выключить Защиту от атак BadUSB.
4. Сохраните внесенные изменения.

Разрешение и запрещение использования экранной клавиатуры при авторизации

Возможность использовать экранную клавиатуру предназначена только для авторизации USB-устройств, не поддерживающих произвольный ввод символов (например, сканеров штрих-кодов). Не рекомендуется использовать экранную клавиатуру для авторизации неизвестных вам USB-устройств.

► *Чтобы разрешить или запретить использование экранной клавиатуры при авторизации, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Защита от атак BadUSB**.
В правой части окна отобразятся параметры компонента.
3. Выполните одно из следующих действий:
 - Установите флажок **Запретить использование экранной клавиатуры для авторизации USB-устройств**, если вы хотите запретить использование экранной клавиатуры для авторизации.
 - Снимите флажок **Запретить использование экранной клавиатуры для авторизации USB-устройств**, если вы хотите разрешить использование экранной клавиатуры для авторизации.
4. Сохраните внесенные изменения.

Авторизация клавиатуры

USB-устройства, определенные операционной системой как клавиатуры и подключенные к компьютеру до установки компонента Защита от атак BadUSB, считаются авторизованными после его установки.

Программа требует авторизацию подключенного USB-устройства, определенного операционной системой как клавиатура, если включен запрос авторизации USB-клавиатур. Пользователь не может использовать неавторизованную клавиатуру до тех пор, пока она не будет авторизована.

Если запрос авторизации USB-клавиатур выключен, пользователь может использовать все подключенные клавиатуры. Сразу после включения запроса авторизации USB-клавиатур программа запрашивает авторизацию для каждой подключенной неавторизованной клавиатуры.

► *Чтобы авторизовать клавиатуру, выполните следующие действия:*

1. При включенной авторизации USB-клавиатур подключите клавиатуру к USB-порту.
Откроется окно **Авторизация клавиатуры <Название клавиатуры>** с информацией о подключенной клавиатуре и цифровым кодом для ее авторизации.
2. С подключенной или экранной клавиатуры, если она доступна, последовательно введите случайно сформированной в окне авторизации цифровой код.
3. Нажмите на кнопку **ОК**.

Если код введен правильно, программа сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

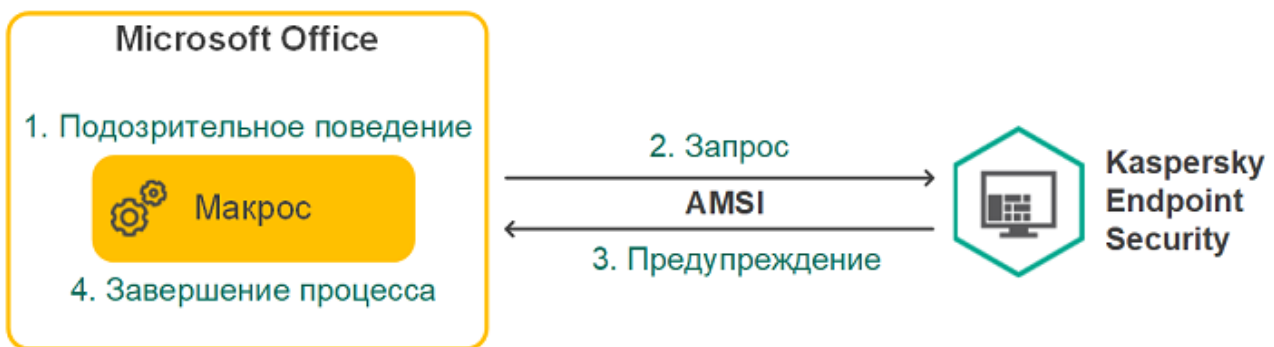
При подключении авторизованной клавиатуры через другой USB-порт компьютера программа снова запрашивает ее авторизацию.

Если цифровой код введен неправильно, программа формирует новый. Число попыток для ввода цифрового кода равно трем. Если цифровой код введен неправильно трижды или закрыто окно **Авторизация клавиатуры <Название клавиатуры>**, программа блокирует ввод с этой клавиатуры. При повторном подключении клавиатуры или перезагрузке операционной системы программа снова предлагает пройти авторизацию клавиатуры.

Поставщик AMSI-защиты

Поставщик AMSI-защиты предназначен для поддержки интерфейса Antimalware Scan Interface от Microsoft. *Интерфейс Antimalware Scan Interface (AMSI)* позволяет сторонним приложениям с поддержкой AMSI отправлять объекты (например, скрипты PowerShell) в Kaspersky Endpoint Security для дополнительной проверки и получать результаты проверки этих объектов. Сторонними приложениями могут быть, например, программы Microsoft Office (см. рис. ниже). Подробнее об интерфейсе AMSI см. в *документации Microsoft* <https://docs.microsoft.com/ru-ru/windows/desktop/amsi/antimalware-scan-interface-portal>.

Поставщик AMSI-защиты может только обнаруживать угрозу и уведомлять стороннее приложение об обнаруженной угрозе. Стороннее приложение после получения уведомления об угрозе не дает выполнить вредоносные действия (например, завершает работу).



Компонент Поставщик AMSI-защиты может отклонить запрос от стороннего приложения, например, если это приложение превысило максимальное количество запросов за промежуток времени. Kaspersky Endpoint Security отправляет информацию об отклонении запроса от стороннего приложения на Сервер администрирования. Компонент Поставщик AMSI-защиты не отклоняет запросы от тех сторонних приложений, для которых установлен флажок **Не блокировать взаимодействие с Поставщиком AMSI-защиты** (см. раздел **"Формирование списка доверенных программ"** на стр. [69](#)).

Поставщик AMSI-защиты доступен для следующих операционных систем рабочих станций и серверов:

- Windows 10 Home / Pro / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

В этом разделе

Включение и выключение Поставщика AMSI-защиты.....	142
Проверка составных файлов Поставщиком AMSI-защиты	142

Включение и выключение Поставщика AMSI-защиты

По умолчанию Поставщик AMSI-защиты включен.

► *Чтобы включить или выключить Поставщик AMSI-защиты, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Базовая защита** → **Поставщик AMSI-защиты**.
3. Выполните одно из следующих действий:
 - Установите флажок **Поставщик AMSI-защиты**, если вы хотите включить Поставщик AMSI-защиты.
 - Снимите флажок **Поставщик AMSI-защиты**, если вы хотите выключить Поставщик AMSI-защиты.
4. Сохраните внесенные изменения.

Проверка составных файлов Поставщиком AMSI-защиты

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы. Чтобы обнаружить скрытые таким образом вирусы и другие программы, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить набор типов проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Чтобы настроить проверку составных файлов Поставщиком AMSI-защиты, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Поставщик AMSI-защиты**.
3. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, дистрибутивы или файлы офисных форматов.
4. В блоке **Ограничение по размеру** выполните одно из следующих действий:
 - Чтобы запретить компоненту Поставщик AMSI-защиты распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение. Компонент Поставщик AMSI-защиты не будет распаковывать составные файлы больше указанного размера.

- Чтобы разрешить компоненту Поставщик AMSI-защиты распаковывать составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

Компонент Поставщик AMSI-защиты проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

5. Сохраните внесенные изменения.

Контроль программ

Контроль программ управляет запуском программ на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании программ. Также Контроль программ снижает риск заражения компьютера, ограничивая доступ к программам.

Настройка Контроля программ состоит из следующих этапов:

1. Создание категорий программ.

Администратор создает категории программ, которыми администратор хочет управлять. Категории программ предназначены для всех компьютеров сети организации независимо от групп администрирования. Для создания категории вы можете использовать следующие критерии: KL-категория (например, *Браузеры*), хеш файла, производитель программы и другие.

2. Создание правил Контроля программ (см. раздел "Добавление и изменение правила Контроля программ" на стр. [63](#)).

Администратор создает правила Контроля программ в политике для группы администрирования. Правило включает в себя категории программ и статус запуска программ из этих категорий: запрещен или разрешен.

3. Выбор режима работы Контроля программ (см. раздел "Выбор режима Контроля программ" на стр. [159](#)).

Администратор выбирает режим работы с программами, которые не входят ни в одно из правил: черный и белый списки.

При попытке пользователя запустить запрещенную программу, Kaspersky Endpoint Security заблокирует запуск программы и покажет уведомление (см. рис. ниже).

Для проверки настройки Контроля программ предусмотрен *тестовый режим*. В этом режиме Kaspersky Endpoint Security выполняет следующие действия:

- разрешает запуск программ, в том числе запрещенных;
- показывает уведомление о запуске запрещенной программы и добавляет информацию в отчет на компьютере пользователя;
- отправляет данные о запуске запрещенных программ в Kaspersky Security Center.

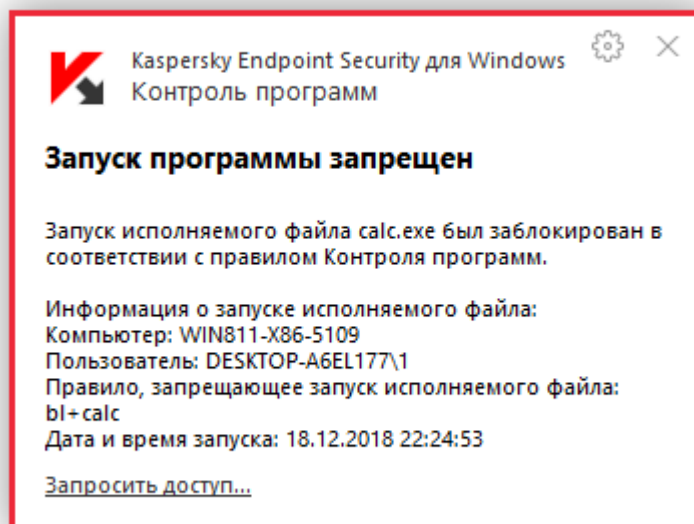


Рисунок 11. Уведомление Контроля программ

Режимы работы Контроля программ

Компонент Контроль программ может работать в двух режимах:

- **Черный список.** Режим, при котором Контроль программ разрешает пользователям запуск любых программ, кроме тех, которые запрещены в правилах Контроля программ.

Этот режим работы Контроля программ установлен по умолчанию.

- **Белый список.** Режим, при котором Контроль программ запрещает пользователям запуск любых программ, кроме тех, которые разрешены и не запрещены в правилах Контроля программ.

Если разрешающие правила Контроля программ сформированы максимально полно, компонент запрещает запуск всех новых программ, не проверенных администратором локальной сети организации, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

Вы можете ознакомиться с рекомендациями по настройке правил контроля программ в режиме белого списка.

Настройка Контроля программ для работы в этих режимах возможна как в локальном интерфейсе Kaspersky Endpoint Security, так и с помощью Kaspersky Security Center.

Однако Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Kaspersky Endpoint Security и необходимые для следующих задач:

- Создание категорий программ.
Правила Контроля программ, сформированные в Консоли администрирования Kaspersky Security Center, основываются на созданных вами категориях программ, а не на включающих и исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security.
- Получение информации о программах, которые установлены на компьютерах локальной сети организации.

Поэтому настройку работы компонента Контроль программ рекомендуется выполнять с помощью Kaspersky Security Center.

Алгоритм работы Контроля программ

Kaspersky Endpoint Security использует алгоритм для принятия решения о запуске программы (см. рис. ниже).

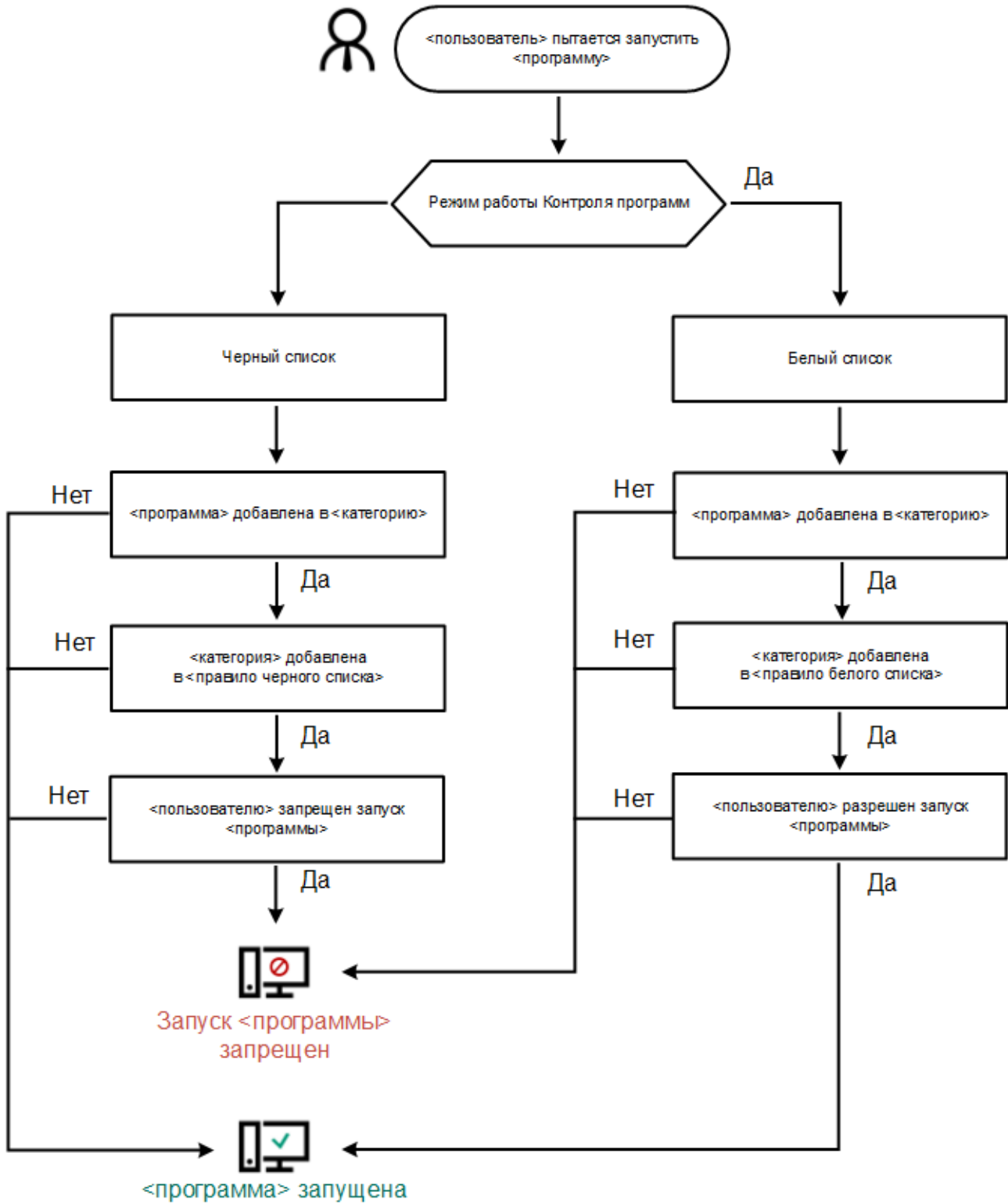


Рисунок 12. Алгоритм работы Контроля программ

В этом разделе

Ограничения функциональности Контроля программ.....	147
Включение и выключение Контроля программ.....	148
Действия с правилами Контроля программ.....	149
Изменение шаблонов сообщений Контроля программ.....	158
О режимах работы Контроля программ.....	159
Выбор режима Контроля программ.....	159

Ограничения функциональности Контроля программ

Работа компонента Контроль программ ограничена в следующих случаях:

- При обновлении версии программы импорт параметров компонента Контроль программ не поддерживается.
- При обновлении версии программы импорт параметров компонента Контроль программ поддерживается только при обновлении версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше до Kaspersky Endpoint Security 11.3.0 для Windows.

При обновлении версий программы, отличных от Kaspersky Endpoint Security 10 Service Pack 2 для Windows, для восстановления работоспособности Контроля программ необходимо заново настроить параметры работы компонента.

- При отсутствии соединения с серверами KSN Kaspersky Endpoint Security получает информацию о репутации программ и их модулей только из локальных баз.

Список программ, для которых Kaspersky Endpoint Security определяет KL-категорию **Программы, доверенные согласно репутации в KSN**, при наличии соединения с серверами KSN может отличаться от списка программ, для которых Kaspersky Endpoint Security определяет KL-категорию **Программы, доверенные согласно репутации в KSN**, при отсутствии соединения с KSN.

- В базе данных Kaspersky Security Center может храниться информация о 150 000 обработанных файлов. При достижении этого количества записей новые файлы не будут обработаны. Для возобновления работы инвентаризации требуется удалить с компьютера, на котором установлена программа Kaspersky Endpoint Security, файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

- Компонент не контролирует запуск скриптов, если скрипт передается интерпретатору не через командную строку.

Если запуск интерпретатора разрешен правилами Контроля программ, то компонент не блокирует скрипт, запущенный из этого интерпретатора.
Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами Контроля программ, то компонент блокирует все скрипты, указанные в командной строке интерпретатора.

- Компонент не контролирует запуск скриптов из интерпретаторов, не поддерживаемых программой Kaspersky Endpoint Security.

Kaspersky Endpoint Security поддерживает следующие интерпретаторы:

- Java;
- PowerShell.

Поддерживаются следующие типы интерпретаторов:

- %ComSpec%;
- %SystemRoot%\system32\regedit.exe;
- %SystemRoot%\regedit.exe;
- %SystemRoot%\system32\regedt32.exe;
- %SystemRoot%\system32\cscript.exe;
- %SystemRoot%\system32\wscript.exe;
- %SystemRoot%\system32\msiexec.exe;
- %SystemRoot%\system32\mshta.exe;
- %SystemRoot%\system32\rundll32.exe;
- %SystemRoot%\system32\wwahost.exe;
- %SystemRoot%\syswow64\cmd.exe;
- %SystemRoot%\syswow64\regedit.exe;
- %SystemRoot%\syswow64\regedt32.exe;
- %SystemRoot%\syswow64\cscript.exe;
- %SystemRoot%\syswow64\wscript.exe;
- %SystemRoot%\syswow64\msiexec.exe;
- %SystemRoot%\syswow64\mshta.exe;
- %SystemRoot%\syswow64\rundll32.exe;
- %SystemRoot%\syswow64\wwahost.exe.

Включение и выключение Контроля программ

По умолчанию Контроль программ выключен.

► *Чтобы включить или выключить Контроль программ выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Контроль программ**.
3. Выполните одно из следующих действий:
 - Установите флажок **Контроль программ**, если вы хотите включить Контроль программ.
 - Снимите флажок **Контроль программ**, если вы хотите выключить Контроль программ.
4. Сохраните внесенные изменения.

Действия с правилами Контроля программ

Kaspersky Endpoint Security контролирует запуск программ пользователями с помощью правил. В правиле Контроля программ содержатся условия срабатывания и действия компонента Контроль программ при срабатывании правила (разрешение или запрещение пользователям запускать программу).

Условия срабатывания правила

Условие срабатывания правила представляет собой соответствие "тип условия - критерий условия - значение условия" (см. рис. ниже). На основании условий срабатывания правила Kaspersky Endpoint Security применяет (или не применяет) правило к программе.

Правило Контроля программ

Название правила:

Описание:

Включающие условия:

Критерий условия	Значение условия

+ Добавить | Изменить | Удалить | Сделать исключением

Исключающие условия:

Критерий условия	Значение условия

+ Добавить | Изменить | Удалить | Сделать вкл. условием

Субъекты и их права:

Субъект	Разрешить	Запретить
Все	<input type="checkbox"/>	<input checked="" type="checkbox"/>

+ Добавить | Удалить

Запретить остальным пользователям
 Доверенные программы обновления

OK | Отмена

Рисунок 13. Правило контроля запуска программ. Параметры условия срабатывания правила

В правилах используются включающие и исключающие условия:

- **Включающие условия.** Kaspersky Endpoint Security применяет правило к программе, если программа соответствует хотя бы одному включающему условию.
- **Исключающие условия.** Kaspersky Endpoint Security не применяет правило к программе, если программа соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию.

Условия срабатывания правила формируются с помощью критериев. Для формирования условий в Kaspersky Endpoint Security используются следующие критерии:

- путь к папке с исполняемым файлом программы или путь к исполняемому файлу программы;
- метаданные: название исполняемого файла программы, версия исполняемого файла программы, название программы, версия программы, производитель программы;
- хеш исполняемого файла программы;
- сертификат: издатель, субъект, отпечаток;
- принадлежность программы к KL-категории;
- расположение исполняемого файла программы на съемном диске.

Для каждого критерия, используемого в условии, нужно указать его значение. Если параметры запускаемой программы соответствуют значениям критериев, указанных во включающем условии, правило срабатывает. В этом случае Контроль программ выполняет действие, прописанное в правиле. Если параметры программы соответствуют значениям критериев, указанных в исключающем условии, Контроль программ не контролирует запуск программы.

Решения компонента Контроль программ при срабатывании правила

При срабатывании правила Контроль программ в соответствии с правилом разрешает или запрещает пользователям (группам пользователей) запускать программы. Вы можете выбирать отдельных пользователей или группы пользователей, которым разрешен или запрещен запуск программ, для которых срабатывает правило.

Если в правиле не указан ни один пользователь, которому разрешен запуск программ, удовлетворяющих правилу, правило называется *запрещающим*.

Если в правиле не указан ни один пользователь, которому запрещен запуск программ, удовлетворяющих правилу, правило называется *разрешающим*.

Приоритет запрещающего правила выше приоритета разрешающего правила. Например, если для группы пользователей назначено разрешающее правило Контроля программы и для одного из пользователей этой группы назначено запрещающее правило Контроля программы, то этому пользователю будет запрещен запуск программы.

Статус работы правила

Правила Контроля программ могут иметь один из следующих статусов работы:

- **Вкл.** Статус означает, что правило используется во время работы компонента Контроль программ.
- **Выкл.** Статус означает, что правило не используется во время работы компонента Контроль программ.
- **Тест.** Статус означает, что Kaspersky Endpoint Security разрешает запуск программ, на которые распространяется действие правила, но заносит информацию о запуске этих программ в отчет.

В этом разделе

Добавление условия срабатывания в правило Контроля программ	152
Изменение статуса правила Контроля программ	157
Тестирование правил Контроля программ	157

Добавление и изменение правила Контроля программ

► *Чтобы добавить или изменить правило Контроля программ, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Контроль программ**.
3. Установите флажок **Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. Выполните одно из следующих действий:
 - Если вы хотите добавить правило, нажмите на кнопку **Добавить**.
 - Если вы хотите изменить существующее правило, выберите правило в списке и нажмите на кнопку **Изменить**.

Откроется окно **Правило Контроля программ**.

5. Задайте или измените параметры правила:
 - a. В поле **Название правила** введите или измените название правила.
 - b. В таблице **Включающие условия** сформируйте (см. раздел "Добавление условия срабатывания в правило Контроля программ" на стр. [152](#)) или измените список включающих условий срабатывания правила с помощью кнопок **Добавить**, **Изменить**, **Удалить**, **Сделать исключением**.
 - c. В таблице **Исключающие условия** сформируйте или измените список исключающих условий срабатывания правила с помощью кнопок **Добавить**, **Изменить**, **Удалить**, **Сделать вкл. условием**.
 - d. Если требуется, измените тип условия срабатывания правила:
 - Чтобы сменить тип условия с включающего на исключающее, выберите условие в таблице **Включающие условия** и нажмите на кнопку **Сделать исключением**.
 - Чтобы сменить тип условия с исключающего на включающее, выберите условие в таблице **Исключающие условия** и нажмите на кнопку **Сделать вкл. условием**.
 - e. Задайте или измените список пользователей и / или групп пользователей, которым разрешено или запрещено запускать программы, удовлетворяющие условиям срабатывания правила. Для этого нажмите на кнопку **Добавить** в таблице **Субъекты и их права**.

По умолчанию в список пользователей добавлено значение **Все**. Действие правила распространяется на всех пользователей.

Если в таблице не указан ни один пользователь, правило не может быть сохранено.

- f. В таблице **Субъекты и их права** установите флажки **Разрешить** или **Запретить** напротив пользователей и / или групп пользователей, чтобы определить их право на запуск программ.
Флажок, установленный по умолчанию, зависит от режима работы Контроля программ (см. раздел "О режимах работы Контроля программ" на стр. [159](#)).
- g. Установите флажок **Запретить остальным пользователям**, если вы хотите, чтобы программа запрещала запуск программ, удовлетворяющих условиям срабатывания правила, всем пользователям, которые не указаны в графе **Субъект** и не входят в группы пользователей, указанные в графе **Субъект**.

Если флажок **Запретить остальным пользователям** снят, Kaspersky Endpoint Security не контролирует запуск программ пользователями, которые не указаны в таблице **Субъекты и их права** и не входят в группы пользователей, указанные в таблице **Субъекты и их права**.

- h. Установите флажок **Доверенные программы обновления**, если вы хотите, чтобы программы, удовлетворяющие условиям срабатывания правила, Kaspersky Endpoint Security считал доверенными программами обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.
6. При миграции параметров Kaspersky Endpoint Security осуществляется также миграция списка исполняемых файлов, созданных доверенными программами обновления.
 7. Сохраните внесенные изменения.

Добавление условия срабатывания в правило Контроля программ

► *Чтобы добавить новое условие срабатывания в правило Контроля программ, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Контроль программ**.
В правой части окна отобразятся параметры компонента Контроль программ.
3. Установите флажок **Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. Выполните одно из следующих действий:
 - Если вы хотите создать новое правило и добавить в него условие срабатывания, нажмите на кнопку **Добавить**.
 - Если вы хотите добавить условие срабатывания в существующее правило, выберите его в списке правил и нажмите на кнопку **Изменить**.

Откроется окно **Правило Контроля программ**.

5. В таблице **Включающие условия** или **Исключающие условия** нажмите на кнопку **Добавить**.

С помощью раскрывающегося списка под кнопкой **Добавить** вы можете добавлять в правило различные условия срабатывания (см. инструкции ниже).

► Чтобы добавить условие срабатывания правила на основе свойств файлов в указанной папке, выполните следующие действия:

1. В раскрывающемся списке под кнопкой **Добавить** выберите пункт **Условия из свойств файлов указанной папки**.

Откроется стандартное окно Microsoft Windows **Выбор папки**.

2. В окне **Выбор папки** выберите папку с исполняемыми файлами программ, на основе свойств которых вы хотите сформировать одно или несколько условий срабатывания правила.

3. Нажмите на кнопку **ОК**.

Откроется окно **Добавление условий**.

4. В раскрывающемся списке **Показать критерий** выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Хеш файла**, **Сертификат**, **KL-категория**, **Метаданные** или **Путь к папке**.

Kaspersky Endpoint Security не поддерживает MD5-хеш файла и не контролирует запуск приложений на основе MD5-хеша. В качестве условия срабатывания правила используется SHA256-хеш.

5. Если в раскрывающемся списке **Показать критерий** вы выбрали элемент **Метаданные**, установите флажки напротив тех свойств исполняемых файлов программы, которые вы хотите использовать в условии срабатывания правила: **Название файла**, **Версия файла**, **Название программы**, **Версия программы**, **Производитель**.

Если не выбрано ни одно из указанных свойств, правило не может быть сохранено.

6. Если в раскрывающемся списке **Показать критерий** вы выбрали элемент **Сертификат**, установите флажки напротив тех параметров, которые вы хотите использовать в условии срабатывания правила: **Издатель**, **Субъект**, **Отпечаток**.

Если не выбран ни один из указанных параметров, правило не может быть сохранено.

Не рекомендуется использовать в качестве условий срабатывания правил только критерии **Издатель** и **Субъект**. Использование этих критериев является ненадежным.

7. Установите флажки напротив названий исполняемых файлов программ, свойства которых вы хотите включить в условия срабатывания правила.
8. Нажмите на кнопку **Далее**.
Отобразится список сформированных условий срабатывания правила.
9. В списке сформированных условий срабатывания правила установите флажки около тех условий срабатывания правила, которые вы хотите добавить в правило Контроля программ.
10. Нажмите на кнопку **Завершить**.

► *Чтобы добавить условие срабатывания правила на основе свойств программ, запускавшихся на компьютере, выполните следующие действия:*

1. В раскрывающемся списке под кнопкой **Добавить** выберите пункт **Условия из свойств запускавшихся программ**.
2. В окне **Добавление условий** в раскрывающемся списке **Показать критерий** выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Хеш файла**, **Сертификат**, **KL-категория**, **Метаданные** или **Путь к папке**.

Kaspersky Endpoint Security не поддерживает MD5-хеш файла и не контролирует запуск приложений на основе MD5-хеша. В качестве условия срабатывания правила используется SHA256-хеш.

3. Если в раскрывающемся списке **Показать критерий** вы выбрали элемент **Метаданные**, установите флажки напротив тех свойств исполняемых файлов программы, которые вы хотите использовать в условии срабатывания правила: **Название файла**, **Версия файла**, **Название программы**, **Версия программы**, **Производитель**.

Если не выбрано ни одно из указанных свойств, правило не может быть сохранено.

4. Если в раскрывающемся списке **Показать критерий** вы выбрали элемент **Сертификат**, установите флажки напротив тех параметров, которые вы хотите использовать в условии срабатывания правила: **Издатель**, **Субъект**, **Отпечаток**.

Если не выбран ни один из указанных параметров, правило не может быть сохранено.

Не рекомендуется использовать в качестве условий срабатывания правил только критерии **Издатель** и **Субъект**. Использование этих критериев является ненадежным.

5. Установите флажки напротив названий исполняемых файлов программ, свойства которых вы хотите включить в условия срабатывания правила.
6. Нажмите на кнопку **Далее**.
Отобразится список сформированных условий срабатывания правила.
7. В списке сформированных условий срабатывания правила установите флажки около тех условий срабатывания правила, которые вы хотите добавить в правило Контроля программ.
8. Нажмите на кнопку **Завершить**.

► *Чтобы добавить условие срабатывания правила на основе KL-категории, выполните следующие действия:*

1. В раскрывающемся списке под кнопкой **Добавить** выберите пункт **Условия "KL-категория"**.
KL-категория - сформированный специалистами "Лаборатории Касперского" список программ, обладающих общими тематическими признаками. Например, KL-категория "Офисные программы" включает в себя программы из пакетов Microsoft Office, Adobe® Acrobat® и другие.
2. В окне **Условия "KL-категория"** установите флажки около названий тех KL-категорий, на основе которых вы хотите создать условия срабатывания правила.
3. Нажмите на кнопку **ОК**.

► *Чтобы добавить условие срабатывания правила, сформированное вручную, выполните следующие действия:*

1. В раскрывающемся списке под кнопкой **Добавить** выберите пункт **Условие вручную**.
2. Нажмите на кнопку **Выбрать** в окне **Пользовательское условие** и укажите путь к исполняемому файлу программы.
3. Выберите критерий, на основе которого вы хотите создать условие срабатывания правила: **Хеш файла**, **Сертификат**, **Метаданные** или **Путь к файлу или папке**.

Kaspersky Endpoint Security не поддерживает MD5-хеш файла и не контролирует запуск приложений на основе MD5-хеша. В качестве условия срабатывания правила используется SHA256-хеш.

Если вы используете символьную ссылку в поле **Путь к файлу или папке**, рекомендуется развернуть символьную ссылку для корректной работы правила Контроля программ. Для этого нажмите на кнопку **Развернуть символьную ссылку**.

4. Настройте параметры выбранного критерия.
5. Нажмите на кнопку **ОК**.

► Чтобы добавить условие срабатывания на основе информации о носителе исполняемого файла программы, выполните следующие действия:

1. В раскрывающемся списке под кнопкой **Добавить** выберите пункт **Условие по носителю файла**.
2. В окне **Условие по носителю файла** в раскрывающемся списке **Носитель** выберите тип запоминающего устройства, запуск программ с которого будет условием срабатывания правила.
3. Нажмите на кнопку **ОК**.

Изменение статуса правила Контроля программ

► Чтобы изменить статус правила Контроля программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Контроль программ**.
3. Установите флажок **Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. В графе **Статус** по левой клавише мыши откройте контекстное меню и выберите один из следующих пунктов:
 - **Вкл.** Статус означает, что правило используется во время работы компонента Контроль программ.
 - **Выкл.** Статус означает, что правило не используется во время работы компонента Контроль программ.
 - **Тест.** Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск программ, на которые распространяется действие этого правила, но заносит информацию о запуске этих программ в отчет.

С помощью статуса **Тест** вы можете назначить действие, аналогичное элементу **Тестировать правила** (см. раздел "**Тестирование правил Контроля программ**" на стр. 157), для части правил, при выбранном элементе **Применять правила** в раскрывающемся списке **Действие**.

5. Сохраните внесенные изменения.

Тестирование правил Контроля программ

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля программ и проанализировать их работу.

Для анализа работы правил Контроля программ требуется изучить события по результатам работы компонента Контроль программ, приходящие в Kaspersky Security Center. Если для всех программ, которые необходимы для работы пользователю компьютера, отсутствуют события о запрете запуска в тестовом режиме, то созданы верные правила. В противном случае рекомендуется уточнить параметры созданных вами правил, создать дополнительные или удалить существующие правила.

По умолчанию для правил Контроля программ выбрано действие **Применять правила**.

► *Чтобы включить тестирование правил Контроля программ или выбрать блокирующее действие Контроля программ, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Контроль программ**.
3. Установите флажок **Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. В раскрывающемся списке **Режим контроля** выберите один из следующих элементов:
 - **Черный список**, если вы хотите разрешать запуск всех программ, кроме программ, указанных в запрещающих правилах.
 - **Белый список**, если вы хотите запрещать запуск всех программ, кроме программ, указанных в разрешающих правилах.
5. Выполните одно из следующих действий:
 - Если вы хотите включить тестовый режим для правил Контроля программ, в раскрывающемся списке **Действие** выберите элемент **Тестировать правила**.
 - Если вы хотите включить блокирующий режим для правил Контроля программ, в раскрывающемся списке **Действие** выберите элемент **Применять правила**.
6. Сохраните внесенные изменения.

Kaspersky Endpoint Security не будет блокировать программы, запуск которых запрещен компонентом Контроль программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

Изменение шаблонов сообщений Контроля программ

Когда пользователь пытается запустить программу, запрещенную правилом Контроля программ, Kaspersky Endpoint Security выводит сообщение о блокировке запуска программы. Если блокировка запуска программы, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации.

Для сообщения о блокировке запуска программы и сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

► *Чтобы изменить шаблон сообщения, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Контроль программ**.
3. Установите флажок **Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. Нажмите на кнопку **Шаблоны**.
Откроется окно **Шаблоны сообщений**.
5. Выполните одно из следующих действий:
 - Если вы хотите изменить шаблон сообщения о блокировке запуска программы, выберите закладку **Блокировка**.
 - Если вы хотите изменить шаблон сообщения для администратора локальной сети организации, выберите закладку **Сообщение администратору**.

6. Измените шаблон сообщения о блокировке или сообщения администратору. Для этого используйте кнопки **По умолчанию** и **Переменная**.
7. Сохраните внесенные изменения.

О режимах работы Контроля программ

Компонент Контроль программ может работать в двух режимах:

- **Черный список.** Режим, при котором Контроль программ разрешает пользователям запуск любых программ, кроме тех, которые запрещены в правилах Контроля программ.

Этот режим работы Контроля программ установлен по умолчанию.

- **Белый список.** Режим, при котором Контроль программ запрещает пользователям запуск любых программ, кроме тех, которые разрешены и не запрещены в правилах Контроля программ.

Если разрешающие правила Контроля программ сформированы максимально полно, компонент запрещает запуск всех новых программ, не проверенных администратором локальной сети организации, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

Вы можете ознакомиться с рекомендациями по настройке правил контроля программ в режиме белого списка.

Настройка Контроля программ для работы в этих режимах возможна как в локальном интерфейсе Kaspersky Endpoint Security, так и с помощью Kaspersky Security Center.

Однако Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Kaspersky Endpoint Security и необходимые для следующих задач:

- Создание категорий программ.
Правила Контроля программ, сформированные в Консоли администрирования Kaspersky Security Center, основываются на созданных вами категориях программ, а не на включающих и исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security.
- Получение информации о программах, которые установлены на компьютерах локальной сети организации.

Поэтому настройку работы компонента Контроль программ рекомендуется выполнять с помощью Kaspersky Security Center.

Выбор режима Контроля программ

► *Чтобы выбрать режим Контроля программ, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Контроль программ**.
3. Установите флажок **Контроль программ**, чтобы параметры компонента стали доступными для изменения.

4. В раскрывающемся списке **Режим контроля** выберите один из следующих элементов:
- **Черный список**, если вы хотите разрешать запуск всех программ, кроме программ, указанных в запрещающих правилах;
 - **Белый список**, если вы хотите запрещать запуск всех программ, кроме программ, указанных в разрешающих правилах.

Для режима белого списка изначально задано правило **Операционная система и ее компоненты**, которое разрешает запуск программ, входящих в KL-категорию "Программы ОС", и правило **Доверенные программы обновления**, которое разрешает запуск программ, входящих в KL-категорию "Доверенные программы обновления". В KL-категорию "Программы ОС" входят программы, обеспечивающие нормальную работу операционной системы. В KL-категорию "Доверенные программы обновления" входят программы обновления наиболее известных производителей программного обеспечения. Вы не можете удалить эти правила. Параметры этих правил недоступны для изменения. По умолчанию правило **Операционная система и ее компоненты** включено, а правило **Доверенные программы обновления** выключено. Запуск программ, соответствующих условиям срабатывания этих правил, разрешен всем пользователям.

Все правила, сформированные при выбранном режиме, сохраняются после смены режима для возможности их повторного использования. Чтобы вернуться к использованию этих правил, достаточно выбрать нужный режим в раскрывающемся списке **Режим контроля**.

5. В раскрывающемся списке **Действие** выберите, какое действие компонент должен выполнять при попытке пользователя запустить программу, запрещенную правилами Контроля программ.
6. Установите флажок **Контролировать DLL и драйверы**, если вы хотите, чтобы программа Kaspersky Endpoint Security контролировала загрузку DLL-модулей при запуске пользователями программ.

Информация о модуле и программе, загрузившей этот модуль, будет сохранена в отчет.

Kaspersky Endpoint Security контролирует только DLL-модули и драйверы, загруженные с момента установки флажка **Контролировать DLL и драйверы**. Перезагрузите компьютер после установки флажка **Контролировать DLL и драйверы**, если вы хотите, чтобы программа Kaspersky Endpoint Security контролировала все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.

При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в разделе **Контроль программ** включено правило по умолчанию **Операционная система и ее компоненты** (см. раздел "**Добавление и изменение правила Контроля программ**" на стр. [63](#)) или другое правило, которое содержит KL-категорию "Доверенные сертификаты" и обеспечивает загрузку доверенных DLL-модулей и драйверов до запуска Kaspersky Endpoint Security. Правила Контроля программ, созданные на основе других KL-категорий (за исключением KL-категории "Доверенные сертификаты"), не применяются при контроле загрузки DLL-модулей и драйверов. Включение контроля загрузки DLL-модулей и драйверов при выключенном правиле **Операционная система и ее компоненты** может привести к нестабильности операционной системы.

Рекомендуется включить защиту паролем (см. раздел "Включение Защиты паролем" на стр. [200](#)) для настройки параметров программы, чтобы иметь возможность выключить запрещающие правила, блокирующие запуск критически важных DLL-модулей и драйверов, не изменяя при этом параметры политики Kaspersky Security Center.

7. Сохраните внесенные изменения.

Адаптивный контроль аномалий

Компонент Адаптивный контроль аномалий доступен только для продуктов Kaspersky Endpoint Security для бизнеса Расширенный и Kaspersky Total Security для бизнеса (более подробная информация о продуктах Kaspersky Endpoint Security для бизнеса доступна на сайте "Лаборатории Касперского" <https://www.kaspersky.ru/business-security/small-to-medium-business>).

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Адаптивный контроль аномалий отслеживает и блокирует подозрительные действия, нехарактерные для компьютеров сети организации. Для отслеживания нехарактерных действий Адаптивный контроль аномалий использует набор правил (например, правило *Запуск Windows PowerShell из офисной программы*). Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев вредоносной активности. Вы можете выбрать поведение Адаптивного контроля аномалий для каждого из правил и, например, разрешить запуск PowerShell-скриптов для автоматизации решения корпоративных задач. Kaspersky Endpoint Security обновляет набор правил с базами программы. Обновление набора правил нужно подтверждать вручную (см. раздел "Применение обновлений для правил Адаптивного контроля аномалий" на стр. [170](#)).

Настройка Адаптивного контроля аномалий

Настройка Адаптивного контроля аномалий состоит из следующих этапов:

1. Обучение Адаптивного контроля аномалий.

После включения Адаптивного контроля аномалий правила работают в *обучающем режиме*. В ходе обучения Адаптивный контроль аномалий отслеживает срабатывание правил и отправляет события срабатывания в Kaspersky Security Center. Каждое правило имеет свой срок действия обучающего режима. Срок действия обучающего режима устанавливают специалисты "Лаборатории Касперского". Обычно срок действия обучающего режима составляет 2 недели.

Если в ходе обучения правило ни разу не сработало, Адаптивный контроль аномалий будет считать действия, связанные с этим правилом, подозрительными. Kaspersky Endpoint Security будет блокировать все действия, связанные с этим правилом.

Если в ходе обучения правило сработало, Kaspersky Endpoint Security регистрирует события в отчете о срабатываниях правил (см. раздел "Просмотр отчетов Адаптивного контроля аномалий" на стр. [171](#)) и в хранилище **Срабатывание правил в обучающем режиме**.

2. Анализ отчета о срабатывании правил.

Администратор анализирует отчет о срабатываниях правил (см. раздел "Просмотр отчетов Адаптивного контроля аномалий" на стр. [171](#)) или содержание хранилища **Срабатывание правил в обучающем режиме**. Далее администратор может выбрать поведение Адаптивного контроля аномалий при срабатывании правила: блокировать или разрешить. Также администратор может продолжить отслеживать срабатывание правила и продлить работу программы в обучающем режиме. Если администратор не предпринимает никаких мер, программа также продолжит работать в обучающем режиме. Отсчет срока действия обучающего режима начинается заново.

Настройка Адаптивного контроля аномалий происходит в режиме реального времени. Настройка Адаптивного контроля аномалий осуществляется по следующим каналам:

- Адаптивный контроль аномалий автоматически начинает блокировать действия, связанные с правилами, которые не сработали в течение обучающего режима.
- Kaspersky Endpoint Security добавляет новые правила или удаляет неактуальные.
- Администратор настраивает работу Адаптивного контроля аномалий после анализа отчета о срабатывании правил и содержимого хранилища **Срабатывание правил в обучающем режиме**. Рекомендуется проверять отчет о срабатывании правил и содержимое хранилища **Срабатывание правил в обучающем режиме**.

При попытке вредоносной программы выполнить действие, Kaspersky Endpoint Security заблокирует действие и покажет уведомление (см. рис. ниже).

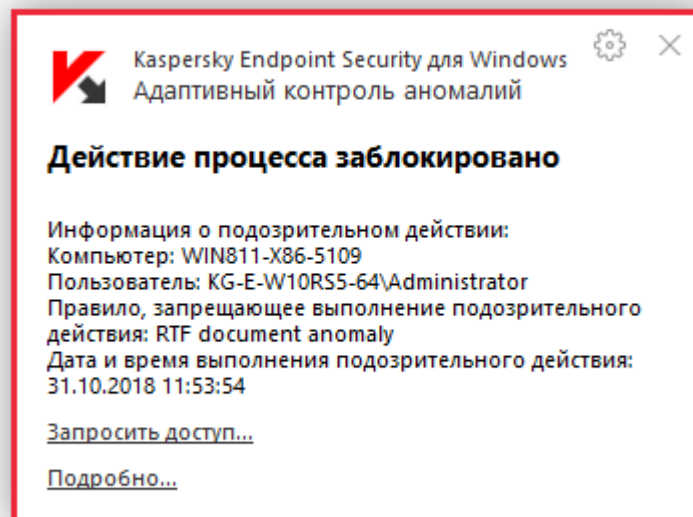


Рисунок 14. Уведомление Адаптивного контроля аномалий

Алгоритм работы Адаптивного контроля аномалий

Kaspersky Endpoint Security принимает решение о выполнении действия, связанного с правилом, по следующему алгоритму (см. рис. ниже).

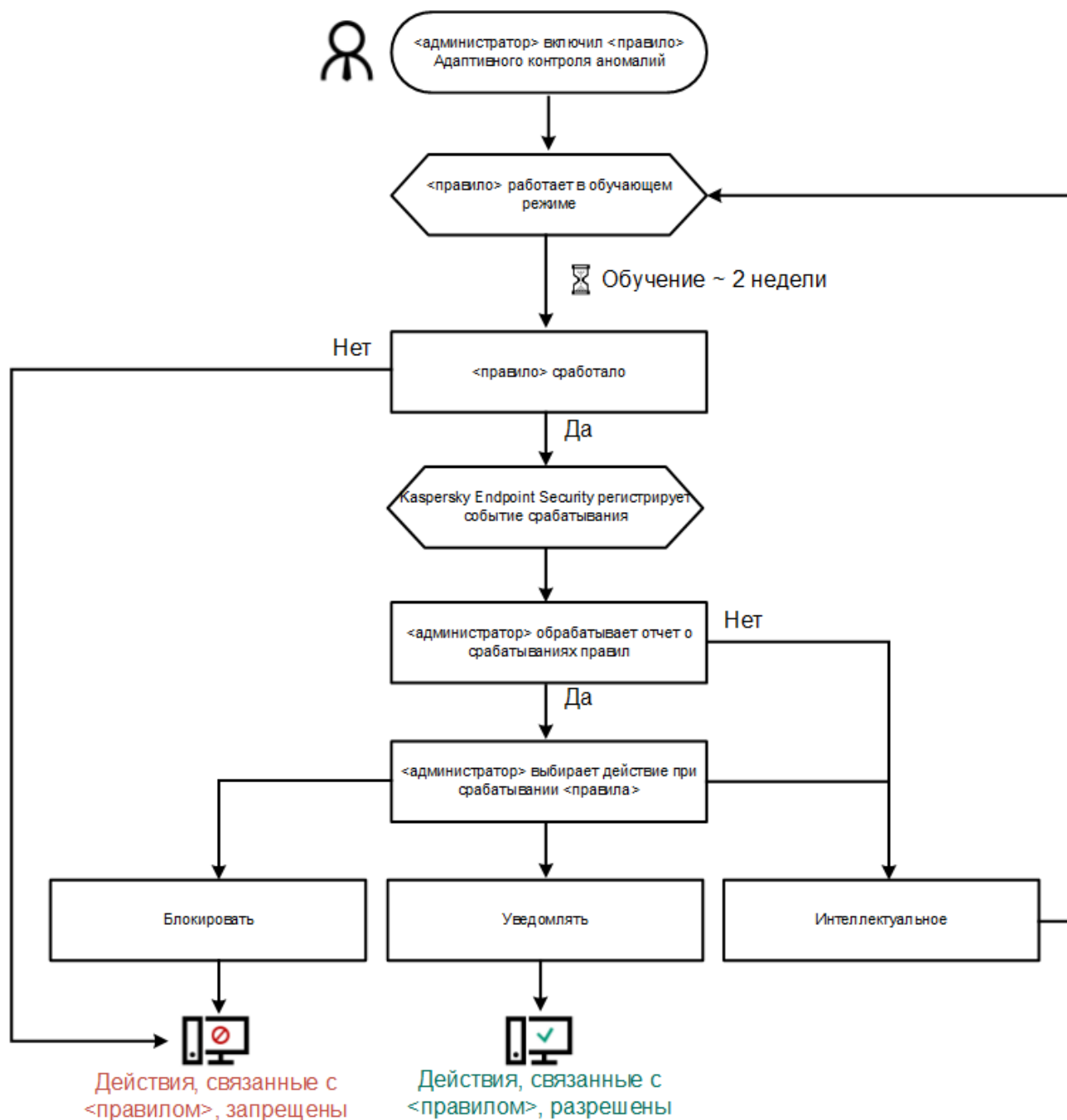


Рисунок 15. Алгоритм работы Адаптивного контроля аномалий

В этом разделе

Включение и выключение Адаптивного контроля аномалий.....	165
Включение и выключение правила Адаптивного контроля аномалий.....	165
Изменение действия при срабатывании правила Адаптивного контроля аномалий.....	166
Создание и изменение исключения для правила Адаптивного контроля аномалий.....	167
Удаление исключения для правила Адаптивного контроля аномалий.....	168
Импорт исключений для правил Адаптивного контроля аномалий.....	169
Экспорт исключений для правил Адаптивного контроля аномалий.....	169
Применение обновлений для правил Адаптивного контроля аномалий.....	170
Изменение шаблонов сообщений Адаптивного контроля аномалий.....	170
Просмотр отчетов Адаптивного контроля аномалий.....	171

Включение и выключение Адаптивного контроля аномалий

По умолчанию Адаптивный контроль аномалий включен.

► *Чтобы включить или выключить Адаптивный контроль аномалий, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. Выполните одно из следующих действий:
 - Установите флажок **Адаптивный контроль аномалий**, если вы хотите включить Адаптивный контроль аномалий.
 - Снимите флажок **Адаптивный контроль аномалий**, если вы хотите выключить Адаптивный контроль аномалий.
4. Сохраните внесенные изменения.

Включение и выключение правила Адаптивного контроля аномалий

► *Чтобы включить или выключить правило Адаптивного контроля аномалий, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Адаптивный контроль аномалий**.

3. В таблице в правой части окна выберите правило.
4. В графе **Статус** по правой клавише мыши откройте контекстное меню и выберите один из следующих пунктов:
 - **Включено.** Статус означает, что правило используется во время работы компонента Адаптивный контроль аномалий.
 - **Выключено.** Статус означает, что правило не используется во время работы компонента Адаптивный контроль аномалий.
5. Сохраните внесенные изменения.

Изменение действия при срабатывании правила Адаптивного контроля аномалий

► Чтобы изменить действие при срабатывании правила Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В таблице в правой части окна выберите правило.
4. В графе **Действие** по правой клавише мыши откройте контекстное меню и выберите один из следующих пунктов:
 - **Интеллектуальное.** Если выбран этот вариант, то правило Адаптивного контроля аномалий работает в обучающем режиме в течение периода, определенного специалистами "Лаборатории Касперского". В этом режиме при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает запись в хранилище **Срабатывание правил в обучающем режиме** Сервера администрирования Kaspersky Security Center. По истечении периода работы обучающего режима Kaspersky Endpoint Security блокирует активность, подпадающую под правило Адаптивного контроля аномалий, и создает в журнале запись, содержащую информацию об этой активности.
 - **Блокировать.** Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security блокирует активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
 - **Информировать.** Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
5. Сохраните внесенные изменения.

Создание и изменение исключения для правила Адаптивного контроля аномалий

Для правил Адаптивного контроля аномалий невозможно создать более 1000 исключений. Не рекомендуется создавать более 200 исключений. Чтобы уменьшить количество используемых исключений, рекомендуется использовать маски в параметрах исключений.

Исключение для правила Адаптивного контроля аномалий включает в себя описание исходных и целевых объектов. *Исходный объект* – объект, который выполняет действия. *Целевой объект* – объект, над которым выполняются действия. Например, вы открыли файл `file.xlsx`. В результате в память компьютера была добавлена библиотека с расширением `dll`, которую использует браузер (исполняемый файл `browser.exe`). В данном примере `file.xlsx` – исходный объект, Excel – исходный процесс, `browser.exe` – целевой объект, Browser – целевой процесс.

► Чтобы создать или изменить исключение для правила Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В таблице в правой части окна выберите правило.
4. Нажмите на кнопку **Изменить**.
Откроется окно **Правило Адаптивного контроля аномалий**.
5. Выполните одно из следующих действий:
 - Если вы хотите добавить исключение, нажмите на кнопку **Добавить**.
 - Если вы хотите изменить существующее исключение, выберите строку в таблице **Исключения** и нажмите на кнопку **Изменить**.
Откроется окно **Исключение из правила**.
6. В поле **Описание** введите описание исключения.
7. Нажмите на кнопку **Обзор** рядом с полем **Пользователь**, чтобы указать пользователей, на которых распространяется исключение.
Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.
8. Задайте параметры исходного объекта или исходного процесса, запущенных объектом:
 - **Исходный процесс**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir*.exe`).
 - **Хеш исходного процесса**. Хеш файла.
 - **Исходный объект**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir*.exe`). Например, путь к файлу `document.docm`, который запускает целевые процессы с помощью скрипта или макроса.

Вы также можете указать другие объекты для исключения, например, веб-адрес, макрос, команду в командной строке, путь реестра и другие. Укажите объект по следующему шаблону: `object://<объект>`, где `<объект>` – название объекта, например, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Вы также можете использовать маски, например, `object://*C:\Windows\temp*`.

- **Хеш исходного объекта.** Хеш файла.

Правило Адаптивного контроля аномалий не распространяется на действия, выполняемые объектом, или на процессы, запущенные объектом.

9. Задайте параметры целевого объекта или целевых процессов, запущенных над объектом.

- **Целевой процесс.** Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir*.exe`).
- **Хеш целевого процесса.** Хеш файла.
- **Целевой объект.** Команда запуска целевого процесса. Укажите команду по следующему шаблону `object://<команда>`, например, `object://cmdline:powershell -Command "$result = 'C:\windows\temp\result_local_users_pwdage.txt'"`. Также вы можете использовать маски, например, `object://*C:\windows\temp*`.
- **Хеш целевого объекта.** Хеш файла.

Правило Адаптивного контроля аномалий не распространяется на действия над объектом или на процессы, запущенные над объектом.

10. Сохраните внесенные изменения.

Удаление исключения для правила Адаптивного контроля аномалий

- Чтобы удалить исключение для правила Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В таблице в правой части окна выберите правило.
4. Нажмите на кнопку **Изменить**.
Откроется окно **Правило Адаптивного контроля аномалий**.
5. В таблице **Исключения из правила** выберите нужную строку.
6. Нажмите на кнопку **Удалить**.
7. Сохраните внесенные изменения.

Импорт исключений для правил Адаптивного контроля аномалий

► Чтобы импортировать исключения для правил Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. Нажмите на кнопку **Импорт**.
Откроется окно **Выбор конфигурационного файла**.
4. В окне **Выбор конфигурационного файла** укажите файл формата XML, из которого вы хотите импортировать список исключений.
5. Нажмите на кнопку **Открыть**.
6. Подтвердите импорт исключений по кнопке **Да**.
7. Сохраните внесенные изменения.

Экспорт исключений для правил Адаптивного контроля аномалий

► Чтобы экспортировать исключения для выбранных правил, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В таблице в правой части окна выберите одно или несколько правил, исключения для которых вы хотите экспортировать.
4. Нажмите на кнопку **Экспорт**.
Откроется окно **Выбор конфигурационного файла**.
5. В окне **Выбор конфигурационного файла** выполните следующие действия:
 - a. Укажите имя файла формата XML, в который вы хотите экспортировать исключения.
 - b. Выберите папку, в которой вы хотите сохранить этот файл.
 - c. Нажмите на кнопку **Сохранить**.
6. В открывшемся диалоговом окне выполните одно из следующих действий:
 - Нажмите на кнопку **Да**, если вы хотите экспортировать исключения только для выбранных правил.
 - Нажмите на кнопку **Нет**, если вы хотите экспортировать исключения для всех правил.
7. Сохраните внесенные изменения.

Применение обновлений для правил Адаптивного контроля аномалий

Новые правила Адаптивного контроля аномалий могут быть добавлены в таблицу правил и существующие правила Адаптивного контроля аномалий могут быть удалены из таблицы правил по результату обновления антивирусных баз. Kaspersky Endpoint Security выделяет удаляемые и добавляемые правила Адаптивного контроля аномалий в таблице, если для этих правил обновление не было применено.

До тех пор, пока обновление не применено, Kaspersky Endpoint Security отображает удаленные в результате обновления правила Адаптивного контроля аномалий в таблице правил и присваивает этим правилам статус *Выключено*. Изменение параметров этих правил невозможно.

► Чтобы применить обновления для правил Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. Нажмите на кнопку **Подтвердить обновления**.

Кнопка **Подтвердить обновления** доступна, если доступно обновление для правил Адаптивного контроля аномалий.

4. Сохраните внесенные изменения.

Изменение шаблонов сообщений Адаптивного контроля аномалий

Когда пользователь пытается выполнить действие, запрещенное правилами Адаптивного контроля аномалий, Kaspersky Endpoint Security выводит сообщение о блокировке потенциально опасных действий. Если блокировка, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации.

Для сообщения о блокировке потенциально опасных действий и сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

► Чтобы изменить шаблон сообщения, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. Установите флажок **Адаптивный контроль аномалий**, чтобы параметры компонента стали доступными для изменения.
4. Нажмите на кнопку **Шаблоны**.

Откроется окно **Шаблоны сообщений**.

5. Выполните одно из следующих действий:
 - Если вы хотите изменить шаблон сообщения о блокировке потенциально опасных действий, выберите закладку **Блокировка**.
 - Если вы хотите изменить шаблон сообщения для администратора локальной сети организации, выберите закладку **Сообщение администратору**.
6. Измените шаблон сообщения о блокировке или сообщения администратору.
7. Сохраните внесенные изменения.

Просмотр отчетов Адаптивного контроля аномалий

► *Чтобы просмотреть отчеты Адаптивного контроля аномалий, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
 2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
 3. В рабочей области выберите закладку **Политики**.
 4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
 5. В разделе **Контроль безопасности** выберите подраздел **Адаптивный контроль аномалий**. В правой части окна отобразятся параметры компонента Адаптивный контроль аномалий.
 6. Выполните одно из следующих действий:
 - Если вы хотите просмотреть отчет о параметрах правил Адаптивного контроля аномалий, нажмите на кнопку **Отчет о состоянии правил**.
 - Если вы хотите просмотреть отчет о срабатываниях правил Адаптивного контроля аномалий, нажмите на кнопку **Отчет о срабатываниях правил**.
 7. Запустится процесс формирования отчета.
- Отчет отобразится в новом окне.

Веб-Контроль

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Веб-Контроль управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть веб-сайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security заблокирует доступ или покажет предупреждение (см. рис. ниже).

Kaspersky Endpoint Security контролирует только HTTP- и HTTPS-трафик.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений (см. раздел "Включение и выключение проверки защищенных соединений" на стр. [191](#)).

Способы управления доступом к веб-сайтам

Веб-Контроль позволяет настраивать доступ к веб-сайтам следующими способами:

- **Категория веб-сайта.** Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз программы). Вы можете ограничить доступ пользователей, например, к категории "Социальные сети" или другим категориям (см. раздел "Приложение 2. Категории содержания веб-ресурсов" на стр. [344](#)).
- **Тип данных.** Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Kaspersky Endpoint Security определяет тип данных по формату файла, а не по расширению.

Kaspersky Endpoint Security не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, Kaspersky Endpoint Security определит тип данных "Архивы", а не "Графические файлы".

- **Отдельный адрес.** Вы можете ввести веб-адрес или использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. [174](#)).

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к типу данных "Файлы офисных программ" только для категории веб-сайтов "Веб-почта".

Правила доступа к веб-сайтам

Веб-Контроль управляет доступом пользователей к веб-сайтам с помощью *правил доступа*. Вы можете настроить следующие дополнительные параметры правила доступа к веб-сайтам:

- Пользователи, на которых распространяется правило.
Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.
- Расписание работы правила.
Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Приоритеты правил доступа

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом. Например, Kaspersky Endpoint Security может определить корпоративный портал как социальную сеть. Чтобы ограничить доступ к социальным сетям и предоставить доступ к корпоративному веб-порталу, создайте два правила: запрещающее правило для категории веб-сайтов "Социальные сети" и разрешающее правило для корпоративного веб-портала. Правило доступа к корпоративному веб-порталу должно иметь приоритет выше, чем правило доступа к социальным сетям.

**Kaspersky
Endpoint Security для Windows**

ДОСТУП ЗАПРЕЩЕН

Запрашиваемая веб-страница не может быть предоставлена.

Адрес: <http://kaspersky.ru/>.

Веб-страница заблокирована правилом "TestRule 90e30b7d-125e-4aef-9d00-f6c375ba5c15".

Причина: принадлежность веб-ресурса к категории(ям) содержания "Неизвестное содержание" и категории(ям) типа данных "Неизвестные данные".

Этот веб-ресурс запрещен в организации. В случае ошибочной блокировки и / или необходимости доступа к веб-ресурсу обратитесь к администратору локальной сети организации ([Запросить доступ](#)).

Сообщение создано: 01.02.2019 21:48:26

**Kaspersky
Endpoint Security для Windows**

ПРЕДУПРЕЖДЕНИЕ

Запрашиваемая веб-страница, возможно, небезопасна или не разрешена политикой организации.

Адрес: <http://kaspersky.ru/>.

Веб-страница заблокирована правилом "TestRule 357871d2-5820-47ac-95c1-59a7226e0417".

Причина: принадлежность веб-ресурса к категории(ям) содержания "Неизвестное содержание" и категории(ям) типа данных "Неизвестные данные".

Перейдите по ссылке <http://kaspersky.ru/>, чтобы открыть запрошенную веб-страницу.
Перейдите по ссылке <http://kaspersky.ru/> для получения доступа ко всему содержимому веб-сайта, на котором расположена запрошенная веб-страница.
Перейдите по ссылке [*://*.kaspersky.ru/](http://*.kaspersky.ru/) для получения доступа ко всем существующим доменам уровня, ниже или равного уровню, отмеченного «*».

Доступ к перечисленным веб-ресурсам будет разрешен в рамках текущей сессии работы Kaspersky Endpoint Security.
В случае ошибочного предупреждения обратитесь к администратору локальной сети организации ([Запросить доступ](#)).

Сообщение создано: 01.02.2019 21:46:17

В этом разделе

Включение и выключение Веб-Контроля.....	174
Правила формирования масок адресов веб-ресурсов	174
Действия с правилами доступа к веб-ресурсам.....	177
Экспорт и импорт списка адресов веб-ресурсов	181
Мониторинг активности пользователей в интернете.....	183
Изменение шаблонов сообщений Веб-Контроля.....	184

Включение и выключение Веб-Контроля

По умолчанию Веб-Контроль включен.

► Чтобы включить или выключить Веб-Контроль, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Веб-Контроль**.
3. Выполните одно из следующих действий:
 - Установите флажок **Веб-Контроль**, если вы хотите включить Веб-Контроль.
 - Снимите флажок **Веб-Контроль**, если вы хотите выключить Веб-Контроль.Если Веб-Контроль выключен, Kaspersky Endpoint Security не контролирует доступ к веб-ресурсам.
4. Сохраните внесенные изменения.

Правила формирования масок адресов веб-ресурсов

Использование *маски адреса веб-ресурса* (далее также "маски адреса") может быть удобно в случаях, когда в процессе создания правила доступа к веб-ресурсам требуется ввести множество схожих адресов веб-ресурсов. Одна грамотно сформированная маска адреса может заменить множество адресов веб-ресурсов.

При формировании маски адреса следует использовать следующие правила:

1. Символ * заменяет любую последовательность из нуля или более символов.
Например, при вводе маски адреса *abc* правило доступа к веб-ресурсам применяется ко всем адресам, содержащим последовательность abc. Пример:
http://www.example.com/page_0-9abcdef.html.
Для включения символа * в состав маски адреса требуется вводить два символа * .
2. Последовательность символов www . в начале маски адреса трактуется как последовательность * . .
Пример: маска адреса www.example.com трактуется как *.example.com.
3. Если маска адреса начинается не с символа * , то содержание маски адреса эквивалентно тому же содержанию с префиксом * . .
4. Последовательность символов * . в начале маски трактуется как * . или пустая строка.
Пример: под действие маски адреса http://www.*.example.com попадает адрес <http://www2.example.com>.
5. Если маска адреса заканчивается символом, отличным от / или * , то содержание маски адреса эквивалентно тому же содержанию с постфиксом /* .
Пример: под действие маски адреса <http://www.example.com> попадают адреса вида <http://www.example.com/abc>, где a, b, c – любые символы.
6. Если маска адреса заканчивается символом / , то содержание маски адреса эквивалентно тому же содержанию с постфиксом /* .
7. Последовательность символов /* в конце маски адреса трактуется как /* или пустая строка.

8. Проверка адресов веб-ресурсов по маске адреса осуществляется с учетом схемы (http или https):
 - Если сетевой протокол в маске адреса отсутствует, то под действие маски адреса попадает адрес с любым сетевым протоколом.
Пример: под действие маски адреса example.com попадают адреса <http://example.com> и <https://example.com>.
 - Если сетевой протокол в маске адреса присутствует, то под действие маски адреса попадают только адреса с таким же сетевым протоколом, как у маски адреса.
Пример: под действие маски адреса http://*.example.com попадает адрес <http://www.example.com> и не попадает адрес <https://www.example.com>.
9. Маска адреса, заключенная в двойные кавычки, трактуется без учета каких-либо дополнительных подстановок, за исключением символа *, если он изначально включен в состав маски адреса. Для масок адреса, заключенных в двойные кавычки, не выполняются правила 5 и 7 (см. примеры 14 – 18 в таблице ниже).
10. При сравнении с маской адреса веб-ресурса не учитываются имя пользователя и пароль, порт соединения и регистр символов.

Таблица 2. Примеры применения правил формирования масок адресов

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
1	*.example.com	http://www.123example.com	Нет	См. правило 1.
2	*.example.com	http://www.123.example.com	Да	См. правило 1.
3	*example.com	http://www.123example.com	Да	См. правило 1.
4	*example.com	http://www.123.example.com	Да	См. правило 1.
5	http://www.*.example.com	http://www.123example.com	Нет	См. правило 1.
6	www.example.com	http://www.example.com	Да	См. правила 2, 1.
7	www.example.com	https://www.example.com	Да	См. правила 2, 1.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Да	См. правила 2, 5, 1.
10	example.com	http://www.example.com	Да	См. правила 3, 1.
11	http://example.com/	http://example.com/abc	Да	См. правила 6.
12	http://example.com/*	http://example.com	Да	См. правило 7.
13	http://example.com	https://example.com	Нет	См. правило 8.
14	"example.com"	http://www.example.com	Нет	См. правило 9.
15	"http://www.example.com"	http://www.example.com/abc	Нет	См. правило 9.
16	"*.example.com"	http://www.example.com	Да	См. правила 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Да	См. правила 1, 9.
18	"www.example.com"	http://www.example.com ; https://www.example.com	Да	См. правила 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Нет	Маска адреса содержит больше информации, чем адрес веб-ресурса.

Действия с правилами доступа к веб-ресурсам

Не рекомендуется создавать более 1000 правил доступа к веб-ресурсам, поскольку это может привести к нестабильности системы.

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое Kaspersky Endpoint Security выполняет при посещении пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют точно задать круг веб-ресурсов, доступ к которым контролирует компонент Веб-Контроль.

Доступны следующие фильтры:

- **Фильтр по содержанию.** Веб-Контроль разделяет веб-ресурсы по категориям содержания (см. раздел "Приложение 2. Категории содержания веб-ресурсов" на стр. 344) и категориям типа данных. Вы можете контролировать доступ пользователей к размещенным на веб-ресурсах данным, относящимся к определенными этими категориями типам данных. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории содержания и / или категории типа данных, Kaspersky Endpoint Security выполняет действие, указанное в правиле.
- **Фильтр по адресам веб-ресурсов.** Вы можете контролировать доступ пользователей ко всем адресам веб-ресурсов или к отдельным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

Если задан и фильтр по содержанию, и фильтр по адресам веб-ресурсов, и заданные адреса веб-ресурсов и / или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типа данных, Kaspersky Endpoint Security контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и / или категорий типа данных, а только к заданным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

- **Фильтр по именам пользователей и групп пользователей.** Вы можете задавать пользователей и / или группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом.
- **Расписание работы правила.** Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда Kaspersky Endpoint Security контролирует доступ к веб-ресурсам, указанным в правиле.

После установки программы Kaspersky Endpoint Security список правил компонента Веб-Контроль не пуст. Предустановлены два правила:

- Правило "Сценарии и таблицы стилей", которое разрешает всем пользователям в любое время доступ к веб-ресурсам, адреса которых содержат названия файлов с расширением css, js, vbs. Например: <http://www.example.com/style.css>, <http://www.example.com/style.css?mode=normal>.
- "Правило по умолчанию". Это правило в зависимости от выбранного действия разрешает или запрещает всем пользователям доступ ко всем веб-ресурсам, которые не попадают под действие других правил.

В этом разделе

Добавление и изменение правила доступа к веб-ресурсам	178
Назначение приоритета правилам доступа к веб-ресурсам.....	180
Проверка работы правил доступа к веб-ресурсам	180
Включение и выключение правила доступа к веб-ресурсам	181

Добавление и изменение правила доступа к веб-ресурсам

► *Чтобы добавить или изменить правило доступа к веб-ресурсам, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Веб-Контроль**.
3. Выполните одно из следующих действий:
 - Если вы хотите добавить правило, нажмите на кнопку **Добавить**.
 - Если вы хотите изменить правило, выберите правило в таблице и нажмите на кнопку **Изменить**.Откроется окно **Правило доступа к веб-ресурсам**.
4. Задайте или измените параметры правила. Для этого выполните следующие действия:
 - a. В поле **Название** введите или измените название правила.
 - b. В раскрывающемся списке **Фильтровать содержание** выберите нужный элемент:
 - **Любое содержание**.
 - **По категориям содержания**.
 - **По типам данных**.
 - **По категориям содержания и типам данных**.
 - c. Если выбран элемент, отличный от **Любое содержание**, откроются блоки для выбора категорий содержания и / или типов данных. Установите флажки напротив названий желаемых категорий содержания и / или типов данных.

Установка флажка напротив названия категории содержания и / или типа данных означает, что Kaspersky Endpoint Security, в соответствии с правилом, контролирует доступ к веб-ресурсам, принадлежащим к выбранным категориям содержания и / или типам данных.
 - d. В раскрывающемся списке **Применять к адресам** выберите нужный элемент:
 - **Ко всем адресам**.
 - **К отдельным адресам**.
 - e. Если выбран элемент **К отдельным адресам**, откроется блок, в котором требуется создать список адресов веб-ресурсов. Вы можете добавлять или изменять адреса и / или группы адресов веб-ресурсов, используя кнопки **Добавить**, **Изменить**, **Удалить**.

Если Проверка защищенных соединений отключена, для протокола https доступна фильтрация только по имени сервера.

- f. В раскрываемом списке **Применять к адресам** выберите нужный элемент:
- **Ко всем пользователям.**
 - **К отдельным пользователям или группам.**
- g. Если выбран элемент **К отдельным пользователям или группам**, откроется блок, в котором вы можете создать список пользователей и / или групп пользователей, доступ которых к веб-ресурсам, описанным в правиле, регулируется этим правилом. Вы можете добавлять или удалять пользователей и / или группы пользователей, используя кнопки **Добавить**, **Удалить**. По кнопке **Добавить** открывается стандартное окно Microsoft Windows **Выбор пользователей или групп**.
- h. Из раскрываемого списка **Действие** выберите нужный элемент:
- **Разрешать.** Если выбрано это значение, то Kaspersky Endpoint Security разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
 - **Запрещать.** Если выбрано это значение, то Kaspersky Endpoint Security запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
 - **Предупреждать.** Если выбрано это значение, то при попытке доступа к веб-ресурсам, удовлетворяющим правилу, Kaspersky Endpoint Security выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
- i. Выберите из раскрываемого списка **Расписание работы правила** название нужного расписания или сформируйте новое расписание на основе выбранного расписания работы правила. Для этого выполните следующие действия:
- i. Нажмите на кнопку **Настройка** напротив раскрываемого списка **Расписание работы правила**.
Откроется окно **Расписание работы правила**.
 - ii. Чтобы добавить в расписание работы правила интервал времени, в течение которого правило не работает, в таблице с изображением расписания работы правила левой клавишей мыши выберите ячейки таблицы, соответствующие нужному вам времени и дню недели.
Цвет ячеек изменится на серый.
 - iii. Чтобы в расписании работы правила изменить интервал времени, в течение которого правило работает, на интервал времени, в течение которого правило не работает, левой клавишей мыши выберите серые ячейки таблицы, соответствующие нужному вам времени и дню недели.
Цвет ячеек изменится на зеленый.
 - iv. Нажмите на кнопку **Сохранить как**.
Откроется окно **Название расписания работы правила**.
 - v. Введите название расписания работы правила или оставьте название, предложенное по умолчанию.
 - vi. Нажмите на кнопку **ОК**.
5. Сохраните внесенные изменения.

Назначение приоритета правилам доступа к веб-ресурсам

Вы можете назначить приоритет каждому правилу из списка правил, расположив их в определенном порядке.

► *Чтобы назначить правилам доступа к веб-ресурсам приоритет, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Веб-Контроль**.
3. В правой части окна выберите правило, приоритет которого вы хотите изменить.
4. С помощью кнопок **Вверх** и **Вниз** переместите правило на желаемую позицию в списке правил.
5. Повторите действие пунктов инструкции 3-4 для тех правил, приоритет которых вы хотите изменить.
6. Сохраните внесенные изменения.

Проверка работы правил доступа к веб-ресурсам

Чтобы оценить, насколько согласованы правила Веб-Контроля, вы можете проверить их работу. Для этого в рамках компонента Веб-Контроль предусмотрена функция "Диагностика правил".

► *Чтобы проверить работу правил доступа к веб-ресурсам, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Веб-Контроль**.
3. В правой части окна нажмите на кнопку **Диагностика**.
Откроется окно **Диагностика правил**.
4. Заполните поля в блоке **Условия**:
 - a. Установите флажок **Укажите адрес**, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к определенному веб-ресурсу. В поле ниже введите адрес веб-ресурса.
 - b. Задайте список пользователей и / или групп пользователей, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к веб-ресурсам для определенных пользователей и / или групп пользователей.
 - c. Из раскрывающегося списка **Фильтровать содержание** выберите нужный элемент (**По категориям содержания**, **По типам данных** или **По категориям содержания и типам данных**), если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к веб-ресурсам определенных категорий содержания и / или категорий типа данных.
 - d. Установите флажок **Учитывать время попытки доступа**, если вы хотите проверить работу правил с учетом дня недели и времени совершения попытки доступа к веб-ресурсам, указанным в условиях диагностики правил. Далее укажите день недели и время.
5. Нажмите на кнопку **Проверить**.

В результате проверки выводится сообщение о действии Kaspersky Endpoint Security в соответствии с первым сработавшим правилом при попытке доступа к заданному веб-ресурсу (разрешение, запрет, предупреждение). Первым срабатывает правило, которое находится в списке правил Веб-Контроля выше других правил, удовлетворяющих условиям диагностики. Сообщение выводится справа от кнопки **Проверить**. В таблице ниже выводится список остальных сработавших правил с указанием действия, которое выполняет Kaspersky Endpoint Security. Правила выводятся в порядке убывания приоритета.

Включение и выключение правила доступа к веб-ресурсам


► *Чтобы включить или выключить правило доступа к веб-ресурсам, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Веб-Контроль**.
3. В правой части окна выберите правило, которое вы хотите включить или выключить.
4. В графе **Статус** выполните следующие действия:
 - Если вы хотите включить использование правила, выберите значение *Вкл.*
 - Если вы хотите выключить использование правила, выберите значение *Выкл.*
5. Сохраните внесенные изменения.

Экспорт и импорт списка адресов веб-ресурсов

Если в правиле доступа к веб-ресурсам вы сформировали список адресов веб-ресурсов, вы можете экспортировать его в файл формата TXT. В дальнейшем вы можете импортировать список из этого файла, чтобы при настройке правила не создавать список адресов веб-ресурсов вручную. Возможность экспорта и импорта списка адресов веб-ресурсов может понадобиться, например, если вы создаете правила со сходными параметрами.

► *Чтобы экспортировать список адресов веб-ресурсов в файл, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Веб-Контроль**.
3. Выберите правило, список адресов веб-ресурсов которого вы хотите экспортировать в файл.
4. Нажмите на кнопку **Изменить**.
Откроется окно **Правило доступа к веб-ресурсам**.
5. Если вы хотите экспортировать не весь список адресов веб-ресурсов, а только его часть, выделите нужные вам адреса веб-ресурсов.
6. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.
Откроется окно подтверждения действия.

7. Выполните одно из следующих действий:

- Если вы хотите экспортировать только выделенные элементы списка адресов веб-ресурсов, в окне подтверждения действия нажмите на кнопку **Да**.
- Если вы хотите экспортировать все элементы списка адресов веб-ресурсов, в окне подтверждения действия нажмите на кнопку **Нет**.

Откроется стандартное окно Microsoft Windows **Сохранить как**.

8. В окне Microsoft Windows **Сохранить как** выберите файл, в который вы хотите экспортировать список адресов веб-ресурсов, и нажмите на кнопку **Сохранить**.

► *Чтобы импортировать в правило список адресов веб-ресурсов из файла, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.

2. В окне параметров программы выберите раздел **Контроль безопасности** → **Веб-Контроль**.


3. Выполните одно из следующих действий:

- Нажмите на кнопку **Добавить**, если вы хотите создать новое правило доступа к веб-ресурсам.
- Выберите правило доступа к веб-ресурсам, которое вы хотите изменить. Далее нажмите на кнопку **Изменить**.

Откроется окно **Правило доступа к веб-ресурсам**.

4. Выполните одно из следующих действий:

- Если вы создаете новое правило доступа к веб-ресурсам, в раскрывающемся списке **Применять к адресам** выберите элемент **К отдельным адресам**.
- Если вы изменяете правило доступа к веб-ресурсам, перейдите к пункту 5 инструкции.

5. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.

Если вы создаете новое правило, откроется стандартное окно Microsoft Windows **Открыть файл**.

Если вы изменяете правило, откроется окно подтверждения действия.

6. Выполните одно из следующих действий:

- Если вы создаете новое правило доступа к веб-ресурсам, перейдите к пункту 7 инструкции.
- Если вы изменяете правило доступа к веб-ресурсам, в окне подтверждения действия выполните одно из следующих действий:
 - Если вы хотите добавить к существующим импортируемые элементы списка адресов веб-ресурсов, нажмите на кнопку **Да**.
 - Если вы хотите удалить существующие элементы списка адресов веб-ресурсов и добавить импортируемые, нажмите на кнопку **Нет**.

Откроется стандартное окно Microsoft Windows **Открыть файл**.

7. В окне Microsoft Windows **Открыть файл** выберите файл со списком адресов веб-ресурсов для импорта.

8. Нажмите на кнопку **Открыть**.




9. В окне **Правило доступа к веб-ресурсам** нажмите на кнопку **ОК**.

Мониторинг активности пользователей в интернете

Kaspersky Endpoint Security позволяет записывать данные о посещении пользователями всех веб-сайтов, в том числе и разрешенных. Таким образом, вы можете получить полную историю просмотров в браузере. Kaspersky Endpoint Security отправляет события активности пользователя в Kaspersky Security Center, локальный журнал Kaspersky Endpoint Security (см. раздел "Работа с отчетами" на стр. 272), журнал событий Windows. Для получения событий в Kaspersky Security Center нужно настроить параметры событий в политике в Консоли администрирования или Web Console. Также вы можете настроить отправку событий Веб-Контроля по электронной почте и отображение уведомлений на экране компьютера пользователя.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений (см. раздел "Включение и выключение проверки защищенных соединений" на стр. 191).

Kaspersky Endpoint Security создает следующие события активности пользователя в интернете:

- блокировка веб-сайта (статус *Критические события* );
- предупреждение о нежелательном веб-сайте (статус *Предупреждения* );
- посещение разрешенного веб-сайта (статус *Информационные сообщения* ).

► Чтобы настроить запись событий Веб-Контроля на компьютере пользователя, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Настройка**.
4. В открывшемся окне выберите раздел **Веб-Контроль**.
Откроется таблица событий Веб-Контроля и способов уведомлений.
5. Настройте для каждого события способ уведомления: **Сохранять в локальном журнале** и **Сохранять в журнале событий Windows**.

Для записи событий посещения разрешенных веб-сайтов нужно дополнительно настроить Веб-Контроль (см. инструкцию ниже).

Также в таблице событий вы можете включить уведомление на экране и уведомление по электронной почте. Для отправки уведомлений по почте нужно настроить параметры SMTP-сервера. Подробнее об отправке уведомлений по почте см. в справке Kaspersky Security Center <https://help.kaspersky.com/KSC/11/ru-RU/>.

6. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security начинает записывать события активности пользователя в интернете.

Веб-Контроль отправляет события активности пользователя в Kaspersky Security Center следующим образом:

- Если вы используете Kaspersky Security Center, Веб-Контроль отправляет события по всем объектам, из которых состоит веб-страница. Поэтому при блокировании одной веб-страницы может быть создано несколько событий. Например, при блокировании веб-страницы <http://www.example.com> Kaspersky Endpoint Security может отправить события по следующим объектам: <http://www.example.com>, <http://www.example.com/icon.ico>, <http://www.example.com/file.js> и так далее.
 - Если вы используете Kaspersky Security Center Cloud Console, Веб-Контроль группирует события и отправляет только протокол и домен веб-сайта. То есть, если пользователь открыл нежелательные веб-страницы <http://www.example.com/main>, <http://www.example.com/contact>, <http://www.example.com/gallery>, Kaspersky Endpoint Security отправит только одно событие с объектом <http://www.example.com>.
- *Чтобы включить запись событий посещения разрешенных веб-сайтов, выполните следующие действия:*
1. В главном окне программы нажмите на кнопку **Настройка**.
 2. В окне параметров программы выберите раздел **Контроль безопасности** → **Веб-Контроль**.
 3. Нажмите на кнопку **Дополнительные параметры**.
 4. В открывшемся окне установите флажок **Записывать данные о посещении разрешенных страниц в журнал**.
 5. Сохраните внесенные изменения.
- В результате вам будет доступна полная история просмотров в браузере.

Изменение шаблонов сообщений Веб-Контроля

В зависимости от действия, заданного в свойствах правил Веб-Контроля, при попытке пользователей получить доступ к веб-ресурсам Kaspersky Endpoint Security выводит сообщение (подменяет ответ HTTP-сервера HTML-страницей с сообщением) одного из следующих типов:

- Сообщение-предупреждение. Такое сообщение предупреждает пользователя о том, что посещение веб-ресурса не рекомендуется и / или не соответствует корпоративной политике безопасности. Kaspersky Endpoint Security выводит сообщение-предупреждение, если в параметрах правила, описывающего этот веб-ресурс, в раскрываемом списке **Действие** выбран элемент **Предупреждать**.

Если, по мнению пользователя, предупреждение ошибочно, по ссылке из предупреждения пользователь может отправить уже сформированное сообщение администратору локальной сети организации.

- Сообщение о блокировке веб-ресурса. Kaspersky Endpoint Security выводит сообщение о блокировке веб-ресурса, если в параметрах правила, которое описывает этот веб-ресурс, в раскрываемом списке **Действие** выбран элемент **Запрещать**.

Если блокировка доступа к веб-ресурсу, по мнению пользователя, была ошибочна, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить уже сформированное сообщение администратору локальной сети организации.

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и сообщения для отправки администратору локальной сети организации предусмотрены шаблоны. Вы можете изменять их содержание.

► *Чтобы изменить шаблон сообщений Веб-Контроля, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Контроль безопасности** → **Веб-Контроль**.
3. В правой части окна нажмите на кнопку **Шаблоны**.
Откроется окно **Шаблоны сообщений**.
4. Выполните одно из следующих действий:
 - Если вы хотите изменить шаблон сообщения для пользователя о том, что веб-ресурс не рекомендован для посещения, выберите закладку **Предупреждение**.
 - Если вы хотите изменить шаблон сообщения о блокировке доступа к веб-ресурсу, выберите закладку **Блокировка**.
 - Если вы хотите изменить шаблон сообщения администратору, выберите закладку **Сообщение администратору**.
5. Измените шаблон сообщения. При этом вы можете использовать раскрывающийся список **Переменная**, а также кнопки **По умолчанию** и **Ссылка** (кнопка не доступна на закладке **Сообщение администратору**).
6. Сохраните внесенные изменения.

Контроль сетевого трафика

Контроль сетевых портов

Во время работы Kaspersky Endpoint Security компоненты Веб-Контроль (на стр. [172](#)), Защита от почтовых угроз (на стр. [130](#)), Защита от веб-угроз (на стр. [124](#)) контролируют потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP- и UDP-порты компьютера пользователя. Например, компонент Защита от почтовых угроз анализирует информацию, передаваемую по SMTP-протоколу, а компонент Защита от веб-угроз анализирует информацию, передаваемую по протоколам HTTP и FTP.

Kaspersky Endpoint Security подразделяет TCP- и UDP-порты компьютера пользователя на несколько групп в соответствии с вероятностью их взлома. Сетевые порты, отведенные для уязвимых служб, рекомендуется контролировать более тщательно, так как эти сетевые порты с большей вероятностью могут являться целью сетевой атаки. Если вы используете нестандартные службы, которым отведены нестандартные сетевые порты, эти сетевые порты также могут являться целью для атакующего компьютера. Вы можете задать список сетевых портов и список программ, запрашивающих сетевой доступ, на которые компоненты Защита от почтовых угроз и Защита от веб-угроз должны обращать особое внимание во время слежения за сетевым трафиком.

Проверка защищенных соединений (HTTPS)

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов. Также Kaspersky Endpoint Security включает использование системного хранилища доверенных сертификатов в программах Firefox и Thunderbird для проверки трафика этих программ.

Компоненты Веб-Контроль (на стр. [172](#)), Защита от почтовых угроз (на стр. [130](#)), Защита от веб-угроз (на стр. [124](#)) могут расшифровывать и проверять сетевой трафик, передаваемый по защищенным соединениям с использованием следующих протоколов:

- SSL 3.0;
- TLS 1.0, TLS 1.1, TLS 1.2.

В этом разделе

Контроль сетевых портов.....	187
Проверка защищенных соединений.....	191

Контроль сетевых портов

Вы можете выполнить следующие действия для настройки параметров контроля сетевого трафика:

- Включить контроль всех сетевых портов.
- Сформировать список контролируемых сетевых портов.
- Сформировать список программ, для которых контролируются все сетевые порты.

В этом разделе

Включение контроля всех сетевых портов	187
Включение контроля портов для программ из списка, сформированного специалистами "Лаборатории Касперского"	187
Формирование списка контролируемых сетевых портов	189
Формирование списка программ, для которых контролируются все сетевые порты	189

Включение контроля всех сетевых портов

► *Чтобы включить контроль всех сетевых портов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать все сетевые порты**.
4. Сохраните внесенные изменения.

Включение контроля портов для программ из списка, сформированного специалистами "Лаборатории Касперского"

► *Чтобы сформировать список контролируемых сетевых портов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.
4. Нажмите на кнопку **Настройка**.
Откроется окно **Сетевые порты**.
5. Установите флажок **Контролировать все порты для программ из списка, рекомендованного "Лабораторией Касперского"**.

Если установлен этот флажок, Kaspersky Endpoint Security контролирует все порты для следующих программ:

- Adobe Reader.
- AIM for Windows.
- Apple Application Support.
- Chrome.
- Digsby.
- Edge.
- Firefox.
- Google Talk.
- ICQ.
- Internet Explorer.
- Java.
- Mail.ru Агент.
- Miranda IM.
- mIRC.
- Opera.
- Pidgin.
- QIP Infium.
- QIP.
- QNext.
- QNextClient.
- Rockmelt.
- Safari.
- Simple Instant Messenger.
- Trillian.
- Windows Live Messenger.
- Windows Messenger.
- X-Chat.
- Yahoo! Messenger.
- Яндекс.Браузер.

Формирование списка контролируемых сетевых портов

► Чтобы сформировать список контролируемых сетевых портов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.
4. Нажмите на кнопку **Настройка**.

Откроется окно **Сетевые порты**. В окне **Сетевые порты** находится список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика. Этот список сетевых портов включен в поставку Kaspersky Endpoint Security.

5. В списке сетевых портов выполните следующие действия:
 - Установите флажки напротив названий тех сетевых портов, которые вы хотите включить в список контролируемых сетевых портов.
По умолчанию флажки установлены для всех сетевых портов, представленных в окне **Сетевые порты**.
 - Снимите флажки напротив названий тех сетевых портов, которые вы хотите исключить из списка контролируемых сетевых портов.
6. Если сетевой порт отсутствует в списке сетевых портов, добавьте его следующим образом:
 - a. По ссылке **Добавить**, расположенной под списком сетевых портов, откройте окно **Сетевой порт**.
 - b. В поле **Порт** введите номер сетевого порта.
 - c. В поле **Описание** введите название сетевого порта.
 - d. Нажмите на кнопку **ОК**.
Окно **Сетевой порт** закроется. Добавленный вами сетевой порт отобразится в конце списка сетевых портов.
7. Сохраните внесенные изменения.

При работе протокола FTP в пассивном режиме соединение может устанавливаться через случайный сетевой порт, который не добавлен в список контролируемых сетевых портов. Чтобы защищать такие соединения, требуется установить флажок **Контролировать все сетевые порты** в блоке **Контролируемые порты** или настроить контроль всех сетевых портов для программ (см. раздел "Формирование списка программ, для которых контролируются все сетевые порты" на стр. 189), с помощью которых устанавливается FTP-соединение.

Формирование списка программ, для которых контролируются все сетевые порты

Вы можете сформировать список программ, для которых Kaspersky Endpoint Security контролирует все сетевые порты.

В список программ, для которых Kaspersky Endpoint Security контролирует все сетевые порты, рекомендуется включить программы, которые принимают или передают данные по протоколу FTP.

► Чтобы сформировать список программ, для которых контролируются все сетевые порты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.
4. Нажмите на кнопку **Настройка**.
Откроется окно **Сетевые порты**.
5. Установите флажок **Контролировать все порты для указанных программ**.
6. В списке программ, расположенном под флажком **Контролировать все порты для указанных программ**, выполните следующие действия:
 - Установите флажки напротив названий программ, для которых нужно контролировать все сетевые порты.
По умолчанию флажки установлены для всех программ, представленных в окне **Сетевые порты**.
 - Снимите флажки напротив названий программ, для которых не нужно контролировать все сетевые порты.
7. Если программа отсутствует в списке программ, добавьте ее следующим образом:
 - a. По ссылке **Добавить**, расположенной под списком программ, откройте контекстное меню.
 - b. Выберите в контекстном меню способ добавления программы в список программ:
 - Выберите пункт **Программы**, если вы хотите выбрать программу из списка программ, установленных на компьютере. Откроется окно **Выбор программы**, с помощью которого вы можете указать название программы.
 - Выберите пункт **Обзор**, если вы хотите указать местонахождение исполняемого файла программы. Откроется стандартное окно Microsoft Windows **Открыть**, с помощью которого вы можете указать название исполняемого файла программы.После выбора программы откроется окно **Программа**.
 - c. В поле **Название** введите название для выбранной программы.
 - d. Нажмите на кнопку **ОК**.
Окно **Программа** закроется. Добавленная вами программа отобразится в конце списка программ.
8. Сохраните внесенные изменения.

Проверка защищенных соединений

Вы можете выполнить следующие действия для настройки проверки защищенных соединений:

- включить проверку защищенных соединений;
- настроить параметры проверки защищенных соединений;
- создать исключение из проверки защищенных соединений.

В этом разделе

Включение и выключение проверки защищенных соединений.....	191
Настройка параметров проверки защищенных соединений	191
Создание исключения из проверки защищенных соединений	193
Просмотр глобальных исключений из проверки защищенного трафика.....	193

Включение и выключение проверки защищенных соединений

► *Чтобы включить или выключить проверку защищенных соединений, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры сети**.
3. В правой части окна в блоке **Проверка защищенных соединений** выполните одно из следующих действий:
 - Установите флажок **Проверять защищенные соединения**, если вы хотите, чтобы программа Kaspersky Endpoint Security контролировала зашифрованный сетевой трафик.
 - Снимите флажок **Проверять защищенные соединения**, если вы не хотите, чтобы программа Kaspersky Endpoint Security контролировала зашифрованный сетевой трафик.
4. Сохраните внесенные изменения.

Настройка параметров проверки защищенных соединений

► *Чтобы настроить параметры проверки защищенных соединений, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры сети**.
3. В правой части окна в блоке **Проверка защищенных соединений** нажмите на кнопку **Дополнительные параметры**.
Откроется окно **Дополнительные параметры**.

4. В раскрывающемся списке **При переходе на домен с недоверенным сертификатом** выберите один из следующих элементов:

- **Разрешать.** Если выбран этот элемент, то при переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security разрешает установку сетевого соединения.

При переходе на домен с недоверенным сертификатом в браузере Kaspersky Endpoint Security отображает HTML-страницу с предупреждением и информацией о причине, по которой этот домен не рекомендован для посещения. По ссылке из HTML-страницы с предупреждением пользователь может получить доступ к запрошенному веб-ресурсу. После перехода по этой ссылке Kaspersky Endpoint Security в течение часа не будет отображать предупреждения о недоверенном сертификате при переходе на другие ресурсы в том же домене.

- **Блокировать.** Если выбран этот элемент, то при переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security блокирует сетевое соединение, устанавливаемое при переходе на этот домен.

При переходе на домен с недоверенным сертификатом в браузере Kaspersky Endpoint Security отображает HTML-страницу с информацией о причине, по которой переход на этот домен заблокирован.

5. В раскрывающемся списке **При возникновении ошибок проверки защищенных соединений** выберите один из следующих элементов:

- **Блокировать соединение.** Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security блокирует это сетевое соединение.

- **Добавлять домен в исключения.** Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security добавляет домен, при переходе на который возникла ошибка, в список доменов с ошибками проверки и не контролирует зашифрованный сетевой трафик при переходе на этот домен.

По ссылке **Домены с ошибками проверки** вы можете открыть окно **Домены с ошибками проверки**, в котором перечислены домены, добавленные в исключения при возникновении ошибки проверки защищенного соединения.

Ссылка **Домены с ошибками проверки** доступна, если выбран элемент **Добавлять домен в исключения**.

При выборе элемента **Блокировать соединение** в раскрывающемся списке **При возникновении ошибок проверки защищенных соединений** Kaspersky Endpoint Security удаляет все исключения, перечисленные в окне **Домены с ошибками проверки**.

6. Установите флажок **Блокировать соединения по протоколу SSL 2.0**, если вы хотите, чтобы программа Kaspersky Endpoint Security блокировала сетевые соединения, устанавливаемые по протоколу SSL 2.0.

Снимите флажок **Блокировать соединения по протоколу SSL 2.0**, если вы хотите, чтобы программа Kaspersky Endpoint Security не блокировала сетевые соединения, устанавливаемые по протоколу SSL 2.0, и не контролировала сетевой трафик, передаваемый по этим соединениям.

Не рекомендуется использовать протокол SSL 2.0, так как он содержит недостатки, влияющие на безопасность передачи данных.

7. Установите флажок **Расшифровать защищенные соединения с сайтом, использующим EV-сертификат**, если вы хотите, чтобы программа Kaspersky Endpoint Security расшифровывала и контролировала защищенные соединения с EV-сертификатом.

EV-сертификаты (англ. Extended Validation Certificate) подтверждают подлинность веб-сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на веб-сайте EV-сертификата с помощью значка замка в адресной строке браузера. Также браузеры могут полностью или частично окрашивать адресную строку в зеленый цвет.

8. Сохраните внесенные изменения.

Создание исключения из проверки защищенных соединений

Kaspersky Endpoint Security не проверяет защищенные соединения, установленные программами, для которых установлен флажок **Не проверять сетевой трафик** в окне **Исключения из проверки для программы** (см. раздел "**Формирование списка доверенных программ**" на стр. [69](#)).

- *Чтобы исключить веб-адрес из проверки защищенных соединений, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры сети**.
3. В правой части окна в блоке **Проверка защищенных соединений** нажмите на кнопку **Доверенные адреса**.

Откроется окно **Доверенные адреса**.

4. Выполните одно из следующих действий:
 - Если вы хотите добавить имя домена или IP-адрес в список исключений, нажмите на кнопку **Добавить**.
 - Если вы хотите изменить имя домена или IP-адрес в списке исключений, нажмите на кнопку **Изменить**.

Откроется окно **Доменное имя или IP-адрес**.

5. Введите имя домена или IP-адрес, если вы хотите, чтобы программа Kaspersky Endpoint Security не проверяла защищенные соединения, устанавливаемые при переходе на эту веб-страницу.
6. Сохраните внесенные изменения.

Просмотр глобальных исключений из проверки защищенного трафика

- *Чтобы просмотреть глобальные исключения из проверки защищенного трафика, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры сети**.

3. В правой части окна в блоке **Проверка защищенных соединений** нажмите на ссылку **сайтах**.

Откроется окно **Глобальные исключения проверки зашифрованного трафика**.

В окне отображается составленная специалистами "Лаборатории Касперского" таблица с информацией о сайтах и программах, для которых Kaspersky Endpoint Security не проверяет защищенные соединения. Таблица может быть обновлена при обновлении баз и модулей Kaspersky Endpoint Security.

Проверка целостности модулей программы

Kaspersky Endpoint Security проверяет файлы программы, находящиеся в папке установки программы, на наличие повреждений или изменений. Например, если библиотека программы имеет некорректную цифровую подпись, то такая библиотека считается поврежденной.

После запуска задачи проверки целостности (см. раздел "Запуск и остановка задачи проверки целостности" на стр. [195](#)) процесс ее выполнения отображается в строке под названием задачи в окне **Задачи**.

Информация о результатах выполнения задачи проверки целостности фиксируется в отчетах (см. раздел "Работа с отчетами" на стр. [272](#)).

В этом разделе

Запуск и остановка задачи проверки целостности	195
Выбор режима запуска для задачи проверки целостности	196

Запуск и остановка задачи проверки целостности

Независимо от выбранного режима запуска вы можете запустить или остановить задачу проверки целостности в любой момент.

► *Чтобы запустить или остановить задачу проверки целостности, выполните следующие действия:*

1. В главном окне программы, нажмите на кнопку **Задачи**.
2. По левой клавише мыши выберите блок с названием задачи проверки целостности.
Раскроется выбранный блок.
3. Выполните одно из следующих действий:
 - Нажмите на кнопку **Запустить**, если вы хотите запустить задачу проверки целостности.
Статус выполнения задачи, отображающийся под названием задачи проверки целостности, изменится на *Выполняется*.
 - Выберите в контекстном меню пункт **Остановить**, если вы хотите остановить задачу проверки целостности.
Статус выполнения задачи, отображающийся под названием задачи проверки целостности, изменится на *Остановлена*.

- Чтобы запустить или остановить задачу проверки целостности при отображении упрощенного интерфейса программы (см. раздел "Упрощенный интерфейс программы" на стр. 46), выполните следующие действия:
1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
 2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:
 - выберите незапущенную задачу проверки целостности, чтобы запустить ее;
 - выберите запущенную задачу проверки целостности, чтобы остановить ее;
 - выберите остановленную задачу проверки целостности, чтобы возобновить ее или запустить ее заново.

Выбор режима запуска для задачи проверки целостности

- Чтобы выбрать режим запуска для задачи проверки целостности, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Задачи** → **Проверка целостности**.
3. В блоке **Режим запуска** выберите один из следующих вариантов:
 - Выберите вариант **Вручную**, если вы хотите запускать задачу проверки целостности вручную.
 - Выберите вариант **По расписанию**, если вы хотите настроить расписание запуска задачи проверки целостности.
4. Если на предыдущем шаге вы выбрали вариант **По расписанию**, задайте параметры расписания запуска задачи. Для этого выполните следующие действия:
 - a. В раскрывающемся списке **Периодичность** укажите, когда следует запускать задачу проверки целостности. Выберите один из следующих вариантов: **Минуты**, **Часы**, **Дни**, **Каждую неделю**, **В указанное время**, **Каждый месяц**, **После запуска программы**.
 - b. В зависимости от выбранного в раскрывающемся списке **Периодичность** элемента задайте значение параметров, которые уточняют время запуска задачи.
 - c. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенную по расписанию задачу проверки целостности.

Если в раскрывающемся списке **Периодичность** выбран элемент **После запуска программы**, **Минуты** или **Часы**, то флажок **Запускать пропущенные задачи** недоступен.

- d. Установите флажок **Выполнять только во время простоя компьютера**, если вы хотите, чтобы Kaspersky Endpoint Security приостанавливал задачу, когда ресурсы компьютера заняты.
Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.
5. Сохраните внесенные изменения.

Защита паролем

Для версии программы Kaspersky Endpoint Security для Windows 11.1.0 и выше порядок работы Защиты паролем изменился. В Kaspersky Endpoint Security для Windows 11.1.0 вы можете ограничить доступ к программе отдельным пользователям и не использовать одну учетную запись. При обновлении с предыдущих версий программы, если Защита паролем включена, Kaspersky Endpoint Security сохраняет ранее заданный пароль. Для первого изменения параметров Защиты паролем используйте имя пользователя KAdmin и ранее заданный пароль.

Компьютер могут использовать несколько пользователей с разным уровнем компьютерной грамотности. Неограниченный доступ пользователей к Kaspersky Endpoint Security и его параметрам может привести к снижению уровня безопасности компьютера в целом. Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы программы).

Если пользователь, который запустил сессию Windows, (*сессионный пользователь*) имеет разрешение на выполнение действия, Kaspersky Endpoint Security не запрашивает имя пользователя и пароль или временный пароль. Пользователь получает доступ к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями.

Если у сессионного пользователя отсутствует разрешение на выполнение действия, пользователь может получить доступ к программе следующими способами:

- Ввод имени пользователя и пароля.

Этот способ удобен для повседневной работы. Для выполнения действия, защищенного паролем, требуется ввести данные доменной учетной записи пользователя с необходимым разрешением.

- Ввод временного пароля.

Этот способ удобен, если пользователь находится вне корпоративной сети и необходимо предоставить ему временное разрешение на выполнение запрещенного действия (например, завершить работу программы). По истечении срока действия временного пароля или истечении сессии программа возвращает параметры Kaspersky Endpoint Security в прежнее состояние.

При попытке пользователя выполнить действие, защищенное паролем, Kaspersky Endpoint Security предложит пользователю ввести имя пользователя и пароль или временный пароль (см. рис. ниже).

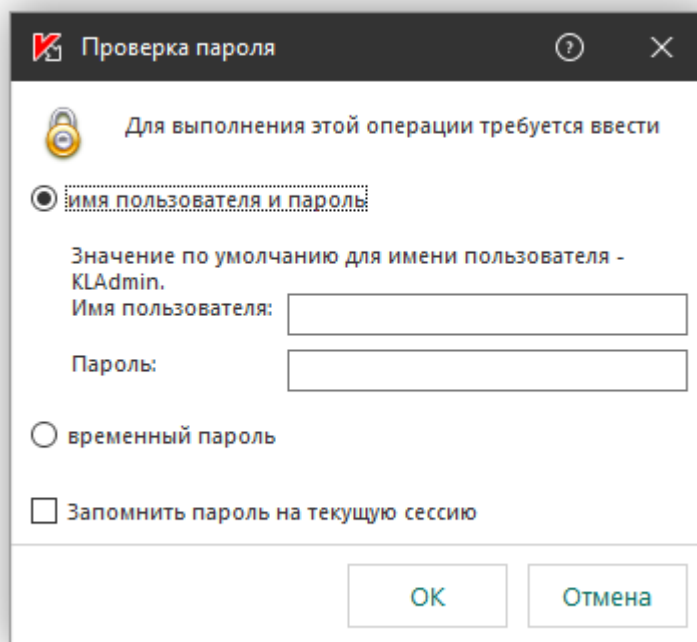


Рисунок 16. Запрос пароля для доступа к Kaspersky Endpoint Security

Имя пользователя и пароль

Для доступа к Kaspersky Endpoint Security необходимо ввести данные доменной учетной записи. Защита паролем поддерживает работу со следующими учетными записями:

- **KLAdmin.** Учетная запись администратора без ограничений доступа к Kaspersky Endpoint Security. Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем. Отменить разрешение для учетной записи KLAdmin невозможно. Kaspersky Endpoint Security требует задать пароль для учетной записи KLAdmin во время включения Защиты паролем.
- **Группа "Все".** Стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети. Пользователи из группы "Все" могут получить доступ к программе в соответствии с предоставленными разрешениями.
- **Отдельные пользователи или группы.** Учетные записи пользователей, для которых вы можете настроить отдельные разрешения. Например, если для группы "Все" выполнение действия запрещено, то вы можете разрешить выполнение действия для отдельного пользователя или группы.
- **Сессионный пользователь.** Учетная запись пользователя, который запустил сессию Windows. Вы можете сменить сессионного пользователя во время ввода пароля (флажок **Запомнить пароль на текущую сессию**). В этом случае Kaspersky Endpoint Security назначает сессионным пользователем, учетные данные которого вы ввели, вместо пользователя, который запустил сессию Windows.

Временный пароль

Временный пароль позволяет предоставить временный доступ к Kaspersky Endpoint Security для отдельного компьютера вне корпоративной сети. Администратор создает временный пароль для отдельного компьютера в Kaspersky Security Center в свойствах компьютера пользователя. Администратор выбирает действия, на которые будет распространяться временный пароль, и срок действия временного пароля.

Алгоритм работы Защиты паролем

Kaspersky Endpoint Security принимает решение о выполнении действия, защищенного паролем, по следующему алгоритму (см. рис. ниже).

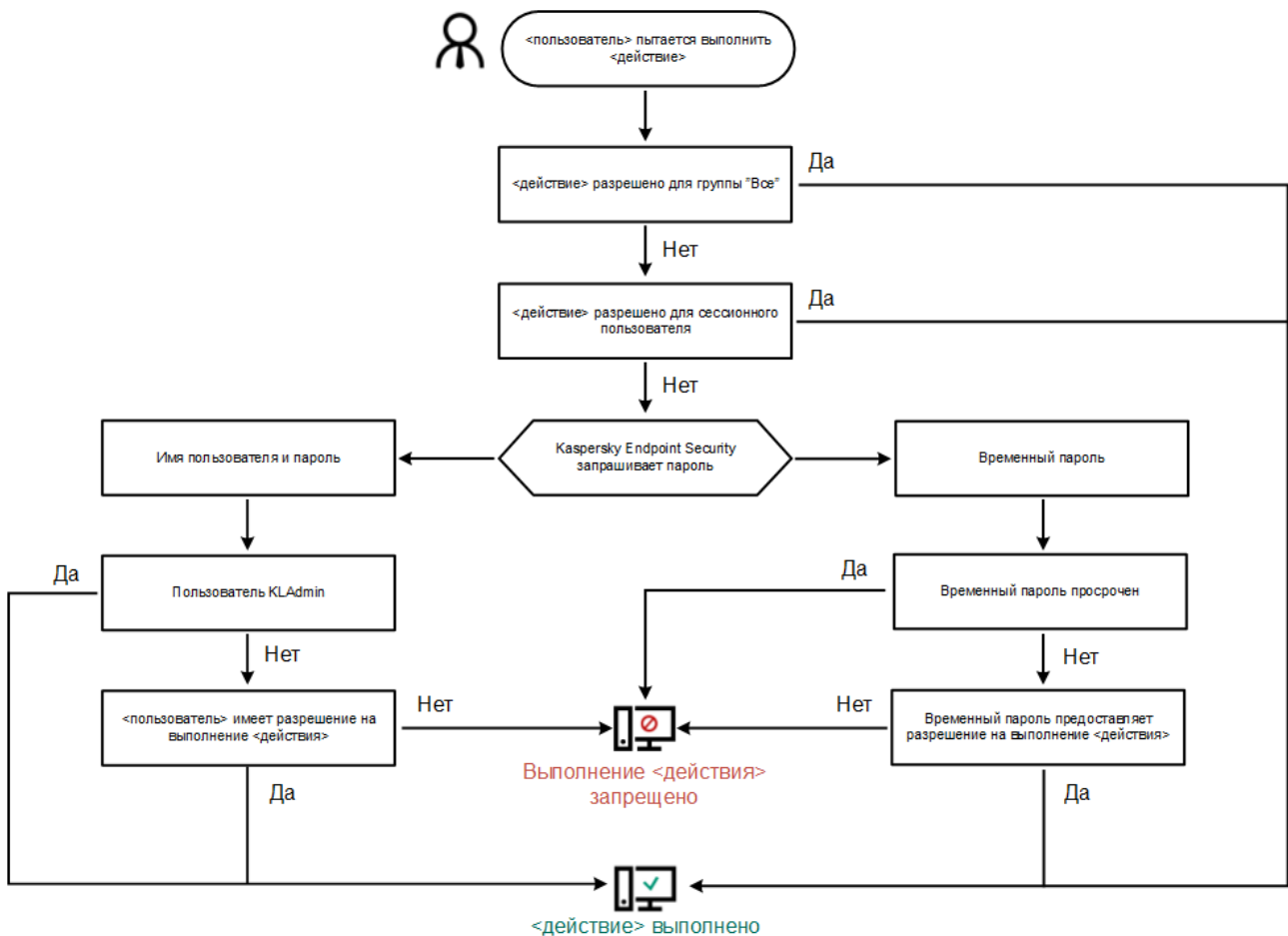


Рисунок 17. Алгоритм работы Защиты паролем

В этом разделе

Включение Защиты паролем	200
Предоставление разрешений для отдельных пользователей или групп	201
Использование временного пароля для предоставления разрешений.....	202
Особенности разрешений Защиты паролем	203

Включение Защиты паролем

Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы программы).

► Чтобы включить Защиту паролем, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Интерфейс**.
3. В блоке **Защита паролем** нажмите на кнопку **Настройка**.
Откроется окно **Защита паролем**.
4. В открывшемся окне установите флажок **Включить защиту паролем**.
5. Задайте пароль для учетной записи KLAAdmin:
 - a. В таблице **Разрешения** откройте список разрешений для учетной записи KLAAdmin двойным щелчком мыши.
Учетная запись KLAAdmin имеет право на выполнение любого действия, защищенного паролем.
 - b. В открывшемся окне нажмите на кнопку **Пароль**.
 - c. Задайте пароль для учетной записи KLAAdmin и подтвердите его.
 - d. Нажмите на кнопку **ОК**.

Если компьютер работает под управлением политики, администратор может сбросить пароль для учетной записи KLAAdmin в свойствах политики. Если компьютер не подключен к Kaspersky Security Center и вы забыли пароль для учетной записи KLAAdmin, восстановить пароль невозможно.

6. Настройте разрешения для всех пользователей внутри корпоративной сети:
 - a. В таблице **Разрешения** откройте список разрешений для группы "Все" двойным щелчком мыши.
Группа "Все" – стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети.
 - b. Установите флажки напротив тех действий, которые будут доступны пользователям без ввода пароля.
Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы программы** снят, вы можете завершить работу программы только с помощью учетной записи KLAAdmin, отдельной учетной записи с нужным разрешением (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. [201](#)) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. [202](#)).

Разрешения Защиты паролем имеют ряд особенностей (см. раздел "Особенности разрешений Защиты паролем" на стр. [203](#)). Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.

- c. Нажмите на кнопку **ОК**.
7. Сохраните внесенные изменения.

После включения Защиты паролем программа ограничит доступ пользователей к Kaspersky Endpoint Security в соответствии с разрешениями для группы "Все". Вы можете выполнить запрещенные для группы "Все" действия только с помощью учетной записи KAdmin, отдельной учетной записи с нужными разрешениями (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. [201](#)) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. [202](#)).

Вы можете выключить Защиту паролем только с помощью учетной записи KAdmin. Выключить защиту паролем с помощью другой учетной записи или с помощью временного пароля невозможно.

Во время проверки пароля вы можете установить флажок **Запомнить пароль на текущую сессию**. В этом случае Kaspersky Endpoint Security не будет требовать ввода пароля при попытке пользователя выполнить другое разрешенное действие, защищенное паролем, в течение сессии.

Предоставление разрешений для отдельных пользователей или групп

Вы можете предоставить доступ к Kaspersky Endpoint Security для отдельных пользователей или групп. Например, если группе "Все" запрещено завершать работу программы, вы можете предоставить отдельному пользователю разрешение **Завершение работы программы**. В результате вы можете завершить работу программы только с помощью учетной записи этого пользователя или учетной записи KAdmin.

► *Чтобы предоставить разрешение для отдельных пользователей или групп, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Интерфейс**.
3. В блоке **Защита паролем** нажмите на кнопку **Настройка**.
Откроется окно **Защита паролем**.
4. В таблице **Разрешения** нажмите на кнопку **Добавить**.
Откроется окно **Разрешения пользователя/группы**.
5. Справа от поля **Пользователь/Группа** нажмите на кнопку **Выбрать**.
Откроется стандартное окно Windows для выбора пользователей или групп.
6. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.
7. В таблице **Разрешения** установите флажки напротив тех действий, которые будут доступны добавленному пользователю или группе без ввода пароля.

Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы программы** снят, вы можете завершить работу программы только с помощью учетной записи KAdmin, отдельной учетной записи с нужным разрешением (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. [201](#)) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. [202](#)).

Разрешения Защиты паролем имеют ряд особенностей (см. раздел "Особенности разрешений Защиты паролем" на стр. 203). Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.

8. Сохраните внесенные изменения.

В результате, если для группы "Все" доступ к программе ограничен, пользователи получают доступ к Kaspersky Endpoint Security в соответствии с разрешениями для этих пользователей.

Использование временного пароля для предоставления разрешений

Временный пароль позволяет предоставить временный доступ к Kaspersky Endpoint Security для отдельного компьютера вне корпоративной сети. Это нужно, чтобы разрешить выполнение запрещенного действия без передачи пользователю учетных данных KLAAdmin. Для использования временного пароля компьютер должен быть добавлен в Kaspersky Security Center.

► *Чтобы предоставить пользователю разрешение на выполнение запрещенного действия с помощью временного пароля, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел **Программы**.
6. В списке установленных на компьютере программ "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows** и откройте свойства программы двойным щелчком мыши.
7. В окне параметров программы выберите раздел **Общие параметры** → **Интерфейс**.
8. В блоке **Защита паролем** нажмите на кнопку **Настройка**.
Откроется окно **Защита паролем**.
9. В блоке **Временный пароль** нажмите на кнопку **Настройка**.
Откроется окно **Создание временного пароля**.
10. В поле **Дата истечения** установите срок действия временного пароля.
11. В таблице **Область действия временного пароля** установите флажки напротив тех действий, которые будут доступны пользователю после ввода временного пароля.
12. Нажмите на кнопку **Создать**.
Откроется окно с временным паролем (см. рис. ниже).
13. Скопируйте и передайте пользователю пароль.

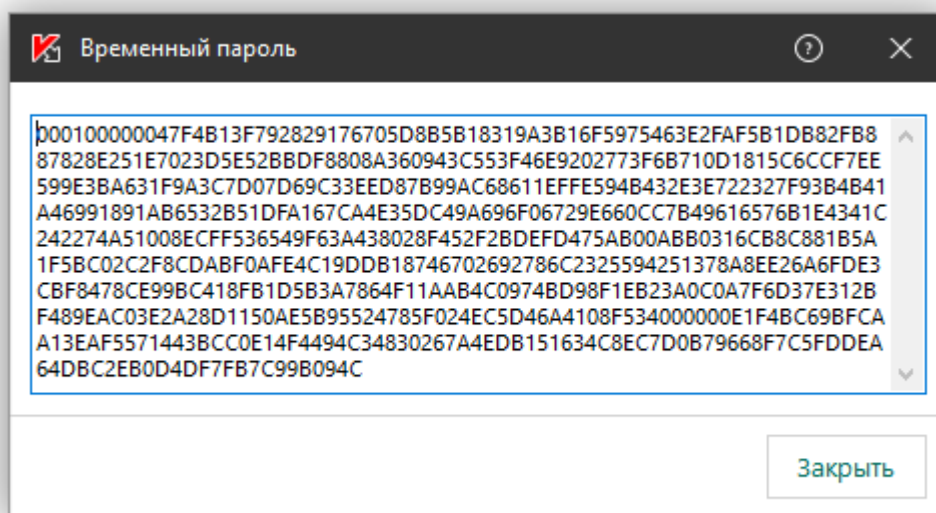



Рисунок 18. Временный пароль

Особенности разрешений Защиты паролем

Разрешения Защиты паролем имеют ряд особенностей и ограничений.


Настройка параметров программы

Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты  открыты).


Завершение работы программы

Особенностей и ограничений нет.

Выключение компонентов защиты

- Предоставить разрешение на выключение компонентов защиты для группы "Все" невозможно. Чтобы разрешить выключение компонентов защиты не только пользователю KLSAdmin, но и другим пользователям, добавьте пользователя или группу (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. [201](#)) с разрешением **Выключение компонентов защиты** в параметрах Защиты паролем.
- Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты  открыты).
- Для выключения компонентов защиты в параметрах программы пользователь должен иметь разрешение **Настройка параметров программы**.
- Для выключения компонентов защиты из контекстного меню (пункт **Приостановка защиты и контроля**) пользователь, кроме разрешения **Выключение компонентов защиты**, должен иметь разрешение **Выключение компонентов контроля**.

Выключение компонентов контроля

- Предоставить разрешение на выключение компонентов контроля для группы "Все" невозможно. Чтобы разрешить выключение компонентов защиты не только пользователю KLAAdmin, но и другим пользователям, добавьте пользователя или группу (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. [201](#)) с разрешением **Выключение компонентов контроля** в параметрах Защиты паролем.
- Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты  открыты).
- Для выключения компонентов контроля в параметрах программы пользователь должен иметь разрешение **Настройка параметров программы**.
- Для выключения компонентов контроля из контекстного меню (пункт **Приостановка защиты и контроля**) пользователь, кроме разрешения **Выключение компонентов контроля**, должен обладать разрешением **Выключение компонентов защиты**.

Выключение политики Kaspersky Security Center

Предоставить разрешение на выключение политики Kaspersky Security Center для группы "Все" невозможно. Чтобы разрешить выключение политики не только пользователю KLAAdmin, но и другим пользователям, добавьте пользователя или группу (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. [201](#)) с разрешением **Выключение политики Kaspersky Security Center** в параметрах Защиты паролем.

Удаление ключа

Особенностей и ограничений нет.

Удаление / изменение / восстановление программы

Особенностей и ограничений нет.

Восстановление доступа к данным на зашифрованных устройствах

Вы можете восстановить доступ к данным на зашифрованных устройствах только с помощью учетной записи KLAAdmin. Разрешить это действие другому пользователю невозможно.

Просмотр отчетов

Особенностей и ограничений нет.

Восстановление из резервного хранилища

Особенностей и ограничений нет.

Шифрование данных

Kaspersky Endpoint Security позволяет шифровать файлы и папки, хранящиеся на локальных дисках компьютера и съемных дисках, съемные и жесткие диски целиком. Шифрование данных снижает риски утечки информации в случае кражи / утери портативного компьютера, съемного диска или жесткого диска, а также при доступе посторонних пользователей и программ к данным. Kaspersky Endpoint Security использует алгоритм шифрования Advanced Encryption Standard (AES).

Если срок действия лицензии истек, то программа не шифрует новые данные, а старые зашифрованные данные остаются зашифрованными и доступными для работы. В этом случае для шифрования новых данных требуется активировать программу по новой лицензии, которая допускает использование шифрования.

В случае истечения срока действия лицензии, нарушения Лицензионного соглашения, удаления лицензионного ключа, удаления программы Kaspersky Endpoint Security или компонентов шифрования с компьютера пользователя не гарантируется, что файлы, зашифрованные ранее, останутся зашифрованными. Это связано с тем, что некоторые программы, например Microsoft Office Word, при редактировании файлов создают их временную копию, которой подменяют исходный файл при его сохранении. В результате при отсутствии или недоступности на компьютере функциональности шифрования файл остается незашифрованным.

Kaspersky Endpoint Security обеспечивает следующие направления защиты данных:

- **Шифрование файлов на локальных дисках компьютера.** Вы можете сформировать списки из файлов (см. раздел "Запуск шифрования файлов на локальных дисках компьютера" на стр. [226](#)) по расширению или группам расширений и из папок, расположенных на локальных дисках компьютера, а также создать правила шифрования файлов, создаваемых отдельными программами (см. раздел "Шифрование файлов, создаваемых и изменяемых отдельными программами" на стр. [229](#)). После применения политики программа Kaspersky Endpoint Security шифрует и расшифровывает следующие файлы:
 - файлы, отдельно добавленные в списки для шифрования и расшифровки;
 - файлы, хранящиеся в папках, добавленных в списки для шифрования и расшифровки;
 - файлы, создаваемые отдельными программами.
- **Шифрование съемных дисков.** Вы можете указать правило шифрования по умолчанию, в соответствии с которым программа выполняет одинаковое действие по отношению ко всем съемным дискам, и указать правила шифрования отдельных съемных дисков.

Правило шифрования по умолчанию имеет меньший приоритет, чем правила шифрования, созданные для отдельных съемных дисков. Правила шифрования, созданные для съемных дисков с указанной моделью устройства, имеют меньший приоритет, чем правила шифрования, созданные для съемных дисков с указанным идентификатором устройства.

Чтобы выбрать правило шифрования файлов на съемном диске, Kaspersky Endpoint Security проверяет, известны ли модель устройства и его идентификатор. Далее программа выполняет одно из следующих действий:

- Если известна только модель устройства, программа применяет правило шифрования, созданное для съемных дисков с данной моделью устройства, если такое правило есть.
- Если известен только идентификатор устройства, программа применяет правило шифрования, созданное для съемных дисков с данным идентификатором устройства, если такое правило есть.

- Если известны и модель устройства, и идентификатор устройства, программа применяет правило шифрования, созданное для съемных дисков с данным идентификатором устройства, если такое правило есть. Если такого правила нет, но есть правило шифрования, созданное для съемных дисков с данной моделью устройства, программа применяет его. Если не заданы правила шифрования ни для данного идентификатора устройства, ни для данной модели устройства, программа применяет правило шифрования по умолчанию.
- Если неизвестны ни модель устройства, ни идентификатор устройства, программа применяет правило шифрования по умолчанию.

Программа позволяет подготовить съемный диск для работы с зашифрованными на нем файлами в портативном режиме. После включения портативного режима становится доступной работа с зашифрованными файлами на съемных дисках, подключенных к компьютеру с недоступной функциональностью шифрования.

- **Управление правами доступа программ к зашифрованным файлам.** Для любой программы вы можете создать правило доступа к зашифрованным файлам, запрещающее доступ к зашифрованным файлам или разрешающее доступ к зашифрованным файлам только в виде шифротекста - последовательности символов, полученной в результате применения шифрования.
- **Создание зашифрованных архивов.** Вы можете создавать зашифрованные архивы и защищать доступ к этим архивам паролем. Доступ к содержимому зашифрованных архивов можно получить только после ввода паролей, которыми вы защитили доступ к этим архивам. Такие архивы можно безопасно передавать по сети или на съемных дисках.
- **Полнодисковое шифрование.** Вы можете выбрать технологию шифрования: Шифрование диска Kaspersky или Шифрование диска BitLocker (далее также "BitLocker").

BitLocker – технология, являющаяся частью операционной системы Windows. Если компьютер оснащен доверенным платформенным модулем (англ. Trusted Platform Module – TPM), BitLocker использует его для хранения ключей восстановления, позволяющих получить доступ к зашифрованному жесткому диску. При загрузке компьютера BitLocker запрашивает у доверенного платформенного модуля ключи восстановления жесткого диска и разблокирует его. Вы можете настроить использование пароля и / или PIN-кода для доступа к ключам восстановления.

Вы можете указать правило полнодискового шифрования по умолчанию и сформировать список жестких дисков для исключения из шифрования. Kaspersky Endpoint Security выполняет полнодисковое шифрование по секторам после применения политики Kaspersky Security Center. Программа шифрует сразу все логические разделы жестких дисков.

После шифрования системных жестких дисков при последующем включении компьютера доступ к ним, а также загрузка операционной системы возможны только после прохождения процедуры аутентификации с помощью Агента аутентификации. Для этого требуется ввести пароль токена или смарт-карты, подключенных к компьютеру, или имя и пароль учетной записи Агента аутентификации, созданной системным администратором локальной сети организации с помощью задачи *Управления учетными записями Агента аутентификации*. Эти учетные записи основаны на учетных записях пользователей Microsoft Windows, под которыми пользователи выполняют вход в операционную систему. Также вы можете использовать технологию единого входа (см. раздел "Включение использования технологии единого входа (SSO)" на стр. [247](#)) (англ. Single Sign-On – SSO), позволяющую осуществлять автоматический вход в операционную систему с помощью имени и пароля учетной записи Агента аутентификации.

Если для компьютера была создана резервная копия, затем данные компьютера были зашифрованы, после чего была восстановлена резервная копия компьютера и данные компьютера снова были зашифрованы, Kaspersky Endpoint Security формирует дубликаты учетных записей Агента аутентификации. Для удаления дубликатов требуется использовать утилиту `klmover` с ключом `dupfix`. Утилита `klmover` поставляется со сборкой Kaspersky Security Center. Подробнее о ее работе вы можете прочитать в справке для Kaspersky Security Center.

Доступ к зашифрованным жестким дискам возможен только с компьютеров, на которых установлена программа Kaspersky Endpoint Security с доступной функциональностью полнодискового шифрования. Это условие сводит к минимуму вероятность утечки информации, хранящейся на зашифрованном жестком диске, при использовании зашифрованного жесткого диска вне локальной сети организации.

Для шифрования жестких и съемных дисков вы можете использовать функцию **Шифровать только занятое пространство**. Рекомендуется применять эту функцию только для новых, ранее не использовавшихся устройств. Если вы применяете шифрование на уже используемом устройстве, рекомендуется зашифровать все устройство. Это гарантирует защиту всех данных – даже удаленных, но еще содержащих извлекаемые сведения.

Перед началом шифрования Kaspersky Endpoint Security получает карту секторов файловой системы. В первом потоке шифруются секторы, занятые файлами на момент запуска шифрования. Во втором потоке шифруются секторы, в которые выполнялась запись после начала шифрования. После завершения шифрования все секторы, содержащие данные, оказываются зашифрованными.

Если после завершения шифрования пользователь удаляет файл, то секторы, в которых хранился этот файл, становятся свободными для дальнейшей записи информации на уровне файловой системы, но остаются зашифрованными. Таким образом, по мере записи файлов на новом устройстве при регулярном запуске шифрования с включенной функцией **Шифровать только занятое пространство** на компьютере через некоторое время будут зашифрованы все секторы.

Данные, необходимые для расшифровки объектов, предоставляет Сервер администрирования Kaspersky Security Center, под управлением которого находился компьютер в момент шифрования. Если по каким-либо причинам компьютер с зашифрованными объектами попал под управление другого Сервера администрирования, то получить доступ к зашифрованным данным возможно одним из следующих способов:

- Серверы администрирования в одной иерархии:
 - Вам не нужно предпринимать никаких дополнительных действий. У пользователя останется доступ к зашифрованным объектам. Ключи шифрования распространяются на все Серверы администрирования.
- Серверы администрирования разрознены:
 - Запросить доступ к зашифрованным объектам у администратора локальной сети организации.
 - Восстановить данные на зашифрованных устройствах с помощью утилиты восстановления.
 - Восстановить конфигурацию Сервера администрирования Kaspersky Security Center, под управлением которого находился компьютер в момент шифрования, из резервной копии и использовать эту конфигурацию на Сервере администрирования, под управлением которого оказался компьютер с зашифрованными объектами.

При отсутствии доступа к зашифрованным данным следуйте специальным инструкциям по работе с зашифрованными данными, .

В этом разделе

Ограничения функциональности шифрования	208
Смена длины ключа шифрования (AES56 / AES256)	209
Полнодисковое шифрование	210
Шифрование файлов на локальных дисках компьютера	225
Шифрование съемных дисков	236
Работа с Агентом аутентификации	247
Просмотр информации о шифровании данных	256
Работа с зашифрованными устройствами при отсутствии доступа к ним	260

Ограничения функциональности шифрования

Шифрование данных имеет следующие ограничения:

- В процессе шифрования программа создает служебные файлы. Для их хранения требуется около 0,5% нефрагментированного свободного пространства на жестком диске компьютера. Если нефрагментированного свободного пространства на жестком диске недостаточно, то шифрование не запускается до тех пор, пока не обеспечено это условие.
- Шифрование данных доступно только при использовании Kaspersky Endpoint Security с системой администрирования Kaspersky Security Center. Шифрование данных при использовании Kaspersky Endpoint Security в автономном режиме невозможно, так как Kaspersky Endpoint Security хранит в Kaspersky Security Center ключи шифрования.
- Управление шифрованием данных доступно в Консоли администрирования Kaspersky Security Center и Kaspersky Security Center Web Console. Управлять шифрованием данных в Kaspersky Security Center Cloud Console невозможно.
- Если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для серверов, то доступно только полнодисковое шифрование с помощью технологии Шифрование диска BitLocker. Если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций, то функциональность шифрования данных доступна в полном объеме.

Функциональность полнодискового шифрования с помощью технологии Шифрование диска Kaspersky недоступна для жестких дисков, которые не отвечают аппаратным и программным требованиям.

Не поддерживается совместимость между функциональностью полнодискового шифрования Kaspersky Endpoint Security и Антивирусом Касперского для UEFI. Антивирус Касперского для UEFI запускается до загрузки операционной системы. При полнодисковом шифровании программа обнаружит отсутствие установленной операционной системы на компьютере. В результате работа Антивируса Касперского для UEFI завершится с ошибкой. Шифрование файлов (FLE) не влияет на работу Антивируса Касперского для UEFI.

Kaspersky Endpoint Security не поддерживает следующие конфигурации:

- схема, при которой загрузчик расположен на одном диске, а операционная система - на другом;
- встроенное программное обеспечение стандарта UEFI 32;

- система с технологией Intel® Rapid Start Technology и диски с разделом гибернации (hibernation partition), даже при отключенном использовании Intel® Rapid Start Technology;
- диски в формате MBR, имеющие более четырех расширенных разделов (extended partitions);
- система, в которой есть файл подкачки, расположенный не на системном диске;
- мультизагрузочная система с несколькими одновременно установленными операционными системами;
- динамические разделы (поддерживаются только разделы основного типа);
- диски, на которых менее 0,5% свободного нефрагментированного пространства;
- диски с размером сектора, отличным от 512 байт или 4096 байт, которые эмулируют 512 байт;
- гибридные диски.

Смена длины ключа шифрования (AES56 / AES256)

Kaspersky Endpoint Security использует алгоритм шифрования AES (Advanced Encryption Standard). Kaspersky Endpoint Security поддерживает алгоритм шифрования AES с эффективной длиной ключа 256 и 56 бит. Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: *Strong encryption (AES256)* или *Lite encryption (AES56)*. Библиотека шифрования AES устанавливается вместе с программой.

Смена длины ключа шифрования доступна только для Kaspersky Endpoint Security 11.2.0 и выше.

Смена длины ключа шифрования состоит из следующих этапов:

1. Расшифруйте объекты, которые программа Kaspersky Endpoint Security зашифровала до начала смены длины ключа шифрования:
 - a. Расшифруйте жесткие диски (см. раздел "Расшифровка жестких дисков" на стр. [217](#)).
 - b. Расшифруйте файлы на локальных дисках (см. раздел "Расшифровка файлов на локальных дисках компьютера" на стр. [231](#)).
 - c. Расшифруйте съемные диски (см. раздел "Расшифровка съемных дисков" на стр. [246](#)).

После смены длины ключа шифрования объекты, зашифрованные ранее, становятся недоступны.

2. Удалите Kaspersky Endpoint Security.
3. Установите Kaspersky Endpoint Security из дистрибутива Kaspersky Endpoint Security с другой библиотекой шифрования.

Вы также можете сменить длину ключа шифрования через обновление программы. Смена длины ключа через обновление программы доступна при выполнении следующих условий:

- На компьютере установлена программа Kaspersky Endpoint Security версии 10 Service Pack 2 и выше.
- На компьютере не установлены компоненты шифрования данных: Шифрование файлов, Полнодисковое шифрование.

По умолчанию компоненты шифрования данных не включены в состав Kaspersky Endpoint Security. Компонент Управление BitLocker не влияет на смену длины ключа шифрования.

Для смены длины ключа шифрования запустите файл `kes_win.msi` или `setup_kes.exe` из дистрибутива с нужной библиотекой шифрования. Также вы можете обновить программу дистанционно с помощью инсталляционного пакета.

Невозможно сменить длину ключа шифрования с помощью дистрибутива той же версии программы, которая установлена на вашем компьютере, без предварительного удаления программы.

Полнодисковое шифрование

Если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций, то для шифрования доступны технологии Шифрование диска BitLocker и Шифрование диска Kaspersky. Если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов, то доступна только технология Шифрование диска BitLocker. Kaspersky Endpoint Security поддерживает полнодисковое шифрование в файловых системах FAT32, NTFS и exFat.

Перед запуском полнодискового шифрования программа выполняет ряд проверок на возможность шифрования устройства, в том числе и проверку совместимости системного жесткого диска с Агентом аутентификации или с компонентами шифрования BitLocker. Для проверки совместимости требуется выполнить перезагрузку компьютера. После перезагрузки компьютера программа в автоматическом режиме выполняет все необходимые проверки. Если проверка на совместимость проходит успешно, то после загрузки операционной системы и запуска программы запускается полнодисковое шифрование. Если в процессе проверки обнаруживается несовместимость системного жесткого диска с Агентом аутентификации или с компонентами шифрования BitLocker, требуется перезагрузить компьютер с помощью аппаратной кнопки (Reset). Kaspersky Endpoint Security фиксирует информацию о несовместимости, на основе которой не запускает полнодисковое шифрование после старта операционной системы. В отчетах Kaspersky Security Center выводится информация об этом событии.

Если аппаратная конфигурация компьютера изменилась, то для проверки системного жесткого диска на совместимость с Агентом аутентификации и компонентами шифрования BitLocker требуется удалить информацию о несовместимости, полученную программой при предыдущей проверке. Для этого перед полнодисковым шифрованием в командной строке требуется ввести команду `avp pbatestreset`. Если после проверки системного жесткого диска на совместимость с Агентом аутентификации операционная система не может запуститься, требуется удалить объекты и данные, оставшиеся после тестовой работы Агента аутентификации (см. раздел "Удаление объектов и данных, оставшихся после тестовой работы Агента аутентификации" на стр. [256](#)), с помощью утилиты восстановления, далее запустить Kaspersky Endpoint Security и выполнить команду `avp pbatestreset` повторно.

После запуска полнодисковое шифрование Kaspersky Endpoint Security шифрует все, что записывается на жесткие диски.

Если во время полнодискового шифрования пользователь выключает или перезагружает компьютер, то перед последующей загрузкой операционной системы загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет полнодисковое шифрование.

Если во время全盘 шифрования операционная система переходит в режим гибернации (hibernation mode), то при выводе операционной системы из режима гибернации загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет全盘 шифрование.

Если во время全盘 шифрования операционная система переходит в спящий режим (sleep mode), то при выводе операционной системы из спящего режима Kaspersky Endpoint Security возобновляет全盘 шифрование без загрузки Агента аутентификации.

Аутентификация пользователя в Агенте аутентификации может выполняться двумя способами:

- путем ввода имени и пароля учетной записи Агента аутентификации, созданной администратором локальной сети организации средствами Kaspersky Security Center;
- путем ввода пароля подключенного к компьютеру токена или смарт-карты.

Использование токена или смарт-карты доступно, только если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES256. Если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES56, то в добавлении файла электронного сертификата в команду будет отказано.

Агент аутентификации поддерживает раскладки клавиатуры для следующих языков:

- Английский (Великобритания);
- Английский (США);
- Арабский (Алжир, Марокко, Тунис, раскладка AZERTY);
- Испанский (Латинская Америка);
- Итальянский;
- Немецкий (Германия и Австрия);
- Немецкий (Швейцария);
- Португальский (Бразилия, раскладка ABNT2);
- Русский (для 105-клавишных клавиатур IBM / Windows с раскладкой ЙЦУКЕН);
- Турецкий (раскладка QWERTY);
- Французский (Франция);
- Французский (Швейцария);
- Французский (Бельгия, раскладка AZERTY);
- Японский (для 106-клавишных клавиатур с раскладкой QWERTY).

Раскладка клавиатуры становится доступной в Агенте аутентификации, если она добавлена в настройках языка и региональных стандартов операционной системы и доступна на экране приветствия Microsoft Windows.

Если имя учетной записи Агента аутентификации содержит символы, которые невозможно ввести с помощью доступных в Агенте аутентификации раскладок клавиатуры, то доступ к зашифрованным жестким дискам возможен только после их восстановления с помощью утилиты восстановления или после восстановления имени и пароля учетной записи Агента аутентификации (см. раздел "Восстановление доступа к диску, защищенному технологией Шифрование диска Kaspersky" на стр. [218](#)).

Kaspersky Endpoint Security работает со следующими токенами, считывателями смарт-карт и смарт-картами:

- SafeNet eToken PRO 64K (4.2b) (USB).
- SafeNet eToken PRO 72K Java (USB).
- SafeNet eToken PRO 72K Java (Smart Card).
- SafeNet eToken 4100 72K Java (Smart Card).
- SafeNet eToken 5100 (USB).
- SafeNet eToken 5105 (USB).
- SafeNet eToken 7300 (USB).
- EMC RSA SecurID 800 (USB).
- Рутокен ЭЦП (USB).
- Рутокен ЭЦП (Flash).
- Aladdin-RD JaCarta PKI (USB).
- Aladdin-RD JaCarta PKI (Smart Card).
- Athena IDProtect Laser (USB).
- Gemalto IDBridge CT40 (Reader).
- Gemalto IDPrime .NET 511.

В этом разделе

Полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky	213
Полнодисковое шифрование с помощью технологии Шифрование диска BitLocker	214
Формирование списка жестких дисков для исключения из шифрования	216
Расшифровка жестких дисков.....	217
Восстановление доступа к диску, защищенному технологией Шифрование диска Kaspersky	218
Восстановление доступа к диску, зашифрованному BitLocker	221
Обновление операционной системы	223
Устранение ошибок при обновлении функциональности шифрования	224

Полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky

Перед запуском полнодискового шифрования рекомендуется убедиться в том, что компьютер не заражен. Для этого запустите полную проверку или проверку важных областей компьютера. Выполнение полнодискового шифрования на компьютере, зараженном руткитом, может привести к неработоспособности компьютера.

► Чтобы выполнить полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Полнодисковое шифрование**.
6. В раскрывающемся списке **Технология шифрования** выберите элемент **Шифрование диска Kaspersky**.

Применение технологии шифрования Шифрование диска Kaspersky невозможно, если на компьютере есть жесткие диски, зашифрованные с помощью BitLocker.

7. В раскрывающемся списке **Режим шифрования** выберите действие **Шифровать все жесткие диски**.

Если на компьютере установлено несколько операционных систем, то после шифрования всех жестких дисков вы сможете выполнить загрузку только той операционной системы, в которой установлена программа.

Если некоторые жесткие диски нужно исключить из шифрования, сформируйте их список (см. раздел "Формирование списка жестких дисков для исключения из шифрования" на стр. [216](#)).

8. Выберите один из следующих способов шифрования:
 - Если вы хотите применить шифрование только к тем секторам жесткого диска, которые заняты файлами, установите флажок **Шифровать только занятое пространство**.
Если вы применяете шифрование на уже используемом диске, рекомендуется зашифровать весь диск. Это гарантирует защиту всех данных – даже удаленных, но еще содержащих извлекаемые сведения. Функцию **Шифровать только занятое пространство** рекомендуется использовать для новых, ранее не использовавшихся дисков.
 - Если вы хотите применить шифрование ко всему жесткому диску, снимите флажок **Шифровать только занятое пространство**.

Если устройство было зашифровано ранее с использованием функции **Шифровать только занятое пространство**, после применения политики в режиме **Шифровать все жесткие диски** секторы, не занятые файлами, по-прежнему не будут зашифрованы.

9. Если в ходе шифрования компьютера возникла проблема несовместимости с аппаратным обеспечением, вы можете установить флажок **Использовать Legacy USB Support**.

Legacy USB Support – функция BIOS / UEFI, которая позволяет использовать USB-устройства (например, токен) на этапе загрузки компьютера до запуска операционной системы (BIOS-режим). Функция Legacy USB Support не влияет на поддержку USB-устройств после запуска операционной системы.

При включенной функции Legacy USB Support Агент аутентификации в BIOS-режиме не поддерживает работу с токенами по USB. Функцию рекомендуется использовать только при возникновении проблемы несовместимости с аппаратным обеспечением и только для тех компьютеров, на которых возникла проблема.

10. Сохраните внесенные изменения.

Полнодисковое шифрование с помощью технологии Шифрование диска BitLocker

Перед запуском полнодискового шифрования рекомендуется убедиться в том, что компьютер не заражен. Для этого запустите полную проверку или проверку важных областей компьютера. Выполнение полнодискового шифрования на компьютере, зараженном руткитом, может привести к неработоспособности компьютера.

Для работы технологии Шифрование диска BitLocker на компьютерах с серверной операционной системой может потребоваться установка компонента **Шифрование диска BitLocker** с помощью мастера добавления ролей.

► Чтобы применить полнодисковое шифрование BitLocker, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Полнодисковое шифрование**.
6. В раскрывающемся списке **Технология шифрования** выберите элемент **Шифрование диска BitLocker**.

7. В раскрывающемся списке **Режим шифрования** выберите элемент **Шифровать все жесткие диски**.

Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой выполнялось шифрование.

8. Если вы хотите включить аутентификацию BitLocker в предзагрузочной среде на планшетах, установите флажок **Включить использование проверки подлинности BitLocker, требующей предзагрузочного ввода с клавиатуры на планшетах**.

Сенсорная клавиатура планшетов недоступна в предзагрузочной среде. Для прохождения аутентификации BitLocker на планшетах пользователю необходимо подключить, например, USB-клавиатуру.

9. Если вы хотите использовать аппаратное шифрование, установите флажок **Использовать аппаратное шифрование**. Это позволяет увеличить скорость шифрования и сократить использование ресурсов компьютера.

10. Выберите один из следующих способов шифрования:

- Если вы хотите применить шифрование только к тем секторам жесткого диска, которые заняты файлами, установите флажок **Шифровать только занятое пространство**.
- Если вы хотите применить шифрование ко всему жесткому диску, снимите флажок **Шифровать только занятое пространство**.

Эта функция применима только к незашифрованным жестким дискам. Если жесткий диск был зашифрован ранее с использованием функции **Шифровать только занятое пространство**, после применения политики в режиме **Шифровать все жесткие диски** секторы, не занятые файлами, по-прежнему не будут зашифрованы.

11. Выберите способ получения доступа к жестким дискам, зашифрованным с помощью BitLocker:

- Если вы хотите использовать для хранения ключей шифрования модуль TPM, выберите вариант **Использовать доверенный платформенный модуль (TPM)**.

Доверенный платформенный модуль (англ. Trusted Platform Module – TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины.

- Если вы не используете модуль TPM для полнодискового шифрования, выберите вариант **Использовать пароль** и в поле **Минимальная длина пароля** укажите, какое минимальное количество символов должен содержать пароль.

Для компьютеров под управлением операционных систем Windows 7 и Windows Server 2008 R2 доступно только шифрование с использованием модуля TPM. Если модуль TPM не установлен, шифрование BitLocker невозможно. Использование пароля на этих компьютерах не поддерживается.

12. Если на предыдущем шаге вы выбрали вариант **Использовать доверенный платформенный модуль (TPM)**, выполните следующие действия:

- Если вы хотите установить PIN-код, который будет запрашиваться у пользователя при попытке доступа к ключу шифрования, установите флажок **Использовать PIN-код** и в поле **Минимальная длина PIN-кода** укажите, какое минимальное количество цифр должен содержать PIN-код.
- Если вы хотите, чтобы в случае отсутствия на компьютере модуля TPM доступ к зашифрованным жестким дискам можно было получить с помощью пароля, установите флажок **Использовать пароль, если доверенный платформенный модуль (TPM) недоступен** и в поле **Минимальная длина пароля** укажите, какое минимальное количество символов должен содержать пароль.

В такой ситуации доступ к ключам шифрования будет осуществляться с помощью заданного пароля так же, как при установленном флажке **Использовать пароль**.

Если флажок **Использовать пароль, если доверенный платформенный модуль (TPM) недоступен** снят и модуль TPM недоступен, то полнодисковое шифрование не запускается.

13. Сохраните внесенные изменения.

После применения политики на клиентском компьютере с установленной программой Kaspersky Endpoint Security появятся следующие запросы:

- Если в политике Kaspersky Security Center настроено шифрование системного жесткого диска:
 - При наличии модуля TPM, появится окно запроса PIN-кода.
 - При отсутствии модуля TPM, появится окно запроса пароля для предзагрузочной аутентификации.
- Если в операционной системе включен режим совместимости с Федеральным стандартом обработки информации (FIPS), то в операционных системах Windows 8, а также в более ранних версиях появится окно запроса на подключение запоминающего устройства для сохранения файла ключа восстановления.

При отсутствии доступа к ключам шифрования пользователь может запросить у администратора локальной сети организации ключ восстановления (см. раздел "Восстановление доступа к диску, зашифрованному BitLocker" на стр. [221](#)) (если ключ восстановления не был сохранен ранее на запоминающем устройстве или был утерян).

Формирование списка жестких дисков для исключения из шифрования

Вы можете сформировать список исключений из шифрования только для технологии Шифрование диска Kaspersky.

- Чтобы сформировать список жестких дисков для исключения из шифрования, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Полнодисковое шифрование**.
6. В раскрывающемся списке **Технология шифрования** выберите вариант **Шифрование диска Kaspersky**.

В таблице **Не шифровать следующие жесткие диски** отобразятся записи о жестких дисках, которые программа не будет шифровать. Если вы ранее не сформировали список жестких дисков для исключения из шифрования, эта таблица пуста.

7. Если вы хотите добавить жесткие диски в список жестких дисков, которые программа не будет шифровать, выполните следующие действия:
 - a. Нажмите на кнопку **Добавить**.
Откроется окно **Добавление устройств из списка Kaspersky Security Center**.
 - b. В окне **Добавление устройств из списка Kaspersky Security Center** укажите значения параметров **Название**, **Компьютер**, **Тип диска**, **Шифрование диска Kaspersky**.
 - c. Нажмите на кнопку **Обновить**.
 - d. В графе **Название** установите флажки в строках таблицы, соответствующих тем жестким дискам, которые вы хотите добавить в список жестких дисков для исключения из шифрования.
 - e. Нажмите на кнопку **ОК**.

Выбранные жесткие диски отобразятся в таблице **Не шифровать следующие жесткие диски**.

8. Если вы хотите удалить жесткие диски из таблицы исключений, выберите одну или несколько строк в таблице **Не шифровать следующие жесткие диски** и нажмите на кнопку **Удалить**.

Чтобы выбрать несколько строк в таблице, выделяйте их, удерживая клавишу **CTRL**.

9. Сохраните внесенные изменения.

Расшифровка жестких дисков

Вы можете расшифровать жесткие диски даже при отсутствии действующей лицензии, допускающей шифрование данных.

- Чтобы расшифровать жесткие диски, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Полнодисковое шифрование**.
6. В раскрываемся списке **Технология шифрования** выберите ту технологию, с помощью которой были зашифрованы жесткие диски.
7. Выполните одно из следующих действий:
 - В раскрываемся списке **Режим шифрования** выберите элемент **Расшифровывать все жесткие диски**, если вы хотите расшифровать все зашифрованные жесткие диски.
 - В таблицу **Не шифровать следующие жесткие диски** добавьте (см. раздел "Формирование списка жестких дисков для исключения из шифрования" на стр. [216](#)) те зашифрованные жесткие диски, которые вы хотите расшифровать.

Этот вариант доступен только для технологии шифрования Шифрование диска Kaspersky.

8. Сохраните внесенные изменения.

Если во время расшифровки жестких дисков, зашифрованных с помощью технологии Шифрование диска Kaspersky, пользователь выключает или перезагружает компьютер, то перед последующей загрузкой операционной системы загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет расшифровку жестких дисков.

Если во время расшифровки жестких дисков, зашифрованных с помощью технологии Шифрование диска Kaspersky, операционная система переходит в режим гибернации (hibernation mode), то при выводе операционной системы из режима гибернации загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет расшифровку жестких дисков. После расшифровки жестких дисков режим гибернации недоступен до первой перезагрузки операционной системы.

Если во время расшифровки жестких дисков операционная система переходит в спящий режим (sleep mode), то при выводе операционной системы из спящего режима Kaspersky Endpoint Security возобновляет расшифровку жестких дисков без загрузки Агента аутентификации.

Восстановление доступа к диску, защищенному технологией Шифрование диска Kaspersky

Если пользователь забыл пароль доступа к жесткому диску, защищенному технологией Шифрование диска Kaspersky, нужно запустить процедуру восстановления ("Запрос - Ответ").

Восстановление доступа к системному жесткому диску

Восстановление доступа к системному жесткому диску, защищенному технологией Шифрование диска Kaspersky, состоит из следующих этапов:

1. Пользователь сообщает администратору блоки запроса (см. рис. ниже).
2. Администратор вводит блоки запроса в Kaspersky Security Center, получает блоки ответа и сообщает блоки ответа пользователю.

3. Пользователь вводит блоки ответа в интерфейсе Агента аутентификации и получает доступ к жесткому диску.

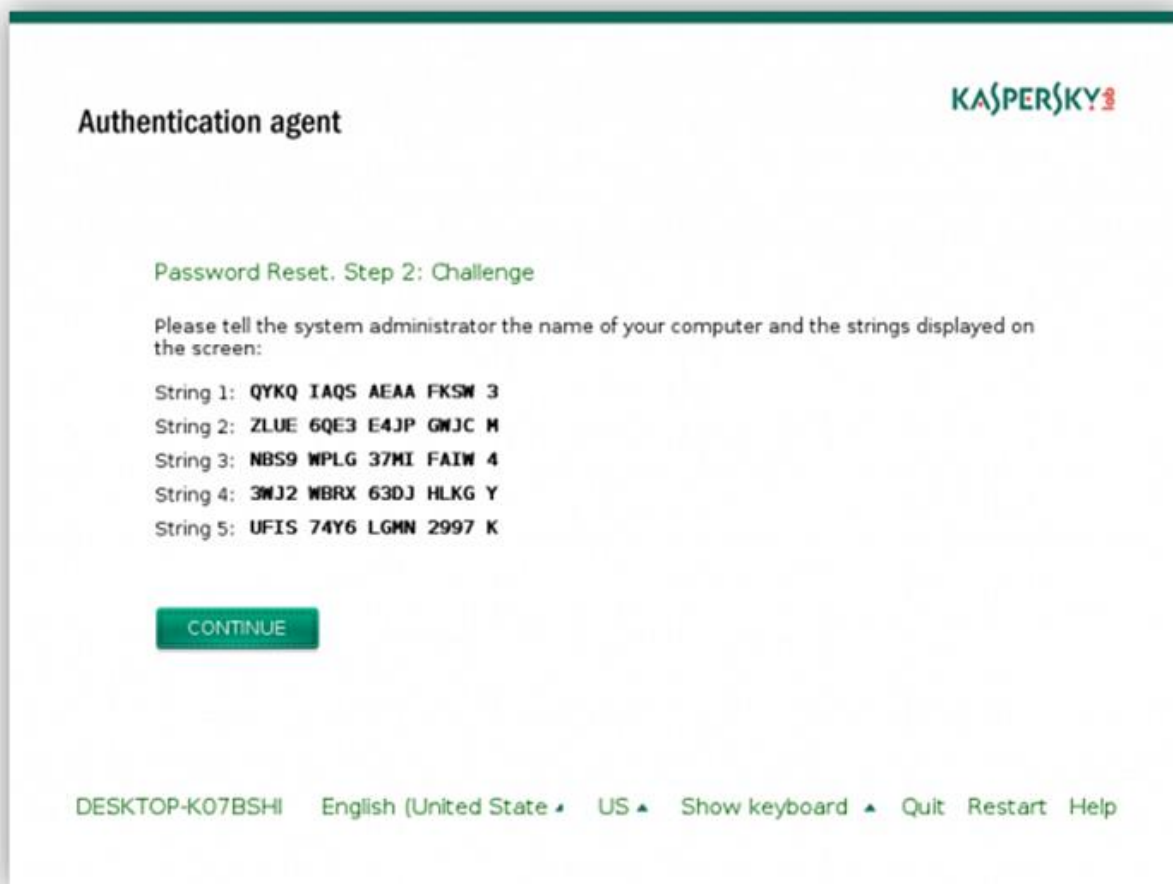


Рисунок 19. Восстановление доступа к системному жесткому диску, защищенного технологией Шифрование диска Kaspersky

Для запуска процедуры восстановления пользователю нужно в интерфейсе Агента аутентификации нажать на кнопку **Forgot your password**.

► Чтобы получить блоки ответа для системного жесткого диска, защищенного технологией Шифрование диска Kaspersky, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Агент аутентификации**.

7. В блоке **Используемый алгоритм шифрования** выберите алгоритм шифрования: **AES56** или **AES256**.

Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: *Strong encryption (AES256)* или *Lite encryption (AES56)*. Библиотека шифрования AES устанавливается вместе с программой.

8. В раскрывающемся списке **Учетная запись** выберите имя учетной записи Агента аутентификации пользователя, запросившего восстановление доступа к диску.
9. В раскрывающемся списке **Жесткий диск** выберите зашифрованный жесткий диск, доступ к которому необходимо восстановить.
10. В блоке **Запрос пользователя** введите блоки запроса, продиктованные пользователем.

В результате содержимое блоков ответа на запрос пользователя о восстановлении имени и пароля учетной записи Агента аутентификации отобразится в поле **Ключ доступа**. Передайте содержимое блоков ответа пользователю. После прохождения процедуры восстановления Агент аутентификации предложит пользователю сменить пароль.

Восстановление доступа к несистемному жесткому диску

Восстановление доступа к несистемному жесткому диску, защищенному технологией Шифрование диска Kaspersky, состоит из следующих этапов:

1. Пользователь отправляет администратору файл запроса.
2. Администратор добавляет файл запроса в Kaspersky Security Center, создает файл ключа доступа и отправляет файл пользователю.
3. Пользователь добавляет файл ключа доступа в Kaspersky Endpoint Security и получает доступ к жесткому диску.

Для запуска процедуры восстановления пользователю нужно обратиться к жесткому диску. В результате Kaspersky Endpoint Security создаст файл запроса (файл с расширением kesdc), который пользователю нужно передать администратору, например, по электронной почте.

► *Чтобы получить файл ключа доступа к зашифрованному несистемному жесткому диску, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Шифрование данных**.
7. На закладке **Шифрование данных** нажмите на кнопку **Обзор**.
8. В окне выбора файла запроса укажите путь к файлу, полученного от пользователя.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.

Восстановление доступа к диску, зашифрованному BitLocker

Если пользователь забыл пароль доступа к жесткому диску, зашифрованному BitLocker, нужно запустить процедуру восстановления ("Запрос - Ответ").

Восстановление доступа к жесткому диску, зашифрованному BitLocker, состоит из следующих этапов:

1. Пользователь сообщает администратору идентификатор ключа восстановления (см. рис. ниже).
2. Администратор проверяет идентификатор ключа восстановления в свойствах компьютера в Kaspersky Security Center. Идентификатор, который предоставил пользователь, должен соответствовать идентификатору, который отображается в свойствах компьютера.
3. Если идентификаторы ключа восстановления совпадают, администратор сообщает пользователю ключ восстановления или передает файл ключа восстановления.

Файл ключа восстановления используется для компьютеров под управлением следующих операционных систем:

- Windows 7;
- Windows 8;
- Windows Server 2008;
- Windows Server 2011;
- Windows Server 2012.

Для остальных операционных систем используется ключ восстановления.

4. Пользователь вводит ключ восстановления и получает доступ к жесткому диску.

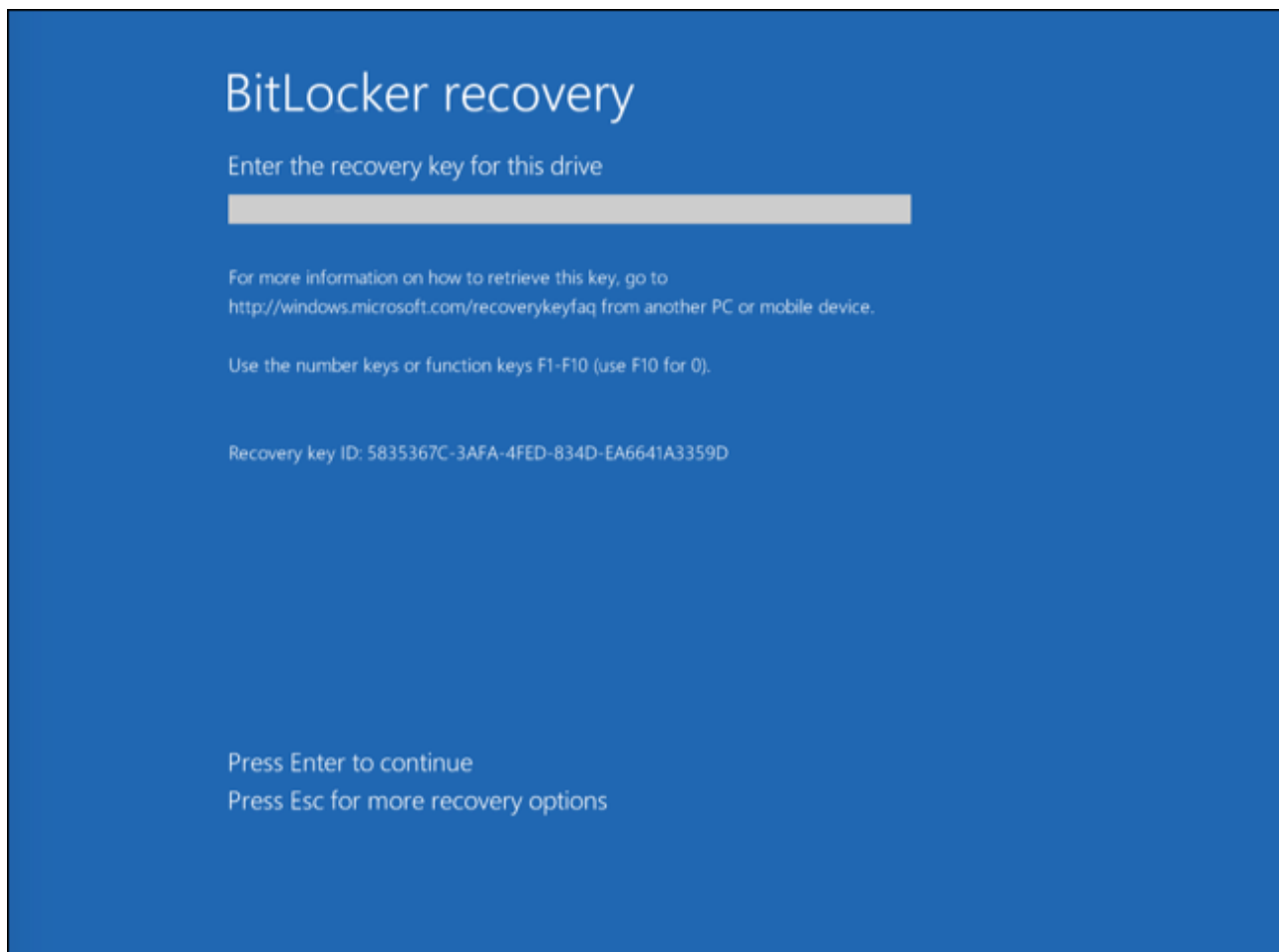


Рисунок 20. Восстановление доступа к жесткому диску, зашифрованному BitLocker

Восстановление доступа к системному диску

Для запуска процедуры восстановления пользователю нужно на этапе предзагрузочной аутентификации нажать клавишу **ESC**.

► *Чтобы просмотреть ключ восстановления для системного диска, зашифрованного BitLocker, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Доступ к системному диску с защитой BitLocker**.
7. Запросите у пользователя идентификатор ключа восстановления, указанный в окне ввода пароля BitLocker, и сравните его с идентификатором в поле **Идентификатор ключа восстановления**.

Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

В результате вам будет доступен ключ восстановления или файл ключа восстановления, который нужно будет передать пользователю.

После загрузки операционной системы пользователю нужно сменить пароль. Для этого пользователю нужно открыть Панель управления операционной системы и перейти в параметры BitLocker. В параметрах BitLocker пользователю нужно сбросить старый пароль и задать новый. Если пользователь не сменил пароль, при следующей загрузке операционной системы вы можете использовать старый ключ восстановления.

Восстановление доступа к несистемному диску

Для запуска процедуры восстановления пользователю нужно в окне предоставления доступа к диску перейти по ссылке **Забыли пароль**. После получения доступа к зашифрованному диску пользователь может включить автоматическую разблокировку диска при аутентификации Windows в параметрах BitLocker.

► *Чтобы просмотреть ключ восстановления для несистемного диска, зашифрованного BitLocker, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Дополнительно** → **Шифрование и защита данных** → **Зашифрованные устройства**.
3. В рабочей области выберите зашифрованное устройство, для которого вы хотите создать файл ключа доступа, и в контекстном меню устройства выберите пункт **Получить доступ к устройству в Kaspersky Endpoint Security для Windows (11.3.0)**.
4. Запросите у пользователя идентификатор ключа восстановления, указанный в окне ввода пароля BitLocker, и сравните его с идентификатором в поле **Идентификатор ключа восстановления**.

Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

Передайте пользователю ключ, указанный в поле **Ключ восстановления**.

Обновление операционной системы

Обновление операционной системы компьютера, защищенного с помощью полнодискового шифрования (FDE), имеет ряд особенностей. Выполняйте обновление операционной системы последовательно: сначала обновите ОС на одном компьютере, затем на небольшой части компьютеров, затем на всех компьютерах сети.

Если вы используете технологию Шифрование диска Kaspersky, то перед запуском операционной системы загружается Агент аутентификации. С помощью Агента аутентификации пользователь выполняет вход в систему и получает доступ к зашифрованным дискам. Далее начинается загрузка операционной системы.

Если запустить обновление операционной системы на компьютере, защищенном с помощью технологии Шифрование диска Kaspersky, мастер обновления ОС может удалить Агент аутентификации. В результате компьютер может быть заблокирован, так как загрузчик ОС не сможет получить доступ к зашифрованному диску.

Безопасное обновление операционной системы состоит из следующих этапов:

1. Расшифровка жестких дисков (на стр. [217](#)).
2. Обновление операционной системы.
3. Шифрование жестких дисков (см. раздел "Полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky" на стр. [213](#)).

Автоматическое обновление операционной системы доступно при выполнении следующих условий:

1. Обновление ОС через WSUS (Windows Server Update Services).
2. На компьютере установлена операционная система Windows 10 версия 1607 (RS1) и выше.
3. На компьютере установлена программа Kaspersky Endpoint Security версии 11.2.0 и выше.

При выполнении всех условий вы можете обновлять операционную систему обычным способом.

Если вы используете технологию Шифрование диска BitLocker, для обновления Windows 10 не нужно расшифровывать жесткие диски. Подробнее о BitLocker см. на [сайте Microsoft](https://docs.microsoft.com/ru-ru/windows/security/information-protection/bitlocker/bitlocker-overview) <https://docs.microsoft.com/ru-ru/windows/security/information-protection/bitlocker/bitlocker-overview>.

Устранение ошибок при обновлении функциональности шифрования

При обновлении с предыдущих версий программы до Kaspersky Endpoint Security для Windows 11.3.0 обновляется функциональность полнодискового шифрования.

При запуске обновления функциональности полнодискового шифрования могут возникнуть следующие ошибки:

- Не удалось инициализировать обновление.
 - Устройство несовместимо с Агентом аутентификации.
- *Чтобы устранить ошибки, возникшие при запуске обновления функциональности полнодискового шифрования, в новой версии программы выполните следующие действия:*
1. Расшифруйте жесткие диски (см. раздел "Расшифровка жестких дисков" на стр. [217](#)).
 2. Повторно зашифруйте жесткие диски (см. раздел "Полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky" на стр. [213](#)).

В процессе обновления функциональности полнодискового шифрования могут возникнуть следующие ошибки:

- Не удалось завершить обновление.
 - Откат обновления функциональности шифрования завершен с ошибкой.
- *Чтобы устранить ошибки, возникшие в процессе обновления функциональности полнодискового шифрования,*

восстановите доступ к зашифрованному устройству с помощью утилиты восстановления (см. раздел "Восстановление данных с помощью утилиты восстановления FDERT" на стр. [261](#)).

Шифрование файлов на локальных дисках компьютера

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Шифрование файлов имеет следующие особенности:

- Kaspersky Endpoint Security шифрует / расшифровывает стандартные папки только для локальных профилей пользователей (англ. local user profiles) операционной системы. Kaspersky Endpoint Security не шифрует и не расшифровывает стандартные папки для перемещаемых профилей пользователей (англ. roaming user profiles), обязательных профилей пользователей (англ. mandatory user profiles), временных профилей пользователей (англ. temporary user profiles), а также перенаправленные папки.
- В список стандартных папок для шифрования входят следующие папки:
 - Документы.
 - Избранное.
 - Рабочий стол.
 - Временные файлы.
 - Файлы Outlook.
- Kaspersky Endpoint Security не выполняет шифрование файлов, изменение которых может повредить работе операционной системы и установленных программ. Например, в список исключений из шифрования входят следующие файлы и папки со всеми вложенными в них папками:
 - %WINDIR%;
 - %PROGRAMFILES% и %PROGRAMFILES(X86)%;
 - файлы реестра Windows.

Список исключений из шифрования недоступен для просмотра и изменения. Файлы и папки из списка исключений из шифрования можно добавить в список для шифрования, но при выполнении шифрования файлов они не будут зашифрованы.

В этом разделе

Запуск шифрования файлов на локальных дисках компьютера	226
Формирование правил доступа программ к зашифрованным файлам	228
Шифрование файлов, создаваемых и изменяемых отдельными программами	229
Формирование правила расшифровки	230
Расшифровка файлов на локальных дисках компьютера	231
Создание зашифрованных архивов	232
Восстановление доступа к зашифрованным файлам	233
Восстановление доступа к зашифрованным данным в случае выхода из строя операционной системы.....	235
Изменение шаблонов сообщений для получения доступа к зашифрованным файлам	235

Запуск шифрования файлов на локальных дисках компьютера

Kaspersky Endpoint Security не шифрует файлы, содержимое которых расположено в облачном хранилище OneDrive, и блокирует копирование зашифрованных файлов в облачное хранилище OneDrive, если эти файлы не добавлены в правило расшифровки (см. раздел "Формирование правила расшифровки" на стр. [230](#)).

► Чтобы зашифровать файлы на локальных дисках компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование файлов**.
6. В правой части окна выберите закладку **Шифрование**.
7. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.
8. На закладке **Шифрование** нажмите на кнопку **Добавить** и в раскрывающемся списке выберите один из следующих элементов:
 - a. Выберите элемент **Стандартные папки**, чтобы добавить в правило шифрования файлы из папок локальных профилей пользователей, предложенных специалистами "Лаборатории Касперского".
 - **Документы**. Файлы в стандартной папке операционной системы *Документы*, а также вложенные папки.
 - **Избранное**. Файлы в стандартной папке операционной системы *Избранное*, а также вложенные папки.

- **Рабочий стол.** Файлы в стандартной папке операционной системы *Рабочий стол*, а также вложенные папки.
 - **Временные файлы.** Временные файлы, связанные с работой установленных на компьютере программ. Например, программы Microsoft Office создают временные файлы с резервными копиями документов.
 - **Файлы Outlook.** Файлы, связанные с работой почтового клиента Outlook: файлы данных (PST), автономные файлы данных (OST), файлы автономной адресной книги (OAB) и файлы персональной адресной книги (PAB).
- b. Выберите элемент **Папку вручную**, чтобы добавить в правило шифрования папку, путь к которой введен вручную.
- При добавлении пути к папке следует использовать следующие правила:
- Используйте переменную окружения (например, %FOLDER%\UserFolder\). Вы можете использовать переменную окружения только один раз и только в начале пути.
 - Не используйте относительные пути. Вы можете использовать набор \. . \ (например, C:\Users\.. \UserFolder\). Набор \. . \ обозначает переход к родительской папке.
 - Не используйте символы * и ?.
 - Не используйте UNC-пути.
 - Используйте ; или , в качестве разделительного символа.
- c. Выберите элемент **Файлы по расширению**, чтобы добавить в правило шифрования отдельные расширения файлов. Kaspersky Endpoint Security шифрует файлы с указанными расширениями на всех локальных дисках компьютера.
- d. Выберите элемент **Файлы по группам расширений**, чтобы добавить в правило шифрования группы расширений файлов (например, группа *Документы Microsoft Office*). Kaspersky Endpoint Security шифрует файлы с расширениями, перечисленными в группах расширений, на всех локальных дисках компьютера.
9. Сохраните внесенные изменения.

Сразу после применения политики Kaspersky Endpoint Security шифрует файлы, включенные в правило шифрования и не включенные в правило расшифровки (см. раздел "Формирование правила расшифровки" на стр. [230](#)).

Если один и тот же файл добавлен и в правило шифрования, и в правило расшифровки, то Kaspersky Endpoint Security не шифрует этот файл, если он не зашифрован, и расшифровывает, если он зашифрован.

Kaspersky Endpoint Security шифрует незашифрованные файлы, если их свойства (путь к файлу или расширение файла) после изменения удовлетворяют критериям правила шифрования.

Kaspersky Endpoint Security откладывает шифрование открытых файлов до тех пор, пока они не будут закрыты. Когда пользователь создает новый файл, свойства которого удовлетворяют критериям правила шифрования, Kaspersky Endpoint Security шифрует файл сразу же при открытии файла.

Если вы переносите зашифрованный файл в другую папку на локальном диске, файл остается зашифрованным, независимо от того, включена ли эта папка в правило шифрования.

Формирование правил доступа программ к зашифрованным файлам

► Чтобы сформировать правила доступа программ к зашифрованным файлам, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование файлов**.
6. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.

Правила доступа действуют только в режиме **Согласно правилам**. Если после применения правил доступа в режиме **Согласно правилам** вы перейдете в режим **Оставлять без изменений**, то Kaspersky Endpoint Security будет игнорировать все правила доступа. Все программы будут иметь доступ ко всем зашифрованным файлам.

7. В правой части окна выберите закладку **Правила для программ**.
8. Если вы хотите выбрать программы исключительно из списка Kaspersky Security Center, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы из списка Kaspersky Security Center**.
 - a. Задайте фильтры для вывода списка программ в таблице. Для этого укажите значения параметров **Программа**, **Производитель**, **Период добавления**, а также флажков из блока **Группа**.
 - b. Нажмите на кнопку **Обновить**.
 - c. В таблице отобразится список программ, удовлетворяющих заданным фильтрам.
 - d. В графе **Программы** установите флажки напротив тех программ в таблице, для которых вы хотите сформировать правила доступа к зашифрованным файлам.
 - e. В раскрывающемся списке **Правило для программ** выберите правило, которое будет определять доступ программ к зашифрованным файлам.
 - f. В раскрывающемся списке **Действие для программ, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security над правилами доступа к зашифрованным файлам, сформированными для указанных выше программ ранее.
 - g. Нажмите на кнопку **ОК**.Информация о правиле доступа программ к зашифрованным файлам отобразится в таблице на закладке **Правила для программ**.
9. Если вы хотите выбрать программы вручную, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы вручную**.
 - a. В поле ввода введите имя или список имен исполняемых файлов программ с их расширениями.
Вы можете также добавить имена исполняемых файлов программ из списка Kaspersky Security Center, нажав на кнопку **Добавить из списка Kaspersky Security Center**.
 - b. Если требуется, в поле **Описание** введите описание списка программ.

- c. В раскрывающемся списке **Правило для программ** выберите правило, которое будет определять доступ программ к зашифрованным файлам.
- d. Нажмите на кнопку **ОК**.

Информация о правиле доступа программ к зашифрованным файлам отобразится в таблице на закладке **Правила для программ**.

10. Сохраните внесенные изменения.

Шифрование файлов, создаваемых и изменяемых отдельными программами

Вы можете создать правило, согласно которому Kaspersky Endpoint Security будет шифровать все файлы, создаваемые и изменяемые указанными в правиле программами.

Файлы, созданные или измененные указанными программами до применения правила шифрования, не будут зашифрованы.

- *Чтобы настроить шифрование файлов, создаваемых и изменяемых отдельными программами, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование файлов**.
6. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.

Правила шифрования действуют только в режиме **Согласно правилам**. Если после применения правил шифрования в режиме **Согласно правилам** вы перейдете в режим **Оставлять без изменений**, то Kaspersky Endpoint Security будет игнорировать все правила шифрования. Файлы, которые были зашифрованы ранее, по-прежнему останутся зашифрованными.

7. В правой части окна выберите закладку **Правила для программ**.
8. Если вы хотите выбрать программы исключительно из списка Kaspersky Security Center, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы из списка Kaspersky Security Center**.

Откроется окно **Добавление программ из списка Kaspersky Security Center**.

Выполните следующие действия:

- a. Задайте фильтры для вывода списка программ в таблице. Для этого укажите значения параметров **Программа**, **Производитель**, **Период добавления**, а также флажков из блока **Группа**.
- b. Нажмите на кнопку **Обновить**.

В таблице отобразится список программ, удовлетворяющих заданным фильтрам.

- c. В графе **Программы** установите флажки напротив тех программ в таблице, создаваемые файлы которых вы хотите шифровать.
- d. В раскрывающемся списке **Правило для программ** выберите элемент **Шифровать все создаваемые файлы**.
- e. В раскрывающемся списке **Действие для программ, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security над правилами шифрования файлов, сформированными для указанных выше программ ранее.
- f. Нажмите на кнопку **ОК**.

Информация о правиле шифрования файлов, создаваемых и изменяемых выбранными программами, отобразится в таблице на закладке **Правила для программ**.

9. Если вы хотите выбрать программы вручную, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы вручную**.

Откроется окно **Добавление / изменение названий исполняемых файлов программ**.

Выполните следующие действия:

- a. В поле ввода введите имя или список имен исполняемых файлов программ с их расширениями.
Вы можете также добавить имена исполняемых файлов программ из списка Kaspersky Security Center, нажав на кнопку **Добавить из списка Kaspersky Security Center**.
- b. Если требуется, в поле **Описание** введите описание списка программ.
- c. В раскрывающемся списке **Правило для программ** выберите элемент **Шифровать все создаваемые файлы**.
- d. Нажмите на кнопку **ОК**.

Информация о правиле шифрования файлов, создаваемых и изменяемых выбранными программами, отобразится в таблице на закладке **Правила для программ**.

10. Сохраните внесенные изменения.

Формирование правила расшифровки

► *Чтобы сформировать правило расшифровки, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование файлов**.
6. В правой части окна выберите закладку **Расшифровка**.
7. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.
8. На закладке **Расшифровка** нажмите на кнопку **Добавить** и в раскрывающемся списке выберите один из следующих элементов:
 - a. Выберите элемент **Стандартные папки**, чтобы добавить в правило расшифровки файлы из папок локальных профилей пользователей, предложенных специалистами "Лаборатории Касперского".
 - b. Выберите элемент **Папку вручную**, чтобы добавить в правило расшифровки папку, путь к которой введен вручную.

- c. Выберите элемент **Файлы по расширению**, чтобы добавить в правило расшифровки отдельные расширения файлов. Kaspersky Endpoint Security не шифрует файлы с указанными расширениями на всех локальных дисках компьютера.
 - d. Выберите элемент **Файлы по группам расширений**, чтобы добавить в правило расшифровки группы расширений файлов (например, группа *Документы Microsoft Office*). Kaspersky Endpoint Security не шифрует файлы с расширениями, перечисленными в группах расширений, на всех локальных дисках компьютера.
9. Сохраните внесенные изменения.

Если один и тот же файл добавлен и в правило шифрования, и в правило расшифровки, то Kaspersky Endpoint Security не шифрует этот файл, если он не зашифрован, и расшифровывает, если он зашифрован.

Расшифровка файлов на локальных дисках компьютера

► Чтобы расшифровать файлы на локальных дисках компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование файлов**.
6. В правой части окна выберите закладку **Шифрование**.
7. Исключите из списка для шифрования файлы и папки, которые вы хотите расшифровать. Для этого в списке выберите файлы и в контекстном меню кнопки **Удалить** выберите пункт **Удалить правило и расшифровать файлы**.

Вы можете удалять сразу несколько элементов из списка для шифрования. Для этого, удерживая клавишу **CTRL**, левой клавишей мыши выберите нужные элементы и в контекстном меню кнопки **Удалить** выберите пункт **Удалить правило и расшифровать файлы**.

Удаленные из списка для шифрования файлы и папки автоматически добавляются в список для расшифровки.

8. Сформируйте список файлов для расшифровки (см. раздел "Формирование правила расшифровки" на стр. [230](#)).
9. Сохраните внесенные изменения.

Сразу после применения политики Kaspersky Endpoint Security расшифровывает зашифрованные файлы, добавленные в список для расшифровки.

Kaspersky Endpoint Security расшифровывает зашифрованные файлы, если их параметры (путь к файлу / название файла / расширение файла) изменяются и начинают удовлетворять параметрам объектов, добавленных в список для расшифровки.

Kaspersky Endpoint Security откладывает расшифровку открытых файлов до тех пор, пока они не будут закрыты.

Создание зашифрованных архивов

Для защиты данных при передаче файлов пользователям вне корпоративной сети вы можете использовать зашифрованные архивы. Зашифрованные архивы удобно использовать для передачи файлов большого размера с помощью съемных дисков, так как почтовые программы имеют ограничения по размеру файла.

Перед созданием зашифрованных архивов Kaspersky Endpoint Security запросит у пользователя пароль. Для обеспечения надежной защиты данных вы можете включить проверку сложности паролей и выбрать критерии сложности. Таким образом, пользователю будет запрещено использовать короткие и простые пароли, например, 1234.

► *Чтобы включить проверку сложности пароля при создании зашифрованных архивов, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Общие параметры шифрования**.
6. В блоке **Параметры паролей** нажмите на кнопку **Настройка**.
7. В открывшемся окне выберите закладку **Зашифрованные архивы**.
8. Настройте параметры сложности пароля при создании зашифрованных архивов.


Вы можете создавать зашифрованные архивы на компьютерах с установленной программой Kaspersky Endpoint Security с функцией шифрования файлов.

При добавлении в зашифрованный архив файла, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security загружает содержимое этого файла и осуществляет шифрование.

► *Чтобы создать зашифрованный архив, выполните следующие действия:*

1. В любом файловом менеджере выделите файлы или папки, которые вы хотите добавить в зашифрованный архив. По правой клавише мыши откройте их контекстное меню.
2. Выберите пункт **Создать зашифрованный архив** в контекстном меню (см. рис. ниже).
3. В открывшемся окне выберите место для сохранения зашифрованного архива на съемном диске, задайте имя и нажмите на кнопку **Сохранить**.
4. В открывшемся окне задайте пароль и повторите его.
Пароль должен соответствовать критериям сложности, заданным в политике.
5. Нажмите на кнопку **Создать**.

Запустится процесс создания зашифрованного архива. В процессе создания зашифрованного архива Kaspersky Endpoint Security не выполняет сжатие файлов. По завершении процесса в указанном месте

на диске будет создан самораспаковывающийся защищенный паролем зашифрованный архив (исполняемый файл с расширением exe) – .

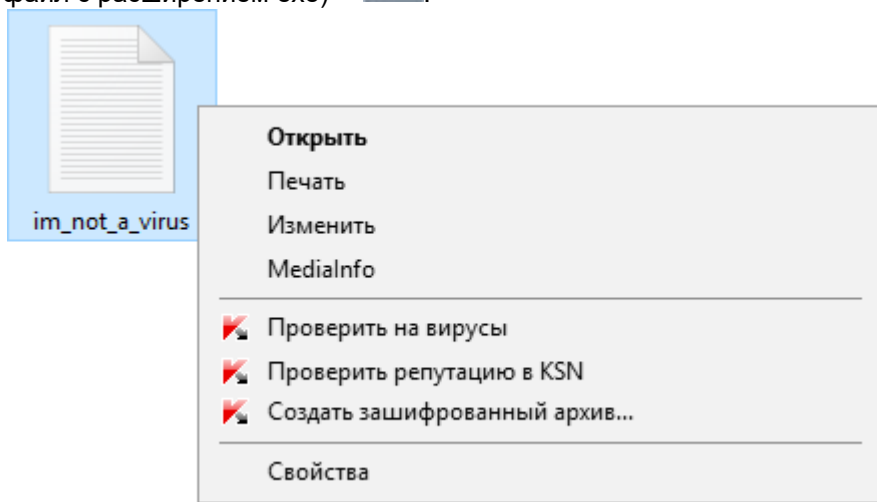


Рисунок 21. Контекстное меню файла

Для получения доступа к файлам в зашифрованном архиве нужно запустить мастер распаковки архива двойным щелчком мыши и ввести пароль. Если вы забыли пароль, восстановить доступ к файлам в зашифрованном архиве невозможно. Вы можете создать зашифрованный архив повторно.

Восстановление доступа к зашифрованными файлам

При шифровании файлов Kaspersky Endpoint Security получает ключ шифрования, необходимый для прямого доступа к зашифрованным файлам. С помощью ключа шифрования пользователь, работающий под любой из учетных записей Windows, которая была активной во время шифрования файлов, может получить прямой доступ к зашифрованным файлам. Пользователям, работающим под учетными записями Windows, которые были неактивны во время шифрования файлов, требуется связь с Kaspersky Security Center для доступа к зашифрованным файлам.

Зашифрованные файлы могут быть недоступны в следующих случаях:

- На компьютере пользователя присутствуют ключи шифрования, но нет связи с Kaspersky Security Center для работы с ними. В этом случае пользователю требуется запросить доступ к зашифрованным файлам у администратора локальной сети организации.

При отсутствии связи с Kaspersky Security Center требуется:

- для доступа к зашифрованным файлам на жестких дисках компьютера запросить один ключ доступа;
- для доступа к зашифрованным файлам на съемных дисках запросить ключ доступа к зашифрованным файлам для каждого съемного диска.
- С компьютера пользователя удалены компоненты шифрования. В этом случае пользователь может открыть зашифрованные файлы на локальных дисках и съемных дисках, но содержимое файлов отображается как зашифрованное.

Пользователь может работать с зашифрованными файлами при следующих условиях:

- Файлы помещены в зашифрованные архивы (см. раздел "Создание зашифрованных архивов" на стр. [232](#)), созданные на компьютере с установленной программой Kaspersky Endpoint Security.
- Файлы хранятся на съемных дисках, для которых разрешена работа в портативном режиме (см. раздел "Портативный режим для работы с зашифрованными файлами на съемных дисках" на стр. [242](#)).

Для получения доступ к зашифрованным файлам пользователю нужно запустить процедуру восстановления ("Запрос - Ответ").

Восстановление доступ к зашифрованным файлам состоит из следующих этапов:

1. Пользователь отправляет администратору файл запроса (см. рис. ниже).
2. Администратор добавляет файл запроса в Kaspersky Security Center, создает файл ключа доступа и отправляет файл пользователю.
3. Пользователь добавляет файл ключа доступа в Kaspersky Endpoint Security и получает доступ к файлам.

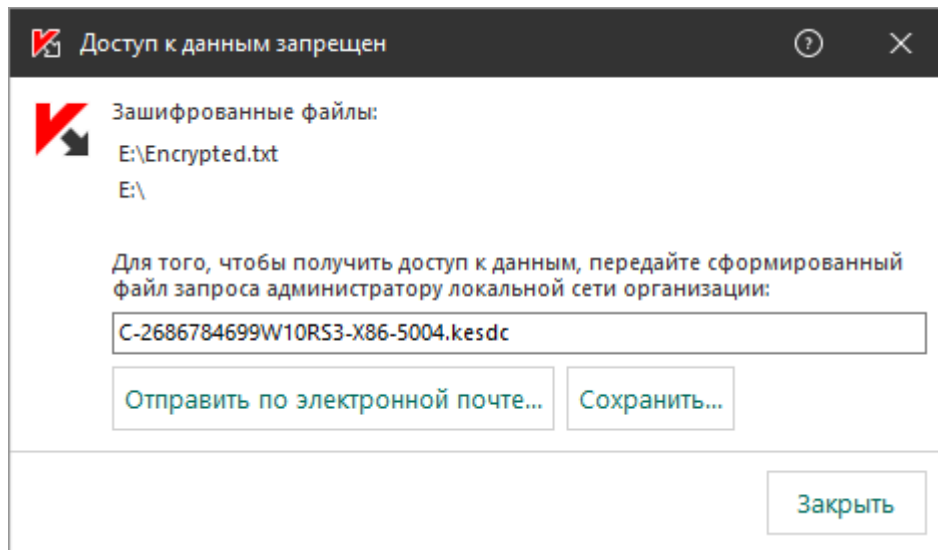


Рисунок 22. Восстановление доступа к зашифрованным файлам

Для запуска процедуры восстановления пользователю нужно обратиться к файлу. В результате Kaspersky Endpoint Security создаст файл запроса (файл с расширением kesdc), который пользователю нужно передать администратору, например, по электронной почте.

Kaspersky Endpoint Security формирует файл запроса доступа ко всем зашифрованным файлам, хранящимся на диске компьютера (локальном диске или съемном диске).

► Чтобы получить файл ключа доступа к зашифрованным данным, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Шифрование данных**.
7. На закладке **Шифрование данных** нажмите на кнопку **Обзор**.
8. В окне выбора файла запроса укажите путь к файлу, полученного от пользователя.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.

После получения файла ключа доступа к зашифрованным данным пользователю нужно запустить файл двойным щелчком мыши. В результате Kaspersky Endpoint Security предоставит доступ ко всем зашифрованным файлам, хранящимся на диске. Для получения доступа к зашифрованным файлам, хранящимся на других дисках, требуется получить отдельные ключи доступа для этих дисков.

Восстановление доступа к зашифрованным данным в случае выхода из строя операционной системы

Восстановление доступа к данным в случае выхода из строя операционной системы доступно только при шифровании файлов (FLE). Восстановить доступ к данным при полнодисковом шифровании (FDE) невозможно.

► Чтобы восстановить доступ к зашифрованным данным в случае выхода из строя операционной системы, выполните следующие действия:

1. Переустановите операционную систему, не форматировав жесткий диск.
2. Установите Kaspersky Endpoint Security.
3. Установите связь между компьютером и Сервером администрирования Kaspersky Security Center, под управлением которого находился компьютер во время шифрования данных.

Доступ к зашифрованным данным будет предоставлен на тех же условиях, которые действовали до выхода операционной системы из строя.

Изменение шаблонов сообщений для получения доступа к зашифрованным файлам

► Чтобы изменить шаблоны сообщений для получения доступа к зашифрованным файлам, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Общие параметры шифрования**.
6. В блоке **Шаблоны** нажмите на кнопку **Шаблоны**.

Откроется окно **Шаблоны**.

7. Выполните следующие действия:

- Если вы хотите изменить шаблон сообщения пользователя, выберите закладку **Сообщение пользователя**. Когда пользователь обращается к зашифрованному файлу при отсутствии на компьютере ключа доступа к зашифрованным файлам, открывается окно **Доступ к данным запрещен**. При нажатии на кнопку **Отправить по электронной почте** окна **Доступ к данным запрещен** автоматически формируется сообщение пользователя. Это сообщение отправляется администратору локальной сети организации вместе с файлом запроса доступа к зашифрованным файлам.
- Если вы хотите изменить шаблон сообщения администратора, выберите закладку **Сообщение администратора**. Это сообщение автоматически формируется при нажатии на кнопку **Отправить по электронной почте** окна **Запрос доступа к зашифрованным файлам** и приходит к пользователю после предоставления ему доступа к зашифрованным файлам.

8. Измените шаблоны сообщений.

Вы можете использовать кнопку **По умолчанию** и раскрывающийся список **Переменная**.

9. Сохраните внесенные изменения.

Шифрование съемных дисков

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Kaspersky Endpoint Security поддерживает шифрование файлов в файловых системах FAT32 и NTFS.

Если к компьютеру подключен съемный диск с неподдерживаемой файловой системой, то шифрование этого съемного диска завершается с ошибкой и Kaspersky Endpoint Security устанавливает статус доступа "только чтение" для этого съемного диска.

Для защиты данных на съемных дисках вы можете использовать следующие виды шифрования:

- Полнодисковое шифрование (англ. Full Disk Encryption – FDE).

Шифрование всего съемного диска, включая файловую систему.

Получить доступ к зашифрованным данным вне корпоративной сети невозможно. Также невозможно получить доступ к зашифрованным данным внутри корпоративной сети, если компьютер не подключен к Kaspersky Security Center ("гостевой" компьютер).

- Шифрование файлов (англ. File Level Encryption – FLE).

Шифрование только файлов на съемном диске. Файловая система при этом остается без изменений.

Шифрование файлов на съемных дисках предоставляет возможность доступа к данным за пределами корпоративной сети с помощью специального режима – *портативный режим* (см. раздел "*Портативный режим для работы с зашифрованными файлами на съемных дисках*" на стр. [242](#)).

Во время шифрования Kaspersky Endpoint Security создает мастер-ключ. Kaspersky Endpoint Security сохраняет мастер-ключ в следующих хранилищах:

- Kaspersky Security Center.
- Компьютер пользователя.
Мастер-ключ зашифрован секретным ключом пользователя.
- Съёмный диск.
Мастер-ключ зашифрован открытым ключом Kaspersky Security Center.

После завершения шифрования данные на съёмном диске доступны внутри корпоративной сети как при использовании обычного съёмного диска без шифрования.

Получение доступа к зашифрованным данным

При подключении съёмного диска с зашифрованными данными Kaspersky Endpoint Security выполняет следующие действия:

1. Проверяет наличие мастер-ключа в локальном хранилище на компьютере пользователя.
Если мастер-ключ найден, пользователь получает доступ к данным на съёмном диске.
Если мастер-ключ не найден, Kaspersky Endpoint Security выполняет следующие действия:
 - a. Отправляет запрос в Kaspersky Security Center.
После получения запроса Kaspersky Security Center отправляет ответ, который содержит мастер-ключ.
 - b. Kaspersky Endpoint Security сохраняет мастер-ключ в локальном хранилище на компьютере пользователя для дальнейшей работы с зашифрованным съёмным диском.
2. Расшифровывает данные.

Особенности шифрования съёмных дисков

Шифрование съёмных дисков имеет следующие особенности:

- Политика с заданными параметрами шифрования съёмных дисков формируется для определенной группы управляемых компьютеров. Поэтому результат применения политики Kaspersky Security Center с настроенным шифрованием / расшифровкой съёмных дисков зависит от того, к какому компьютеру подключен съёмный диск.
- Kaspersky Endpoint Security не выполняет шифрование / расшифровку файлов со статусом доступа "только чтение", хранящихся на съёмных дисках.
- В качестве съёмных дисков поддерживаются следующие типы устройств:
 - носители информации, подключаемые по шине USB;
 - жесткие диски, подключаемые по шинам USB и FireWire;
 - SSD-диски, подключаемые по шинам USB и FireWire.

В этом разделе

Запуск шифрования съемных дисков	238
Добавление правила шифрования для съемных дисков	240
Изменение правила шифрования для съемных дисков	241
Портативный режим для работы с зашифрованными файлами на съемных дисках	242
Расшифровка съемных дисков	246

Запуск шифрования съемных дисков

Вы можете расшифровать съемный диск с помощью политики. Политика с заданными параметрами шифрования съемных дисков формируется для определенной группы администрирования. Поэтому результат расшифровки данных на съемных дисках зависит от того, к какому компьютеру подключен съемный диск.

Kaspersky Endpoint Security поддерживает шифрование файловых систем FAT32 и NTFS. Если к компьютеру подключен съемный диск с неподдерживаемой файловой системой, шифрование съемного диска завершится с ошибкой и Kaspersky Endpoint Security установит для этого съемного диска право доступа "только чтение".

► Чтобы зашифровать съемные диски, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование съемных дисков**.
6. В раскрывающемся списке **Режим шифрования** выберите действие, которое по умолчанию выполняет Kaspersky Endpoint Security со съемными дисками:
 - **Шифровать весь съемный диск (FDE)**. Kaspersky Endpoint Security посекторно шифрует содержимое съемного диска. Таким образом, зашифрованными оказываются не только файлы, которые хранятся на съемном диске, но и файловые системы, включая имена файлов и структуры папок на съемном диске.
 - **Шифровать все файлы (FLE)**. Kaspersky Endpoint Security шифрует все файлы, которые хранятся на съемных дисках. Программа не шифрует файловые системы съемных дисков, включая имена файлов и структуры папок.
 - **Шифровать только новые файлы (FLE)**. Kaspersky Endpoint Security шифрует только те файлы, которые были добавлены на съемные диски или которые хранились на съемных дисках и были изменены после последнего применения политики Kaspersky Security Center.

Kaspersky Endpoint Security повторно не шифрует уже зашифрованный съемный диск.

7. Если вы хотите использовать портативный режим (см. раздел "Портативный режим для работы с зашифрованными файлами на съемных дисках" на стр. [242](#)) для шифрования съемных дисков, установите флажок **Портативный режим**.

Портативный режим – режим шифрования файлов (FLE) на съемных дисках, который предоставляет возможность доступа к данным за пределами корпоративной сети. Также портативный режим позволяет работать с зашифрованными данными на компьютерах, на которых не установлена программа Kaspersky Endpoint Security.

8. Если вы хотите зашифровать новый съемный диск, рекомендуется установить флажок **Шифровать только занятое пространство**. Если флажок снят, Kaspersky Endpoint Security зашифрует все файлы, в том числе остатки удаленных или измененных файлов.
9. Если вы хотите настроить шифрование для отдельных съемных дисков, задайте правила шифрования (см. раздел "Добавление правила шифрования для съемных дисков" на стр. [240](#)).
10. Если вы хотите использовать полнодисковое шифрование съемных дисков в офлайн-режиме, установите флажок **Разрешать шифрование съемных дисков в офлайн-режиме**.

Офлайн-режим шифрования – режим шифрования съемных дисков (FDE) при отсутствии связи с Kaspersky Security Center. При шифровании Kaspersky Endpoint Security сохраняет мастер-ключ только на компьютере пользователя. Kaspersky Endpoint Security отправит мастер-ключ в Kaspersky Security Center при следующей синхронизации.

Если компьютер, на котором сохранен мастер-ключ, поврежден и данные в Kaspersky Security Center не отправлены, получить доступ к съемному диску невозможно.

Если флажок **Разрешать шифрование съемных дисков в офлайн-режиме** снят и подключение к Kaspersky Security Center отсутствует, шифрование съемного диска невозможно.

11. Сохраните внесенные изменения.

В результате применения политики, если пользователь подключает съемный диск или съемный диск уже подключен, Kaspersky Endpoint Security запрашивает подтверждение для выполнения операции шифрования (см. рис. ниже).

Программа позволяет выполнить следующие действия:

- Если пользователь подтверждает запрос на шифрование, Kaspersky Endpoint Security шифрует данные.
- Если пользователь отклоняет запрос на шифрование, Kaspersky Endpoint Security оставляет данные без изменений и устанавливает для этого съемного диска право доступа "только чтение".
- Если пользователь не отвечает на запрос на шифрование, Kaspersky Endpoint Security оставляет данные без изменений и устанавливает для этого съемного диска право доступа "только чтение". Программа повторно запрашивает подтверждение при последующем применении политики или при последующем подключении этого съемного диска.

Если во время шифрования данных пользователь инициирует безопасное извлечение съемного диска, Kaspersky Endpoint Security прерывает шифрование данных и позволяет извлечь съемный диск до завершения операции шифрования. Шифрование данных будет продолжено при следующем подключении съемного диска к этому компьютеру.

Если шифрование съемного диска не удалось, просмотрите отчет **Шифрование данных** в интерфейсе Kaspersky Endpoint Security. Доступ к файлам может быть заблокирован другой программой. В этом случае попробуйте извлечь и заново подключить съемный диск к компьютеру.

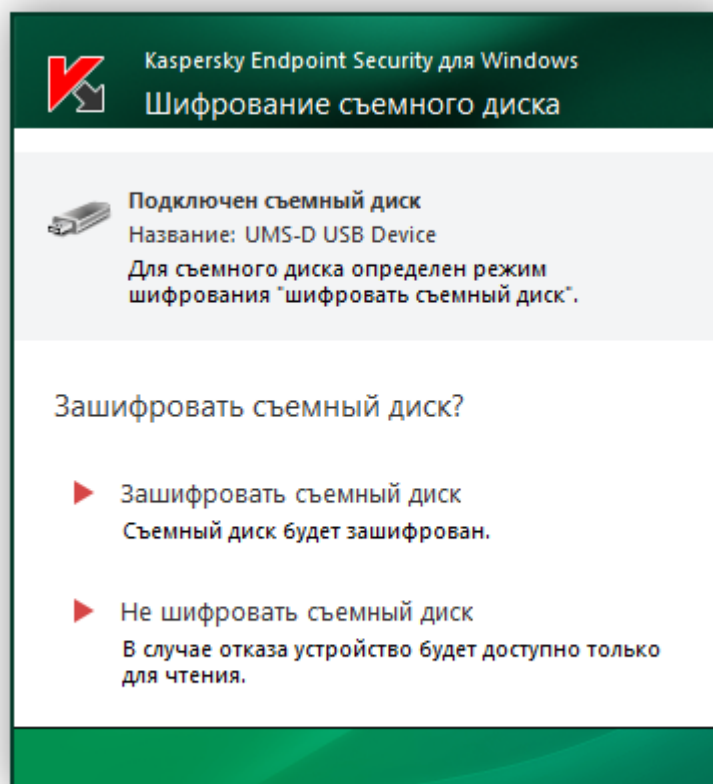


Рисунок 23. Уведомление о шифровании съемного диска

Добавление правила шифрования для съемных дисков

► Чтобы добавить правило шифрования для съемных дисков, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование съемных дисков**.

6. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите один из следующих элементов:
 - Если вы хотите добавить правила шифрования для съемных дисков, которые находятся в списке доверенных устройств компонента Контроль устройств, выберите элемент **Из списка доверенных устройств данной политики**.
 - Если вы хотите добавить правила шифрования для съемных дисков, которые находятся в списке Kaspersky Security Center, выберите элемент **Из списка устройств Kaspersky Security Center**.

7. В раскрывающемся списке **Режим шифрования для выбранных устройств** выберите действие, которое выполняет Kaspersky Endpoint Security с файлами, хранящимися на выбранных съемных дисках.
8. Установите флажок **Портативный режим**, если вы хотите, чтобы перед шифрованием Kaspersky Endpoint Security выполнял подготовку съемных дисков к работе с зашифрованными на них файлами в портативном режиме.

Портативный режим позволяет работать с зашифрованными файлами съемных дисков на компьютерах с недоступной функциональностью шифрования (см. стр. [233](#)).

9. Установите флажок **Шифровать только занятое пространство**, если вы хотите, чтобы Kaspersky Endpoint Security шифровал только те секторы диска, которые заняты файлами.

Если вы применяете шифрование на уже используемом диске, рекомендуется зашифровать весь диск. Это гарантирует защиту всех данных - даже удаленных, но еще содержащих извлекаемые сведения. Функцию **Шифровать только занятое пространство** рекомендуется использовать для новых, ранее не использовавшихся дисков.

Если устройство было зашифровано ранее с использованием функции **Шифровать только занятое пространство**, после применения политики в режиме **Шифровать весь съемный диск** секторы, не занятые файлами, по-прежнему не будут зашифрованы.

10. В раскрывающемся списке **Действие для устройств, выбранных ранее** выберите действие, выполняемое Kaspersky Endpoint Security с правилами шифрования, которые были определены для съемных дисков ранее:
 - Если вы хотите, чтобы созданное ранее правило шифрования съемного диска осталось без изменений, выберите элемент **Пропустить**.
 - Если вы хотите, чтобы созданное ранее правило шифрования съемного диска было заменено новым правилом, выберите элемент **Обновить**.

11. Сохраните внесенные изменения.

Добавленные правила шифрования съемных дисков будут применены к съемным дискам, подключенным к любым компьютерам организации.

Изменение правила шифрования для съемных дисков

► Чтобы изменить правило шифрования для съемного диска, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование съемных дисков**.
6. В списке съемных дисков, для которых определены правила шифрования, выберите запись о нужном вам съемном диске.
7. Нажмите на кнопку **Задать правило**, чтобы изменить правило шифрования для этого съемного диска.

Откроется контекстное меню кнопки **Задать правило**.

8. В контекстном меню кнопки **Задать правило** выберите действие, которое выполняет Kaspersky Endpoint Security с файлами на выбранном съемном диске.
9. Сохраните внесенные изменения.

Измененные правила шифрования съемных дисков будут применены к съемным дискам, подключенным к любым компьютерам, работающим под управлением измененной политики Kaspersky Security Center.

Портативный режим для работы с зашифрованными файлами на съемных дисках

Портативный режим – режим шифрования файлов (FLE) на съемных дисках, который предоставляет возможность доступа к данным за пределами корпоративной сети. Также портативный режим позволяет работать с зашифрованными данными на компьютерах, на которых не установлена программа Kaspersky Endpoint Security.

Портативный режим удобно использовать в следующих случаях:

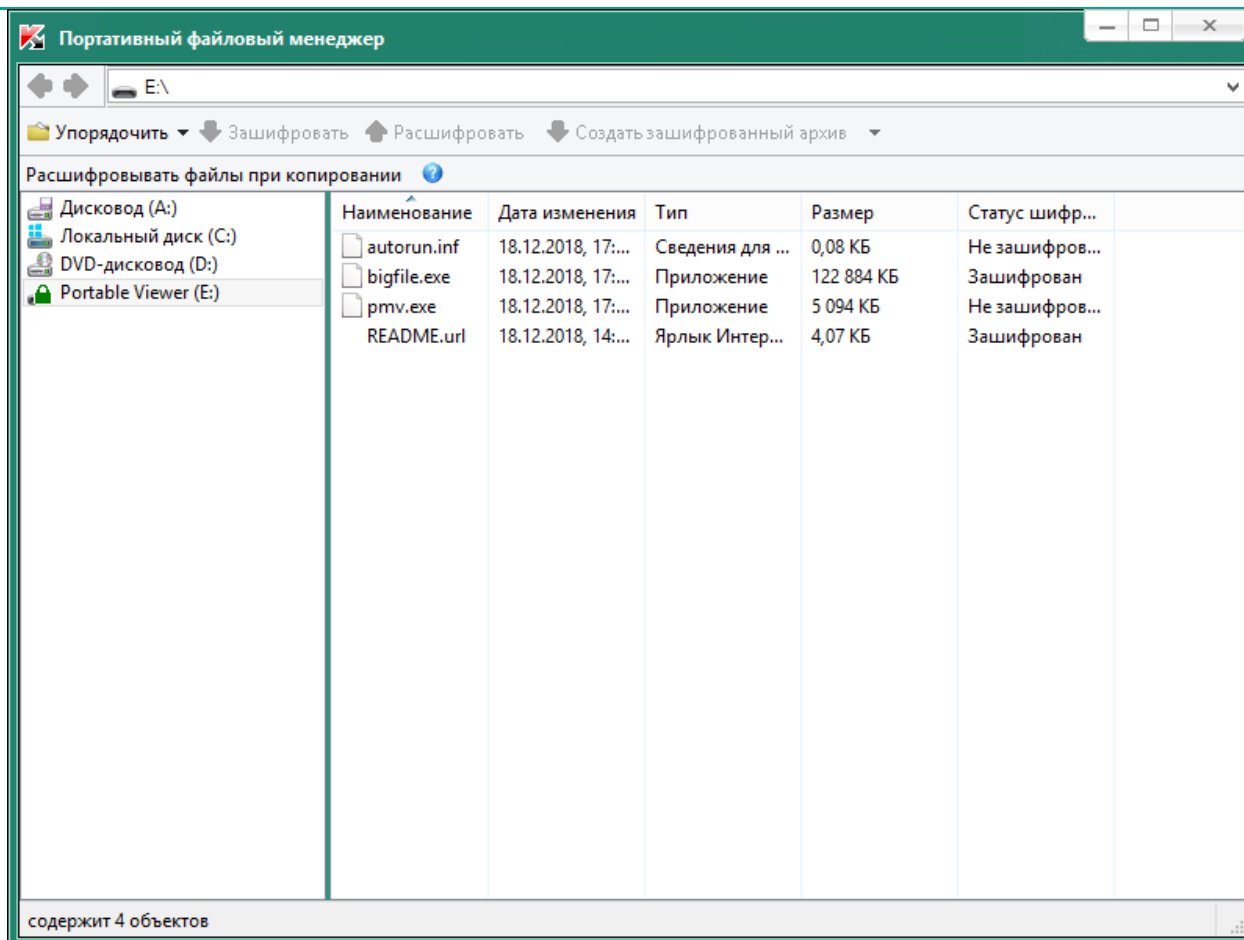
- Нет связи между компьютером и Сервером администрирования Kaspersky Security Center.
- Изменилась инфраструктура со сменой Сервера администрирования Kaspersky Security Center.
- На компьютере не установлена программа Kaspersky Endpoint Security.

Портативный файловый менеджер

Для работы в портативном режиме Kaspersky Endpoint Security устанавливает на съемный диск специальный модуль шифрования – *портативный файловый менеджер*. Портативный файловый менеджер предоставляет интерфейс для работы с зашифрованными данными, если на компьютере не установлена программа Kaspersky Endpoint Security (см. рис. ниже). Если на компьютере установлена программа Kaspersky Endpoint Security, вы можете работать с зашифрованными съемными дисками с помощью обычных файлового менеджера (например, Проводника).

Портативный файловый менеджер хранит ключ для шифрования файлов на съемном диске. Ключ зашифрован паролем пользователя. Пользователь задает пароль перед шифрованием файлов на съемном диске.

Портативный файловый менеджер запускается автоматически при подключении съемного диска к компьютеру, на котором не установлена программа Kaspersky Endpoint Security. Если на компьютере выключен автозапуск программ, запустите портативный файловый менеджер вручную. Для этого запустите файл pmv.exe, который хранится на съемном диске.



Поддержка портативного режима для работы с зашифрованными файлами

► Чтобы включить поддержку портативного режима для работы с зашифрованными файлами на съемных дисках, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование съемных дисков**.
6. В раскрывающемся списке **Режим шифрования для выбранных устройств** выберите элемент **Шифровать все файлы** или элемент **Шифровать только новые файлы**.

Портативный режим доступен только при шифровании файлов (FLE). Включить поддержку портативного режима для полнодискового шифрования (FDE) невозможно.

7. Установите флажок **Портативный режим**.
8. Если нужно, добавьте правила шифрования для отдельных съемных дисков (см. раздел "Добавление правила шифрования для съемных дисков" на стр. [240](#)).
9. Сохраните внесенные изменения.
10. После применения политики подключите съемный диск к компьютеру.
11. Подтвердите операцию шифрования съемного диска.
Откроется окно создания пароля для портативного файлового менеджера.
12. Задайте пароль, соответствующий требованиям к уровню сложности, и подтвердите его.
13. Нажмите на кнопку **ОК**.

Kaspersky Endpoint Security зашифрует файлы на съемном диске. Портативный файловый менеджер для работы с зашифрованными файлами будет также добавлен на съемный диск. Если на съемном диске уже есть зашифрованные файлы, то Kaspersky Endpoint Security зашифрует их повторно с помощью собственного ключа. Это позволяет пользователю получить доступ ко всем файлам на съемном диске в портативном режиме.

Получение доступа к зашифрованным файлам на съемном диске

После шифрования файлов на съемном диске с поддержкой портативного режима доступны следующие способы доступа к файлам:

- Если на компьютере не установлена программа Kaspersky Endpoint Security, портативный файловый менеджер предложит ввести пароль. Пароль нужно будет вводить при каждой перезагрузке компьютера или переподключении съемного диска.
- Если компьютер находится за пределами корпоративной сети и на компьютере установлена программа Kaspersky Endpoint Security, программа предложит ввести пароль или отправить запрос на доступ к файлам администратору. После получения доступа к файлам на съемном диске Kaspersky Endpoint Security сохранит секретный ключ в хранилище ключей компьютера. Это позволит в дальнейшем получить доступ к файлам без ввода пароля или запроса администратору.
- Если компьютер находится внутри корпоративной сети и на компьютере установлена программа Kaspersky Endpoint Security, вы получите доступ к устройству без ввода пароля. Kaspersky Endpoint Security получит секретный ключ от Сервера администрирования Kaspersky Security Center к которому подключен компьютер.

Восстановление пароля для работы в портативном режиме

Если вы забыли пароль для работы в портативном режиме, вам нужно подключить съемный диск к компьютеру с установленной программой Kaspersky Endpoint Security внутри корпоративной сети. Вы получите доступ к файлам, так как в хранилище ключей компьютера или на Сервере администрирования сохранен секретный ключ. Расшифруйте и снова зашифруйте файлы с новым паролем.

Особенности работы портативного режима при подключении съемного диска к компьютеру из другой сети

Если компьютер находится за пределами корпоративной сети и на компьютере установлена программа Kaspersky Endpoint Security, вы можете получить доступ к файлам следующими способами:

- **Доступ по паролю**

После ввода пароля вы сможете просматривать, изменять и сохранять файлы на съемном диске (*прозрачный доступ*). Kaspersky Endpoint Security может установить для съемного диска право доступа "только чтение", если в параметрах политики для шифрования съемных дисков настроены следующие параметры:

- Выключена поддержка портативного режима.
- Выбран режим **Шифровать все файлы** или **Шифровать только новые файлы**.

В остальных случаях вы получите полный доступ к съемному диску (право "чтение и запись"). Вам будет доступно добавление и удаление файлов.

Вы можете изменить права доступа к съемному диску, даже если съемный диск подключен к компьютеру. Если права доступа к съемному диску изменились, Kaspersky Endpoint Security заблокирует доступ к файлам и запросит пароль повторно.

После ввода пароля применить параметры политики шифрования для съемного диска невозможно. Таким образом, расшифровать или перешифровать файлы на съемном диске невозможно.

- **Запрос доступа к файлам у администратора**

Если вы забыли пароль для работы в портативном режиме, запросите доступ к файлам у администратора. Для доступа к файлам пользователю нужно отправить файл запроса (файл с расширением kesdc) администратору. Пользователь может отправить файл запроса, например, по электронной почте. Администратор отправит файл доступа к зашифрованным данным (файл с расширением kesdr).

После прохождения процедуры восстановления пароля ("Запрос - Ответ") вы получите прозрачный доступ к файлам на съемном диске и полный доступ к съемному диску (право "запись и чтение").

Вы можете применить политику для шифрования съемных дисков и, например, расшифровать файлы. После восстановления пароля или при обновлении политики программа Kaspersky Endpoint Security предложит подтвердить изменения.

► *Чтобы получить файл доступа к зашифрованным данным, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Шифрование данных**.
7. На закладке **Шифрование данных** нажмите на кнопку **Обзор**.
8. В окне выбора файла запроса укажите путь к файлу, полученного от пользователя.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.

Расшифровка съемных дисков

Вы можете расшифровать съемный диск с помощью политики. Политика с заданными параметрами шифрования съемных дисков формируется для определенной группы администрирования. Поэтому результат расшифровки данных на съемных дисках зависит от того, к какому компьютеру подключен съемный диск.

► *Чтобы расшифровать съемные диски, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование съемных дисков**.
6. Если вы хотите расшифровать все зашифрованные файлы, хранящиеся на съемных дисках, в раскрывающемся списке **Режим шифрования** выберите действие **Расшифровывать весь съемный диск**.
7. Если вы хотите расшифровать данные, хранящиеся на отдельных съемных дисках, измените правила шифрования съемных дисков, данные которых вы хотите расшифровать. Для этого выполните следующие действия:
 - a. В списке съемных дисков, для которых определены правила шифрования, выберите запись о нужном вам съемном диске.
 - b. Нажмите на кнопку **Задать правило**, чтобы изменить правило шифрования для этого съемного диска.
Откроется контекстное меню кнопки **Задать правило**.
 - c. В контекстном меню кнопки **Задать правило** выберите пункт **Расшифровывать все файлы**.
8. Сохраните внесенные изменения.

В результате, если пользователь подключает съемный диск или он уже подключен, Kaspersky Endpoint Security расшифровывает съемный диск. Программа предупреждает пользователя, что процедура расшифровки может занять некоторое время. Если во время расшифровки данных пользователь инициирует безопасное извлечение съемного диска, Kaspersky Endpoint Security прерывает расшифровку данных и позволяет извлечь съемный диск до завершения операции расшифровки. Расшифровка данных будет продолжена после следующего подключения съемного диска к компьютеру.

Если расшифровка съемного диска не удалась, просмотрите отчет **Шифрование данных** в интерфейсе Kaspersky Endpoint Security. Доступ к файлам может быть заблокирован другой программой. В этом случае попробуйте извлечь и заново подключить съемный диск к компьютеру.

Работа с Агентом аутентификации

Если системные жесткие диски зашифрованы, перед загрузкой операционной системы загружается Агент аутентификации. С помощью Агента аутентификации требуется пройти процедуру аутентификации для получения доступа к зашифрованным системным жестким дискам и загрузки операционной системы.

После успешного прохождения процедуры аутентификации загружается операционная система. При последующих перезагрузках операционной системы требуется повторно проходить процедуру аутентификации.

Возможны случаи, когда пользователь не может пройти процедуру аутентификации. Например, аутентификация невозможна, если пользователь забыл учетные данные Агента аутентификации, пароль от токена или смарт-карты или потерял токен или смарт-карту.

Если пользователь забыл учетные данные Агента аутентификации или пароль от токена или смарт-карты, то для восстановления требуется обратиться к администратору локальной сети организации.

Если пользователь потерял токен или смарт-карту, администратору требуется добавить файл электронного сертификата (см. раздел "Использование токена и смарт-карты при работе с Агентом аутентификации" на стр. [253](#)) нового токена или новой смарт-карты в команду для создания учетной записи Агента аутентификации. После этого пользователю требуется пройти процедуру получения доступа к зашифрованным устройствам или восстановления данных на зашифрованных устройствах (см. раздел "Работа с зашифрованными устройствами при отсутствии доступа к ним" на стр. [260](#)).

В этом разделе

Включение использования технологии единого входа (SSO)	247
Управление учетными записями Агента аутентификации	248
Использование токена и смарт-карты при работе с Агентом аутентификации	253
Выбор уровня трассировки Агента аутентификации	253
Изменение справочных текстов Агента аутентификации	254
Удаление объектов и данных, оставшихся после тестовой работы Агента аутентификации.....	256

Включение использования технологии единого входа (SSO)

Технология единого входа (англ. Single Sign-On – SSO) позволяет выполнить автоматический вход в операционную систему с помощью учетных данных Агента аутентификации.

При использовании технологии единого входа Агент аутентификации игнорирует требования к надежности пароля, заданные в Kaspersky Security Center. Вы можете задать требования к надежности пароля в параметрах операционной системы.

Технология единого входа несовместима со сторонними поставщиками учетных данных.

► Чтобы включить использование технологии единого входа, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Общие параметры шифрования**.
6. В блоке **Параметры паролей** нажмите на кнопку **Настройка**.
7. В открывшемся окне на закладке **Агент аутентификации** установите флажок **Использовать технологию единого входа (SSO)**.
8. Сохраните внесенные изменения.

В результате пользователю нужно пройти процедуру аутентификации только один раз с помощью агента. Проходить процедуру аутентификации для загрузки операционной системы не требуется. Операционная система загружается автоматически.

Для работы технологии единого входа пароль учетной записи Windows и пароль учетной записи Агента аутентификации должны совпадать. Если пароли не совпадают, то пользователю нужно выполнить процедуру аутентификации дважды: в интерфейсе Агента аутентификации и перед загрузкой операционной системы. После этого Kaspersky Endpoint Security заменит пароль учетной записи Windows на пароль учетной записи Агента аутентификации.

Управление учетными записями Агента аутентификации

Агент аутентификации нужен для работы с дисками, которые защищены с помощью технологии Шифрование диска Kaspersky (FDE). Перед загрузкой операционной системы пользователю нужно пройти аутентификацию с помощью агента. Для настройки параметров аутентификации пользователей предназначена задача *Управление учетными записями Агента аутентификации*. Вы можете использовать как локальные задачи для отдельных компьютеров, так и групповые задачи для компьютеров из отдельных групп администрирования или выборки компьютеров.

Настроить расписание запуска задачи *Управление учетными записями Агента аутентификации* невозможно. Также невозможно принудительно остановить выполнение задачи.

► Чтобы создать задачу *Управление учетными записями Агента аутентификации*, выполните следующие действия:

1. В Консоли администрирования перейдите в папку **Сервер администрирования** → **Задачи**.
Откроется список задач.
2. Нажмите на кнопку **Новая задача**.
Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (11.3.0)** → **Управление учетными записями Агента аутентификации**.

Шаг 2. Выбор команды управления учетными записями Агента аутентификации

Сформируйте список команд управления учетными записями Агента аутентификации. Команды управления позволяют добавлять, изменять и удалять учетный записи Агента аутентификации (см. инструкции ниже). Только пользователи, которые имеют учетную запись Агента аутентификации, могут пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. 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, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 5. Определение названия задачи

Введите название задачи, например, *Учетные записи администраторов*.

Шаг 6. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

В результате после выполнения задачи при следующей загрузке компьютера новый пользователь может пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Для добавления учетной записи Агента аутентификации нужно добавить специальную команду в задачу *Управление учетными записями Агента аутентификации*. Групповую задачу удобно использовать, например, для добавления учетной записи администратора на все компьютеры.

Kaspersky Endpoint Security позволяет автоматически создавать учетные записи Агента аутентификации перед шифрованием диска. Вы можете включить автоматическое создание учетных записей Агента аутентификации в параметрах политики полнодискового шифрования (см. раздел "Полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky" на стр. [213](#)). Также вы можете использовать технологию единого входа (SSO) (см. раздел "Включение использования технологии единого входа (SSO)" на стр. [247](#)).

► *Чтобы добавить учетную запись Агента аутентификации, выполните следующие действия:*

1. Откройте свойства задачи *Управление учетными записями Агента аутентификации*.
2. В свойствах задачи выберите раздел **Параметры**.
3. Нажмите на кнопку **Добавить** → **Команду для добавления учетной записи**.

4. В открывшемся окне в поле **Учетная запись Windows** укажите имя учетной записи Microsoft Windows, на основе которой будет создана учетная запись Агента аутентификации.
5. Если вы ввели имя учетной записи Windows вручную, нажмите на кнопку **Разрешить**, чтобы определить идентификатор безопасности учетной записи (англ. SID – Security Identifier).

Если вы не определяете идентификатор безопасности по кнопке **Разрешить**, то он будет определен в момент выполнения задачи на компьютере.

Определение идентификатора безопасности учетной записи Windows нужно для проверки корректности ввода имени учетной записи Windows. Если учетная запись Windows не существует на компьютере или в доверенном домене, задача *Управление учетными записями Агента аутентификации* будет завершена с ошибкой.

6. Установите флажок **Заменить существующую учетную запись**, если вы хотите, чтобы уже заведенная для Агента аутентификации учетная запись с таким же именем была заменена на добавляемую.

Этот шаг доступен, если вы добавляете команду для создания учетной записи Агента аутентификации в свойствах групповой задачи управления учетными записями Агента аутентификации. Этот шаг недоступен, если вы добавляете команду для создания учетной записи Агента аутентификации в свойствах локальной задачи **Шифрование всего носителя, управление учетными записями**.

7. В поле **Имя пользователя** введите имя учетной записи Агента аутентификации, которое требуется вводить при аутентификации для доступа к зашифрованным жестким дискам.
8. Установите флажок **Разрешать вход по паролю**, если вы хотите, чтобы при аутентификации для получения доступа к зашифрованным жестким дискам программа требовала пароль учетной записи Агента аутентификации. Задайте пароль учетной записи Агента аутентификации. Если нужно, вы можете запросить у пользователя новый пароль после первой аутентификации.
9. Установите флажок **Разрешать вход по сертификату**, если вы хотите, чтобы при аутентификации для доступа к зашифрованным жестким дискам программа требовала подключения токена или смарт-карты к компьютеру. Выберите файл сертификата для аутентификации с помощью смарт-карты или токена.
10. Если требуется, в поле **Описание команды** введите информацию об учетной записи Агента аутентификации, необходимую вам для работы с командой.
11. Выполните одно из следующих действий:
 - Выберите вариант **Разрешать аутентификацию**, если вы хотите, чтобы программа разрешала доступ к аутентификации в Агенте аутентификации пользователю, работающему под учетной записью, указанной в команде.
 - Выберите вариант **Запрещать аутентификацию**, если вы хотите, чтобы программа запрещала доступ к аутентификации в Агенте аутентификации пользователю, работающему под учетной записью, указанной в команде.
12. Сохраните внесенные изменения.

Для изменения пароля и других данных учетной записи Агента аутентификации нужно добавить специальную команду в задачу *Управление учетными записями Агента аутентификации*. Групповую задачу удобно использовать, например, для замены сертификата токена администратора на всех компьютерах.

► Чтобы изменить учетную запись Агента аутентификации, выполните следующие действия:

1. Откройте свойства задачи *Управление учетными записями Агента аутентификации*.
2. В свойствах задачи выберите раздел **Параметры**.
3. Нажмите на кнопку **Добавить** → **Команду для изменения учетной записи**.
4. В открывшемся окне в поле **Учетная запись Windows** укажите имя учетной записи пользователя Microsoft Windows, которую вы хотите изменить.
5. Если вы ввели имя учетной записи Windows вручную, нажмите на кнопку **Разрешить**, чтобы определить идентификатор безопасности учетной записи (англ. SID – Security Identifier).

Если вы не определяете идентификатор безопасности по кнопке **Разрешить**, то он будет определен в момент выполнения задачи на компьютере.

Определение идентификатора безопасности учетной записи Windows нужно для проверки корректности ввода имени учетной записи Windows. Если учетная запись Windows не существует на компьютере или в доверенном домене, задача *Управление учетными записями Агента аутентификации* будет завершена с ошибкой.

6. Установите флажок **Изменить имя пользователя** и введите новое имя учетной записи Агента аутентификации, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, программа Kaspersky Endpoint Security изменила имя пользователя на указанное в поле ниже.
7. Установите флажок **Изменить параметры входа по паролю**, если вы хотите сделать доступными для изменения параметры входа по паролю.
8. Установите флажок **Разрешать вход по паролю**, если вы хотите, чтобы при аутентификации для получения доступа к зашифрованным жестким дискам программа требовала пароль учетной записи Агента аутентификации. Задайте пароль учетной записи Агента аутентификации.
9. Установите флажок **Изменить правило смены пароля при аутентификации в Агенте аутентификации**, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, программа Kaspersky Endpoint Security изменила значение параметра смены пароля на установленное ниже.
10. Установите значение параметра смены пароля при аутентификации в Агенте аутентификации.
11. Установите флажок **Изменить параметры входа по сертификату**, если вы хотите сделать доступными для изменения параметры входа по электронному сертификату токена или смарт-карте.
12. Установите флажок **Разрешать вход по сертификату**, если вы хотите, чтобы при аутентификации для доступа к зашифрованным жестким дискам программа требовала ввод пароля к подключенному к компьютеру токenu или смарт-карте. Выберите файл сертификата для аутентификации с помощью смарт-карты или токена.
13. Установите флажок **Изменить описание команды** и измените описание команды, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, программа Kaspersky Endpoint Security изменила описание команды.
14. Установите флажок **Изменить правило доступа к аутентификации в Агенте аутентификации**, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, программа Kaspersky Endpoint Security изменила правило доступа пользователя к аутентификации в Агенте аутентификации на установленное ниже.

15. Установите правило доступа к аутентификации в Агенте аутентификации.
16. Сохраните внесенные изменения.

Для удаления учетной записи Агента аутентификации нужно добавить специальную команду в задачу *Управление учетными записями Агента аутентификации*. Групповую задачу удобно использовать, например, для удаления учетной записи уволенного сотрудника.

► *Чтобы удалить учетную запись Агента аутентификации, выполните следующие действия:*

1. Откройте свойства задачи *Управление учетными записями Агента аутентификации*.
2. В свойствах задачи выберите раздел **Параметры**.
3. Нажмите на кнопку **Добавить** → **Команду для удаления учетной записи**.
4. В открывшемся окне в поле **Учетная запись Windows** укажите имя учетной записи пользователя Windows, на основе которой создана учетная запись для Агента аутентификации, которую вы хотите удалить.
5. Если вы ввели имя учетной записи Windows вручную, нажмите на кнопку **Разрешить**, чтобы определить идентификатор безопасности учетной записи (англ. SID – Security Identifier).

Если вы не определяете идентификатор безопасности по кнопке **Разрешить**, то он будет определен в момент выполнения задачи на компьютере.

Определение идентификатора безопасности учетной записи Windows нужно для проверки корректности ввода имени учетной записи Windows. Если учетная запись Windows не существует на компьютере или в доверенном домене, задача *Управление учетными записями Агента аутентификации* будет завершена с ошибкой.

6. Сохраните внесенные изменения.

Для просмотра списка пользователей, которые могут пройти аутентификацию с помощью агента и загрузить операционную систему, нужно перейти в свойства управляемого компьютера.

► *Чтобы просмотреть список учетных записей Агента аутентификации, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел **Задачи**.
Откроется список локальных задач.
6. Выберите задачу **Управление учетными записями Агента аутентификации**.
7. В свойствах задачи выберите раздел **Параметры**.

В результате вам будет доступен список учетных записей Агента аутентификации на этом компьютере. Только пользователи из списка могут пройти аутентификацию с помощью агента и загрузить операционную систему.

Использование токена и смарт-карты при работе с Агентом аутентификации

При аутентификации для доступа к зашифрованным жестким дискам можно использовать токен или смарт-карту. Для этого необходимо добавить файл электронного сертификата токена или смарт-карты в задачу *Управление учетными записями Агента аутентификации*.

Использование токена или смарт-карты доступно, только если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES256. Если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES56, то в добавлении файла электронного сертификата в команду будет отказано.

Чтобы добавить файл электронного сертификата токена или смарт-карты в команду для создания учетной записи Агента аутентификации, его требуется предварительно сохранить с помощью стороннего программного обеспечения, предназначенного для управления сертификатами.

Сертификат токена или смарт-карты должен обладать следующими свойствами:

- Сертификат удовлетворяет стандарту X.509, а файл сертификата имеет кодировку DER.
- Сертификат содержит RSA-ключ длиной не менее 1024 бит.

Если электронный сертификат токена или смарт-карты не удовлетворяет этим требованиям, загрузить файл сертификата в команду для создания учетной записи Агента аутентификации невозможно.

Также параметр `KeyUsage` сертификата должен иметь значение `keyEncipherment` или `dataEncipherment`. Параметр `KeyUsage` определяет назначение сертификата. Если параметр имеет другое значение, Kaspersky Security Center загрузит файл сертификата, но покажет предупреждение.

Выбор уровня трассировки Агента аутентификации

Программа записывает служебную информацию о работе Агента аутентификации, а также информацию о действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.

► *Чтобы выбрать уровень трассировки Агента аутентификации, выполните следующие действия:*

1. Сразу после запуска компьютера с зашифрованными жесткими дисками по кнопке **F3** вызовите окно для настройки параметров Агента аутентификации.
2. В окне настройки параметров Агента аутентификации выберите уровень трассировки:
 - **Disable debug logging (default)**. Если выбран этот вариант, то программа не записывает информацию о событиях работы Агента аутентификации в файл трассировки.
 - **Enable debug logging**. Если выбран этот вариант, то программа записывает информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.

- **Enable verbose logging.** Если выбран этот вариант, то программа записывает детальную информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.

Уровень детализации записей для этого варианта выше, чем при выборе уровня **Enable debug logging**. Высокий уровень детализации записей может замедлять загрузку Агента аутентификации и операционной системы.

- **Enable debug logging and select serial port.** Если выбран этот вариант, то программа записывает информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки, а также передает ее через COM-порт.

Если компьютер с зашифрованными жесткими дисками соединен с другим компьютером через COM-порт, то события работы Агента аутентификации можно исследовать с помощью этого компьютера.

- **Enable verbose debug logging and select serial port.** Если выбран этот вариант, то программа записывает детальную информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки, а также передает ее через COM-порт.

Уровень детализации записей для этого варианта выше, чем при выборе уровня **Enable debug logging and select serial port**. Высокий уровень детализации записей может замедлять загрузку Агента аутентификации и операционной системы.

Запись в файл трассировки Агента аутентификации выполняется в случае, если на компьютере есть зашифрованные жесткие диски или выполняется полнодисковое шифрование.

Файл трассировки Агента аутентификации не передается в "Лабораторию Касперского", как другие файлы трассировки программы. При необходимости вы можете самостоятельно отправить файл трассировки Агента аутентификации в "Лабораторию Касперского" для анализа.

Изменение справочных текстов Агента аутентификации

Перед изменением справочных текстов Агента аутентификации ознакомьтесь со списком поддерживаемых символов в предзагрузочной среде (см. ниже).

► *Чтобы изменить справочные тексты Агента аутентификации, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Общие параметры шифрования**.

6. Нажмите на кнопку **Справка** в блоке **Шаблоны**.

Откроется окно **Справочные тексты Агента аутентификации**.

7. Выполните следующие действия:

- Выберите закладку **Аутентификация**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе ввода учетных данных.
- Выберите закладку **Смена пароля**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе смены пароля для учетной записи Агента аутентификации.
- Выберите закладку **Восстановление пароля**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе восстановления пароля для учетной записи Агента аутентификации.

8. Измените справочные тексты.

Если вы хотите восстановить исходный текст, нажмите на кнопку **По умолчанию**.

Вы можете ввести справочный текст, содержащий 16 или менее строк. Максимальная длина строки составляет 64 символа.

9. Сохраните внесенные изменения.

Ограничения поддержки символов в справочных текстах Агента аутентификации

В предзагрузочной среде поддерживаются следующие символы Unicode:

- основная латиница (0000 - 007F);
- дополнительные символы Latin-1 (0080 - 00FF);
- расширенная латиница-A (0100 - 017F);
- расширенная латиница-B (0180 - 024F);
- некомбинируемые протяженные символы-идентификаторы (02B0 - 02FF);
- комбинируемые диакритические знаки (0300 - 036F);
- греческий и коптский алфавиты (0370 - 03FF);
- кириллица (0400 - 04FF);
- иврит (0590 - 05FF);
- арабское письмо (0600 - 06FF);
- дополнительная расширенная латиница (1E00 - 1EFF);
- знаки пунктуации (2000 - 206F);
- символы валют (20A0 - 20CF);
- буквоподобные символы (2100 - 214F);
- геометрические фигуры (25A0 - 25FF);
- формы представления арабских букв-B (FE70 - FEFF).

Символы, не указанные в этом списке, не поддерживаются в предзагрузочной среде. Не рекомендуется использовать такие символы в справочных текстах Агента аутентификации.

Удаление объектов и данных, оставшихся после тестовой работы Агента аутентификации

Если в процессе удаления программы Kaspersky Endpoint Security обнаруживаются объекты и данные, оставшиеся на системном жестком диске после тестовой работы Агента аутентификации, то удаление программы прерывается и становится невозможным до тех пор, пока эти объекты и данные не будут удалены.

Объекты и данные могут остаться на системном жестком диске после тестовой работы Агента аутентификации только в исключительных ситуациях. Например, если после применения политики Kaspersky Security Center с установленными параметрами шифрования компьютер не перезагрузился или после тестовой работы Агента аутентификации программа не запускается.

Вы можете удалить объекты и данные, оставшиеся на системном жестком диске после тестовой работы Агента аутентификации, следующими способами:

- с помощью политики Kaspersky Security Center;
 - с помощью утилиты восстановления (см. раздел "Восстановление данных с помощью утилиты восстановления FDERT" на стр. [261](#)).
- *Чтобы удалить объекты и данные, оставшиеся после тестовой работы Агента аутентификации, с помощью политики Kaspersky Security Center, выполните следующие действия:*
1. Примените к компьютеру политику Kaspersky Security Center с установленными параметрами для расшифровки (см. раздел "Расшифровка жестких дисков" на стр. [217](#)) всех жестких дисков компьютера.
 2. Запустите Kaspersky Endpoint Security.
- *Чтобы удалить данные о несовместимости программы с Агентом аутентификации,*
- в командной строке введите команду `avp pbatestreset`.

Для выполнения команды `avp pbatestreset` требуются установленные компоненты шифрования данных.

Просмотр информации о шифровании данных

В процессе шифрования и расшифровки данных Kaspersky Endpoint Security отправляет на Kaspersky Security Center информацию о статусах применения параметров шифрования на клиентских компьютерах.

Возможны следующие статусы шифрования:

- *Не задана политика шифрования.* Для компьютера не назначена политика шифрования Kaspersky Security Center.
- *В процессе применения политики.* На компьютере выполняется шифрование и / или расшифровка данных.
- *Ошибка.* Во время шифрования и / или расшифровки данных на компьютере возникла ошибка.

- *Требуется перезагрузка.* Для инициализации или завершения шифрования или расшифровки данных на компьютере требуется перезагрузка операционной системы.
- *Соответствует политике.* Шифрование данных на компьютере выполнено в соответствии с параметрами шифрования, указанными в примененной к компьютеру политике Kaspersky Security Center.
- *Отменено пользователем.* Пользователь отказался подтвердить выполнение операции шифрования файлов на съемном диске.

В этом разделе

Просмотр статусов шифрования	257
Просмотр статистики шифрования на информационных панелях Kaspersky Security Center	258
Просмотр ошибок шифрования файлов на локальных дисках компьютера	259
Просмотр отчета о шифровании данных	259

Просмотр статусов шифрования

- *Чтобы просмотреть статус шифрования данных компьютера, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
На закладке **Устройства** в рабочей области отображаются свойства компьютеров выбранной группы администрирования.
4. На закладке **Устройства** рабочей области сдвиньте полосу прокрутки до упора вправо.
5. Если графа **Статус шифрования** не отображается, выполните следующие действия:
 - a. По правой клавиши мыши откройте контекстное меню для заголовочной части таблицы.
 - b. В контекстном меню в выпадающем списке **Вид** выберите **Добавить или удалить графы**.
Откроется окно **Добавление или удаление граф**.
 - c. В окне **Добавление или удаление граф** установите флажок **Статус шифрования**.
 - d. Нажмите на кнопку **ОК**.

В графе **Статус шифрования** отображаются статусы шифрования данных для компьютеров выбранной группы администрирования. Этот статус формируется на основе информации о шифровании файлов на локальных дисках компьютера и полнодисковом шифровании.

Просмотр статистики шифрования на информационных панелях Kaspersky Security Center

► Чтобы просмотреть статусы шифрования на информационных панелях Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите узел **Сервер администрирования – <Имя компьютера>**.
3. В рабочей области, расположенной справа от дерева Консоли администрирования, выберите закладку **Статистика**.
4. Создайте новую страницу с информационными панелями со статистикой шифрования данных. Для этого выполните следующие действия:
 - a. На закладке **Статистика** нажмите на кнопку **Настроить вид**.
Откроется окно **Свойства: Статистика**.
 - b. В окне **Свойства: Статистика** нажмите на кнопку **Добавить**.
Откроется окно **Свойства: Новая страница**.
 - c. В разделе **Общие** окна **Свойства: Новая страница** введите название страницы.
 - d. В разделе **Информационные панели** нажмите на кнопку **Добавить**.
Откроется окно **Новая информационная панель**.
 - e. В окне **Новая информационная панель** в группе **Состояние защиты** выберите элемент **Шифрование устройств**.
 - f. Нажмите на кнопку **ОК**.
Откроется окно **Свойства: Шифрование устройств**.
 - g. Измените при необходимости параметры информационной панели. Для этого воспользуйтесь разделами **Вид** и **Устройства** окна **Свойства: Шифрование устройств**.
 - h. Нажмите на кнопку **ОК**.
 - i. Повторите пункты d – h инструкции, при этом в окне **Новая информационная панель** в группе **Состояние защиты** выберите элемент **Шифрование съемных дисков**.
Добавленные информационные панели отобразятся в списке **Информационные панели** окна **Свойства: Новая страница**.
 - j. В окне **Свойства: Новая страница** нажмите на кнопку **ОК**.
Название созданной на предыдущих шагах страницы с информационными панелями отобразится в списке **Страницы** окна **Свойства: Статистика**.
 - k. В окне **Свойства: Статистика** нажмите на кнопку **Заккрыть**.
5. На закладке **Статистика** откройте страницу, созданную на предыдущих шагах инструкции.
Отобразятся информационные панели, на которых вы можете просмотреть статусы шифрования компьютеров и съемных дисков.

Просмотр ошибок шифрования файлов на локальных дисках компьютера

► Чтобы просмотреть ошибки шифрования файлов на локальных дисках компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, где находится компьютер пользователя, для которого вы хотите просмотреть список ошибок шифрования файлов.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите в списке компьютер и по правой клавише мыши вызовите контекстное меню.
5. В контекстном меню компьютера выберите пункт **Свойства**. В открывшемся окне **Свойства: <название компьютера>** выберите раздел **Защита**.
6. В разделе **Защита** окна **Свойства: <название компьютера>** по ссылке **Просмотреть ошибки шифрования данных** откройте окно **Ошибки шифрования данных**.

В этом окне отображается информация об ошибках шифрования файлов на локальных дисках компьютера. Если ошибка исправлена, то Kaspersky Security Center удаляет информацию о ней из окна **Ошибки шифрования данных**.

Просмотр отчета о шифровании данных

► Чтобы просмотреть отчет о шифровании данных, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**.
Запустится мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. В окне **Выбор типа шаблона отчета** в разделе **Другое** выберите один из следующих пунктов:
 - **Отчет о статусе шифрования управляемых устройств.**
 - **Отчет о статусе шифрования запоминающих устройств.**
 - **Отчет об ошибках шифрования файлов.**
 - **Отчет о блокировании доступа к зашифрованным файлам.**

После завершения работы мастера создания шаблона отчета в таблице на закладке **Отчеты** появится новый шаблон отчета.

5. Выберите шаблон отчета, созданный на предыдущих шагах инструкции.
6. В контекстном меню шаблона выберите пункт **Показать отчет**.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Работа с зашифрованными устройствами при отсутствии доступа к ним

Получение доступа к зашифрованным устройствам

Пользователю может потребоваться запросить доступ к зашифрованным устройствам в следующих случаях:

- Жесткий диск был зашифрован на другом компьютере.
- На компьютере нет ключа шифрования для устройства (например, в момент первого обращения к зашифрованному съемному диску на этом компьютере), и связь с Kaspersky Security Center отсутствует.

После того как пользователь применил ключ доступа к зашифрованному устройству, Kaspersky Endpoint Security сохраняет ключ шифрования на компьютере пользователя и предоставляет доступ к этому устройству при последующих обращениях, даже если связь с Kaspersky Security Center отсутствует.

Получение доступа к зашифрованным устройствам осуществляется следующим образом:

1. Пользователь создает через интерфейс программы Kaspersky Endpoint Security файл запроса доступа с расширением kesdc и передает его администратору локальной сети организации.
2. Администратор создает в Консоли администрирования Kaspersky Security Center файл ключа доступа с расширением kesdr и передает его пользователю.
3. Пользователь применяет ключ доступа.

Восстановление данных на зашифрованных устройствах

Для работы с зашифрованными устройствами пользователь может использовать утилиту восстановления зашифрованных устройств (далее – "утилита восстановления"). Это может потребоваться в следующих случаях:

- Процедура получения доступа с помощью ключа доступа прошла неуспешно.
- На компьютере с зашифрованным устройством не установлены компоненты шифрования.

Данные, необходимые для восстановления доступа к зашифрованным устройствам с помощью утилиты восстановления, в течение некоторого времени находятся в памяти компьютера пользователя в открытом виде. Чтобы снизить вероятность несанкционированного доступа к этим данным, рекомендуется выполнять восстановление доступа к зашифрованным устройствам на доверенных компьютерах.

Восстановление данных на зашифрованных устройствах осуществляется следующим способом:

1. Пользователь создает с помощью утилиты восстановления файл запроса доступа с расширением fdertc и передает его администратору локальной сети организации.
2. Администратор создает в Консоли администрирования Kaspersky Security Center файл ключа доступа с расширением fdertg и передает его пользователю.
3. Пользователь применяет ключ доступа.

Для восстановления данных на зашифрованных системных жестких дисках пользователь также может указать в утилите восстановления учетные данные Агента аутентификации. Если метаданные учетной записи Агента аутентификации повреждены, то пользователю потребуется пройти процедуру восстановления с помощью файла запроса доступа.

Перед восстановлением данных на зашифрованных устройствах рекомендуется вывести компьютер, на котором будет выполняться процедура, из-под действия политики Kaspersky Security Center или отключить шифрование в параметрах политики Kaspersky Security Center. Это позволяет предотвратить повторное шифрование устройства.

В этом разделе

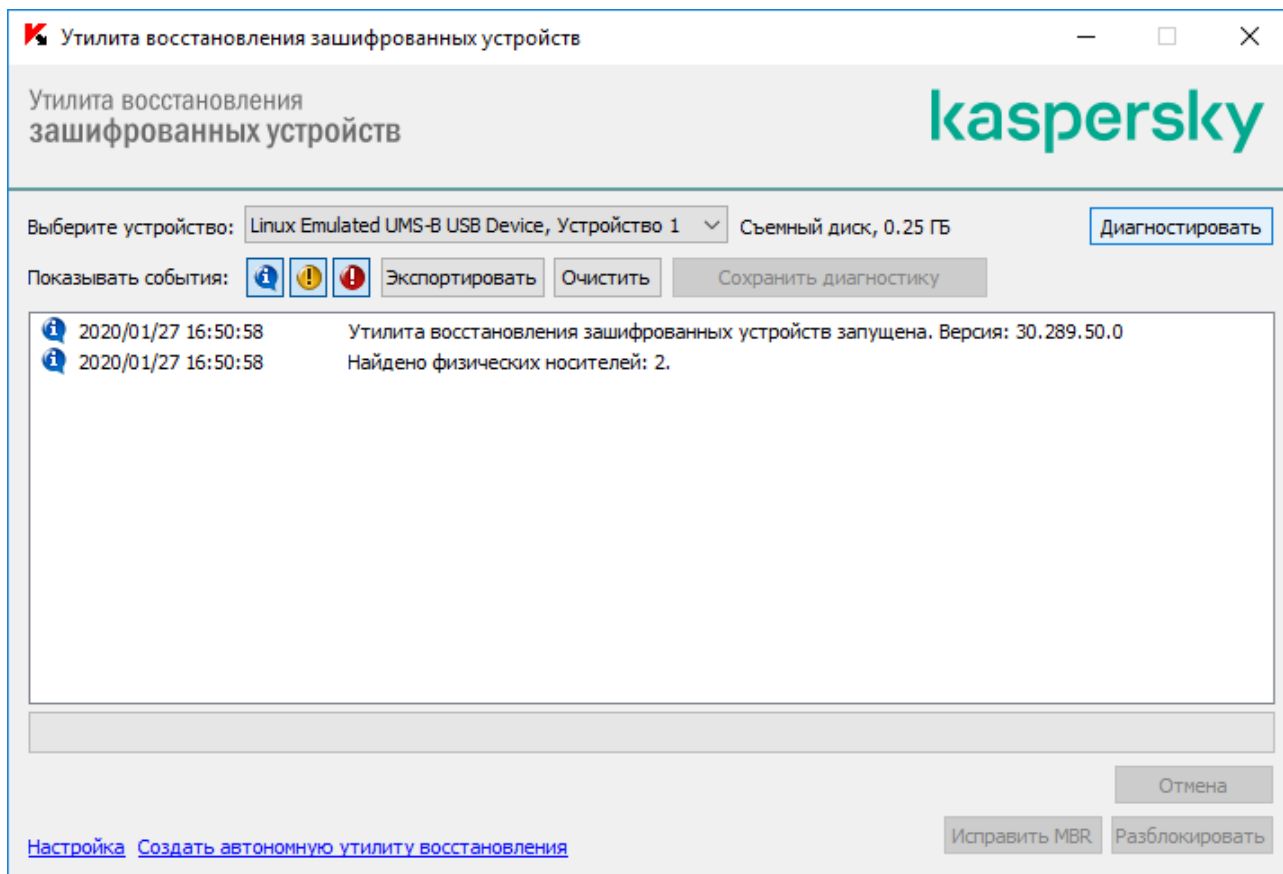
Восстановление данных с помощью утилиты восстановления FDERT	261
Создание диска аварийного восстановления операционной системы	265

Восстановление данных с помощью утилиты восстановления FDERT

При неисправности жесткого диска файловая система может быть повреждена. Таким образом, данные, защищенные технологией Шифрование диска Kaspersky, будут недоступны. Вы можете расшифровать данные и скопировать данные на новый диск.

Восстановление данных на диске, защищенные технологией Шифрование диска Kaspersky, состоит из следующих этапов:

1. Создание автономной утилиты восстановления (см. рис. ниже).
2. Подключение диска к компьютеру, на котором отсутствуют компоненты шифрования Kaspersky Endpoint Security.
3. Запуск утилиты восстановления и диагностика жесткого диска.
4. Доступ к данным на диске. Для этого нужно ввести учетные данные Агента аутентификации или запустить процедуру восстановления ("Запрос - Ответ").



Создание автономной утилиты восстановления

► Чтобы создать исполняемый файл утилиты восстановления, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Поддержка**.
2. В открывшемся окне нажмите на кнопку **Восстановление зашифрованного устройства**.
Запустится утилита восстановления зашифрованных устройств.
3. В окне утилиты восстановления нажмите на кнопку **Создать автономную утилиту восстановления**.
4. Сохраните автономную утилиту восстановления в память компьютера.

В результате исполняемый файл утилиты восстановления `fdert.exe` будет сохранен в указанной папке. Скопируйте утилиту восстановления на компьютер, на котором отсутствуют компоненты шифрования Kaspersky Endpoint Security. Это позволяет предотвратить повторное шифрование диска.

Данные, необходимые для восстановления доступа к зашифрованным устройствам с помощью утилиты восстановления, в течение некоторого времени находятся в памяти компьютера пользователя в открытом виде. Чтобы снизить вероятность несанкционированного доступа к этим данным, рекомендуется выполнять восстановление доступа к зашифрованным устройствам на доверенных компьютерах.

Восстановление данных на жестком диске

- Чтобы восстановить доступ к зашифрованному устройству с помощью утилиты восстановления, выполните следующие действия:

1. Запустите исполняемый файл утилиты восстановления `fdert.exe`, созданный с помощью программы Kaspersky Endpoint Security.
2. В окне утилиты восстановления в раскрывающемся списке **Выберите устройство** выберите зашифрованное устройство, доступ к которому вы хотите восстановить.
3. Нажмите на кнопку **Диагностировать**, чтобы утилита могла определить, какое действие следует выполнить с зашифрованным устройством: разблокировать или расшифровать.

Если на компьютере доступна функциональность шифрования Kaspersky Endpoint Security, то утилита восстановления предлагает разблокировать устройство. При разблокировке устройство не расшифровывается, но к нему в результате предоставляется прямой доступ. Если на компьютере недоступна функциональность шифрования Kaspersky Endpoint Security, то утилита восстановления предлагает расшифровать устройство.

4. Если вы хотите импортировать диагностическую информацию, нажмите на кнопку **Сохранить диагностику**.

Утилита сохранит архив с файлами с диагностической информацией.

5. Нажмите на кнопку **Исправить MBR**, если в результате диагностики зашифрованного системного жесткого диска вы получили сообщение о каких-либо проблемах, связанных с главной загрузочной записью (MBR) устройства.

Исправление главной загрузочной записи устройства может ускорить получение информации, необходимой для разблокировки или расшифровки устройства.

6. Нажмите на кнопку **Разблокировать** или **Расшифровать** в зависимости от результатов диагностики.
7. Если вы хотите восстановить данные с помощью учетной записи Агента аутентификации, выберите вариант **Использовать параметры учетной записи Агента аутентификации** и введите учетные данные Агента аутентификации.

Этот способ возможен только при восстановлении данных на системном жестком диске. Если системный жесткий диск был поврежден и данные об учетной записи Агента аутентификации потеряны, то для восстановления данных на зашифрованном устройстве необходимо получить ключ доступа у администратора локальной сети организации.

8. Если вы хотите запустить процедуру восстановления, выполните следующие действия:
 - a. Выберите вариант **Указать ключ доступа к устройству вручную**.
 - b. Нажмите на кнопку **Получить ключ доступа** и сохраните файл запроса в память компьютера (файл с расширением `fdertc`).
 - c. Передайте файл запроса доступа администратору локальной сети организации.

Не закрывайте окно **Получение ключа доступа к устройству**, пока вы не получите ключ доступа. При повторном открытии этого окна созданный администратором ранее ключ доступа будет невозможно применить.

- d. Получите и сохраните файл доступа (файл с расширением `fdetr`), созданный и переданный вам администратором локальной сети организации (см. инструкцию ниже).
- e. Загрузите файл доступа в окне **Получение ключа доступа к устройству**.

9. Если вы выполняете расшифровку устройства, требуется настроить дополнительные параметры расшифровки:
 - Укажите область для расшифровки:
 - Если вы хотите расшифровать все устройство, выберите вариант **Расшифровать все устройство**.
 - Если вы хотите расшифровать часть данных на устройстве, выберите вариант **Расшифровать отдельные области устройства** и задайте границы области для расшифровки.
 - Выберите место записи расшифрованных данных:
 - Если вы хотите, чтобы данные на исходном устройстве были перезаписаны расшифрованными данными, снимите флажок **Расшифровка в файл образа диска**.
 - Если вы хотите сохранить расшифрованные данные отдельно от исходных зашифрованных данных, установите флажок **Расшифровка в файл образа диска** и с помощью кнопки **Обзор** укажите путь, по которому файл формата VHD должен быть сохранен.

10. Нажмите на кнопку **ОК**.

Запустится процесс разблокировки / расшифровки устройства.

► *Чтобы создать файл доступа к зашифрованным данным, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Дополнительно** → **Шифрование и защита данных** → **Зашифрованные устройства**.
3. В рабочей области выберите зашифрованное устройство, для которого вы хотите создать файл ключа доступа, и в контекстном меню устройства выберите пункт **Получить доступ к устройству в Kaspersky Endpoint Security для Windows (11.3.0)**.

Если вы не уверены, для какого компьютера был сформирован файл запроса доступа, в дереве Консоли администрирования выберите папку **Дополнительно** → **Шифрование и защита данных** и в рабочей области нажмите на ссылку **Получить ключ шифрования устройства в Kaspersky Endpoint Security для Windows (11.3.0)**.

4. В открывшемся окне выберите используемый алгоритм шифрования: **AES256** или **AES56**.

Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: *Strong encryption (AES256)* или *Lite encryption (AES56)*. Библиотека шифрования AES устанавливается вместе с программой.
5. Нажмите на кнопку **Обзор** и в открывшемся окне укажите путь к файлу запроса, полученного от пользователя, с расширением `fdertc`.
6. Нажмите на кнопку **Открыть**.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.

Создание диска аварийного восстановления операционной системы

Диск аварийного восстановления операционной системы может быть полезен в ситуации, когда по каким-либо причинам доступ к зашифрованному системному жесткому диску невозможен и операционная система не может быть загружена.

Вы можете загрузить образ операционной системы Windows с помощью диска аварийного восстановления и восстановить доступ к зашифрованному системному диску с помощью утилиты восстановления, включенной в состав образа операционной системы.

► *Чтобы создать диск аварийного восстановления операционной системы, выполните следующие действия:*

1. Создайте исполняемый файл утилиты восстановления зашифрованных устройств (см. раздел "Восстановление данных с помощью утилиты восстановления FDERT" на стр. [261](#)).
2. Создайте пользовательский образ среды предустановки Windows. В процессе создания пользовательского образа среды предустановки Windows добавьте в образ исполняемый файл утилиты восстановления зашифрованных устройств.
3. Поместите пользовательский образ среды предустановки Windows на загрузочный носитель, например компакт-диск или съемный диск.

Инструкцию о создании пользовательского образа среды предустановки Windows вы можете прочитать в справочной документации Microsoft (например, на ресурсе Microsoft TechNet).

Интеграция с другими решениями "Лаборатории Касперского"

Kaspersky Endpoint Security может взаимодействовать с другими решениями и программами "Лаборатории Касперского":

Kaspersky Anti Targeted Attack Platform (далее также "КАТА") – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. АРТ – Advanced Persistent Threat), атаки "нулевого дня" и другие.

Kaspersky Sandbox – решение для обнаружения и блокировки сложных угроз. На серверах Kaspersky Sandbox развернуты виртуальные образы операционных систем, в которых запускаются проверяемые объекты. Kaspersky Sandbox анализирует поведение этих объектов для выявления вредоносной активности и признаков целевых атак.

В этом разделе

Kaspersky Anti Targeted Attack Platform (КАТА)	266
Kaspersky Sandbox	267

Kaspersky Anti Targeted Attack Platform (КАТА)

Kaspersky Anti Targeted Attack Platform (далее также "КАТА") – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. АРТ – Advanced Persistent Threat), атаки "нулевого дня" и другие. Для обеспечения взаимодействия с КАТА предназначен компонент Endpoint Sensor. Endpoint Sensor входит в состав Endpoint Agent. Для интеграции с КАТА выберите компонент Endpoint Agent при установке программы (например, в инсталляционном пакете). После установки программы в политике будут доступны параметры Endpoint Sensor. Вы можете удалить Endpoint Sensor только вместе с Kaspersky Endpoint Security.

Если на компьютере установлен компонент Endpoint Sensor с помощью инструментов развертывания КАТА, компонент будет переустановлен. Endpoint Sensor будет настроен в соответствии с политикой Kaspersky Endpoint Security для Windows.

Endpoint Sensor устанавливается на клиентских компьютерах. На этих компьютерах компонент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Endpoint Sensor передает информацию на сервер КАТА.

Функциональность компонента доступна для следующих операционных систем:

- Windows 7 Enterprise Service Pack 1;
- Windows 8.1.1 Enterprise;
- Windows 10 RS3 / RS4 / RS5 / 19H1;

- Windows Server 2008 R2 Enterprise (64-разрядная);
- Windows Server 2012 Standard / R2 Standard (64-разрядная);
- Windows Server 2016 Standard (64-разрядная).

Подробную информацию о работе KATA см. в справке *Kaspersky Anti Targeted Attack Platform* <https://help.kaspersky.com/KATA/3.6/ru-RU/>.

На компьютерах с компонентом Endpoint Sensor вам нужно разрешить входящее соединение с сервером KATA напрямую, без использования прокси-сервера.

► Чтобы включить или выключить компонент Endpoint Sensor, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. Выберите раздел **Endpoint Sensor**.
6. Выполните одно из следующих действий:
 - Если вы хотите включить Endpoint Sensor, установите флажок **Endpoint Sensor**.
 - Если вы хотите выключить Endpoint Sensor, снимите флажок **Endpoint Sensor**.
7. Если на предыдущем шаге вы установили флажок, выполните следующие действия:
 - a. В поле **Адрес сервера** укажите адрес сервера Kaspersky Anti Targeted Attack Platform, состоящий из следующих частей:
 - i. название протокола;
 - ii. IP-адрес или полное доменное имя (FQDN) сервера;
 - iii. путь к сборщику событий Windows на сервере.
 - b. В поле **Порт** укажите номер порта, используемого для соединения с сервером Kaspersky Anti Targeted Attack Platform.
8. Нажмите на кнопку **ОК**.

Kaspersky Sandbox

Kaspersky Sandbox – решение для обнаружения и блокировки сложных угроз. На серверах Kaspersky Sandbox развернуты виртуальные образы операционных систем, в которых запускаются проверяемые объекты. Kaspersky Sandbox анализирует поведение этих объектов для выявления вредоносной активности и признаков целевых атак.

Kaspersky Endpoint Security с помощью технологии Kaspersky Sandbox проверяет только исполняемые файлы (например, EXE) и файлы Microsoft Office (DOC, DOCX, XLS, PPT и другие).

Интеграция с Kaspersky Sandbox

Для обеспечения взаимодействия с Kaspersky Sandbox предназначена программа Kaspersky Endpoint Agent. Kaspersky Endpoint Agent входит в комплект поставки Kaspersky Endpoint Security. Вы можете установить Kaspersky Endpoint Agent при установке Kaspersky Endpoint Security. Для этого выберите компонент Endpoint Agent при установке программы (например, в инсталляционном пакете). После установки программы с Endpoint Agent в список установленных программ будут добавлены две программы: Kaspersky Endpoint Security и Kaspersky Endpoint Agent. Подробнее о программных и аппаратных требованиях Kaspersky Endpoint Agent см. в *справке для Kaspersky Sandbox* (<https://help.kaspersky.com/KSB/1.0/ru-RU/187409.htm>).

При обновлении Kaspersky Endpoint Security с установленным компонентом Endpoint Sensor до версии 11.2.0 и выше программа Kaspersky Endpoint Agent будет установлена автоматически. Если вы использовали Kaspersky Endpoint Security без компонента Endpoint Sensor, программа Kaspersky Endpoint Agent не будет установлена.

Программа Kaspersky Endpoint Agent будет автоматически удалена при удалении Kaspersky Endpoint Security, если в параметрах Kaspersky Endpoint Security включен компонент Endpoint Sensor.

Программа Kaspersky Endpoint Agent может быть установлена с помощью других инструментов развертывания. При развертывании программы Kaspersky Endpoint Agent в составе Kaspersky Endpoint Security программа будет переустановлена.

Управление Kaspersky Endpoint Agent

Kaspersky Endpoint Agent не имеет локального интерфейса. Вы можете настроить программу только с помощью Kaspersky Security Center. Для этого установите плагин управления Kaspersky Endpoint Agent. Вы можете установить плагин управления Kaspersky Endpoint Agent вместе с плагином управления Kaspersky Sandbox.

Подробную информацию о работе Kaspersky Endpoint Agent вы можете прочитать в *справке для Kaspersky Sandbox* (<https://help.kaspersky.com/KSB/1.0/ru-RU/187409.htm>).

Служба уведомлений

В процессе работы Kaspersky Endpoint Security возникают различного рода события. Уведомления об этих событиях могут иметь информационный характер или нести важную информацию. Например, уведомление может информировать об успешно выполненном обновлении баз и модулей программы, а может фиксировать ошибку в работе некоторого компонента, которую вам требуется устранить.

Kaspersky Endpoint Security позволяет вносить информацию о событиях, возникающих в работе программы, в журнал событий Microsoft Windows и / или в журнал Kaspersky Endpoint Security.

Kaspersky Endpoint Security может доставлять уведомления следующими способами:

- с помощью всплывающих уведомлений в области уведомлений панели задач Microsoft Windows;
- по электронной почте.

Вы можете настроить способы доставки уведомлений. Способ доставки уведомлений устанавливается для каждого типа событий.

Вы можете выполнить следующие действия для настройки службы уведомлений:

- настроить параметры журналов событий, где Kaspersky Endpoint Security сохраняет события;
- настроить отображение уведомлений на экране;
- настроить доставку уведомлений по электронной почте.

Работая с таблицей событий для настройки службы уведомлений, вы можете выполнять следующие действия:

- фильтровать события службы уведомлений по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска событий службы уведомлений;
- сортировать события службы уведомлений;
- изменять порядок и набор граф, отображаемых в списке событий службы уведомлений.

В этом разделе

Настройка параметров журналов событий.....	269
Настройка отображения и доставки уведомлений	270
Настройка отображения предупреждений о состоянии программы в области уведомлений	271

Настройка параметров журналов событий

► Чтобы настроить параметры журналов событий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Интерфейс**.

3. В блоке **Уведомления** нажмите на кнопку **Настройка**.

Откроется окно **Уведомления**.

В левой части окна представлены компоненты и задачи Kaspersky Endpoint Security. В правой части окна отображается список событий, сформированный для выбранного компонента или выбранной задачи.

События могут содержать следующие данные пользователя:

- пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
 - пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
 - имя пользователя Microsoft Windows;
 - адреса веб-страниц, открываемых пользователем.
4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить параметры журналов событий.
 5. В графах **Сохранять в локальном отчете** и **Сохранять в журнале событий Windows** установите флажки напротив нужных событий.

События, напротив которых установлен флажок в графе **Сохранять в локальном отчете**, отображаются в **Журналах приложений и служб** в разделе **Журнал событий Kaspersky**.

События, напротив которых установлен флажок в графе **Сохранять в журнале событий Windows**, отображаются в **Журналах Windows** в разделе **Приложение**. Чтобы открыть журналы событий, выберите **Пуск** → **Панель управления** → **Администрирование** → **Просмотр событий**.

6. Сохраните внесенные изменения.

Настройка отображения и доставки уведомлений

► *Чтобы настроить отображение и доставку уведомлений, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Настройка**.

Откроется окно **Уведомления**.

В левой части окна представлены компоненты и задачи Kaspersky Endpoint Security. В правой части окна отображается список событий, сформированный для выбранного компонента или выбранной задачи.

События могут содержать следующие данные пользователя:



- пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
 - пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
 - имя пользователя Microsoft Windows;
 - адреса веб-страниц, открываемых пользователем.
4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить доставку уведомлений.

5. В графе **Уведомлять на экране** установите флажки напротив нужных событий.
Информация о выбранных событиях отображается на экране в виде всплывающих уведомлений в области уведомлений панели задач Microsoft Windows.
6. В графе **Уведомлять по почте** установите флажки напротив нужных событий.
Информация о выбранных событиях доставляется по электронной почте, если заданы параметры доставки почтовых уведомлений.
7. Нажмите на кнопку **Настройка почтовых уведомлений**.
Откроется окно **Настройка почтовых уведомлений**.
8. Установите флажок **Отправлять сообщения о событиях**, чтобы включить доставку информации о событиях в работе Kaspersky Endpoint Security, отмеченных в графе **Уведомлять по почте**.
9. Укажите параметры доставки почтовых уведомлений.
10. Сохраните внесенные изменения.

Настройка отображения предупреждений о состоянии программы в области уведомлений

► *Чтобы настроить отображение предупреждений о состоянии программы в области уведомлений, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Интерфейс**.
3. В блоке **Предупреждения** установите флажки напротив тех категорий событий, уведомления о которых вы хотите видеть в области уведомлений Microsoft Windows.
4. Сохраните внесенные изменения.

При возникновении событий, относящихся к выбранным категориям, значок программы (см. раздел "Значок программы в области уведомлений" на стр. [44](#)) в области уведомлений будет меняться на  или  в зависимости от важности предупреждения.


Работа с отчетами

Информация о работе каждого компонента Kaspersky Endpoint Security, о событиях шифрования данных, о выполнении каждой задачи проверки, задачи обновления и задачи проверки целостности, а также о работе программы в целом сохраняется в отчетах.

Отчеты хранятся в папке C:\ProgramData\Kaspersky Lab\KES\Report.

Отчеты могут содержать следующие данные пользователя:




- пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
- пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
- имя пользователя Microsoft Windows;
- адреса веб-страниц, открываемых пользователем.

Данные в отчете представлены в виде таблицы. Каждая строка таблицы содержит информацию об отдельном событии, атрибуты события находятся в графах таблицы. Некоторые графы являются составными и содержат вложенные графы с дополнительными атрибутами. Чтобы просмотреть дополнительные атрибуты, нажмите на кнопку  рядом с названием графы. События, зарегистрированные в работе разных компонентов или при выполнении разных задач, имеют разный набор атрибутов.

Доступны следующие отчеты:


- Отчет **Системный аудит**. Содержит информацию о событиях, возникающих в процессе взаимодействия пользователя с программой, а также в ходе работы программы в целом и не относящихся к каким-либо отдельным компонентам или задачам Kaspersky Endpoint Security.
- Отчеты о работе компонентов Kaspersky Endpoint Security.
- Отчеты о выполнении задач Kaspersky Endpoint Security.
- Отчет **Шифрование данных**. Содержит информацию о событиях, возникающих при шифровании и расшифровке данных.

В отчетах применяются следующие уровни важности событий:

- **Информационные сообщения**. Значок . События справочного характера, как правило, не несущие важной информации.
- **Предупреждения**. Значок . События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе Kaspersky Endpoint Security.
- **Критические события**. Значок . События критической важности, указывающие на проблемы в работе Kaspersky Endpoint Security или на уязвимости в защите компьютера пользователя.

Для удобства работы с отчетами вы можете изменять представление данных на экране следующими способами:

- фильтровать список событий по различным критериям;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке;
- сортировать список событий по каждой графе отчета;

- отображать и скрывать сгруппированные с помощью фильтра события по кнопке ;
- изменять порядок и набор граф, отображаемых в отчете.

При необходимости вы можете сохранить сформированный отчет в текстовый файл. Также вы можете удалять информацию из отчетов (см. раздел "Удаление информации из отчетов" на стр. [276](#)) по компонентам и задачам Kaspersky Endpoint Security, объединенным в группы.

Если Kaspersky Endpoint Security работает под управлением Kaspersky Security Center, то информация о событиях может быть передана на Сервер администрирования Kaspersky Security Center (подробнее см. в справке Kaspersky Security Center <https://help.kaspersky.com/KSC/11/ru-RU/>).

В этом разделе

Просмотр отчетов	273
Просмотр информации о событии в отчете	273
Настройка максимального срока хранения отчетов	274
Настройка максимального размера файла отчета	274
Сохранение отчета в файл	275
Удаление информации из отчетов	276

Просмотр отчетов

Если для пользователя доступен просмотр отчетов, то для этого пользователя доступен просмотр всех событий, отраженных в отчетах.

► *Чтобы просмотреть отчеты, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Отчеты**.
Откроется окно **Отчеты**.
2. В левой части окна **Отчеты** в списке компонентов и задач выберите компонент или задачу.
В правой части окна отобразится отчет, содержащий список событий по результатам работы выбранного компонента или выбранной задачи Kaspersky Endpoint Security.

Вы можете отсортировать события в отчете по значениям в ячейках одной из граф. По умолчанию события в отчете отсортированы по возрастанию значений в ячейках графы **Дата события**.

Просмотр информации о событии в отчете

Вы можете просматривать подробную сводную информацию о каждом событии в отчете.

► *Чтобы просмотреть подробную сводную информацию о событии в отчете, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Отчеты**.

Откроется окно **Отчеты**.

2. В левой части окна выберите нужный вам отчет о работе компонента или задачи.

В правой части окна в таблице отобразятся события, входящие в состав отчета. Для поиска отдельных событий в отчете можно использовать функции фильтрации, поиска и сортировки.

3. Выберите в отчете нужное вам событие.

В нижней части окна отобразится блок со сводной информацией о событии.

Настройка максимального срока хранения отчетов

По умолчанию максимальный срок хранения отчетов о событиях, фиксируемых Kaspersky Endpoint Security, составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчета. Вы можете отменить ограничение по времени или изменить максимальный срок хранения отчетов.

► *Чтобы настроить максимальный срок хранения отчетов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.

2. В окне параметров программы выберите раздел **Общие параметры** → **Отчеты и хранение**.

3. В правой части окна в блоке **Отчеты** выполните одно из следующих действий:

- Установите флажок **Хранить отчеты не более**, если хотите ограничить срок хранения отчетов. В поле справа от флажка **Хранить отчеты не более** укажите максимальный срок хранения отчетов.

По умолчанию максимальный срок хранения отчетов составляет 30 дней.

- Снимите флажок **Хранить отчеты не более**, если хотите отменить ограничение срока хранения отчетов.

По умолчанию ограничение срока хранения отчетов включено.

4. Сохраните внесенные изменения.

Настройка максимального размера файла отчета

Вы можете указать максимальный размер файла, содержащего отчет. По умолчанию максимальный размер файла отчета составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчета таким образом, чтобы не превышался максимальный размер файла отчета. Вы можете отменить ограничение на размер файла отчета или установить другое значение.

► *Чтобы настроить максимальный размер файла отчета, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Отчеты и хранение**.
3. В правой части окна в блоке **Отчеты** выполните одно из следующих действий:
 - Установите флажок **Максимальный размер файла**, если хотите ограничить размер файла отчета. В поле справа от флажка **Максимальный размер файла** укажите максимальный размер файла отчета.
По умолчанию ограничение размера файла отчета составляет 1024 МБ.
 - Снимите флажок **Максимальный размера файла**, если хотите отменить ограничение на размер файла отчета.
По умолчанию ограничение размера файла отчета включено.
4. Сохраните внесенные изменения.

Сохранение отчета в файл

Пользователь сам несет ответственность за обеспечение безопасности информации из сохраненного в файл отчета и, в частности, за контроль и ограничение доступа к этой информации.

Сформированный отчет вы можете сохранить в файл текстового формата TXT или CSV.

Kaspersky Endpoint Security сохраняет событие в отчет в том виде, в каком событие отображается на экране, то есть с тем же составом и с той же последовательностью атрибутов события.

► *Чтобы сохранить отчет в файл, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Отчеты**.
Откроется окно **Отчеты**.
2. В левой части окна **Отчеты** в списке компонентов и задач выберите компонент или задачу.
В правой части окна отобразится отчет, содержащий список событий о работе выбранного компонента или задачи Kaspersky Endpoint Security.

3. Если требуется, измените представление данных в отчете с помощью следующих способов:
 - фильтрация событий;
 - поиск событий;
 - изменение расположения граф;
 - сортировка событий.
4. Нажмите на кнопку **Сохранить отчет**, расположенную в верхней правой части окна.
Откроется контекстное меню.
5. В контекстном меню выберите нужную кодировку для сохранения файла отчета: **Сохранить в ANSI** или **Сохранить в Unicode**.
Откроется стандартное окно Microsoft Windows **Сохранить как**.
6. В открывшемся окне **Сохранить как** укажите папку, в которую вы хотите сохранить файл отчета.
7. В поле **Имя файла** введите название файла отчета.
8. В поле **Тип файла** выберите нужный формат файла отчета: TXT или CSV.
9. Сохраните внесенные изменения.

Удаление информации из отчетов

► *Чтобы удалить информацию из отчетов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Отчеты и хранение**.
3. В правой части окна в блоке **Отчеты** нажмите на кнопку **Удалить отчеты**.
Откроется окно **Удаление отчетов**.
4. Установите флажки для тех отчетов, из которых вы хотите удалить информацию:
 - **Все отчеты**.
 - **Отчет компонентов защиты**. Содержит информацию о работе следующих компонентов Kaspersky Endpoint Security:
 - Анализ поведения.
 - Защита от эксплойтов.
 - Предотвращение вторжений.
 - Защита от файловых угроз.
 - Защита от веб-угроз.
 - Защита от почтовых угроз.
 - Защита от сетевых угроз.
 - Защита от атак BadUSB.
 - Поставщик AMSI-защиты.

- **Отчет компонентов контроля.** Содержит информацию о работе следующих компонентов Kaspersky Endpoint Security:
 - Контроль программ.
 - Контроль устройств.
 - Веб-Контроль.
 - Адаптивный контроль аномалий.
- **Отчет о шифровании данных.** Содержит информации о выполненных задачах шифрования данных.
- **Отчет задач проверки.** Содержит информацию о следующих выполненных задачах проверки:
 - Полная проверка.
 - Проверка важных областей.
 - Выборочная проверка.

Информация о выполнении задачи Проверка целостности удаляется, только если установлен флажок **Все отчеты**.

- **Отчет задач обновления.** Содержит информацию о выполненных задачах обновления.
 - **Отчет компонента Сетевой экран.** Содержит информацию о работе Сетевого экрана.
 - **Отчет компонента Endpoint Sensor.** Содержит информацию о работе компонента Endpoint Sensor.
5. Нажмите на кнопку **ОК**.

Работа с резервным хранилищем

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке C:\ProgramData\Kaspersky Lab\KES\QB.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security.

В Kaspersky Endpoint Security отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете попытаться восстановить файл из его резервной копии в папку исходного размещения файла.

Если Kaspersky Endpoint Security работает под управлением Kaspersky Security Center, то резервные копии файлов могут быть переданы на Сервер администрирования Kaspersky Security Center. Подробнее о работе резервными копиями файлов в Kaspersky Security Center можно прочитать в Справочной системе Kaspersky Security Center.

В этом разделе

Настройка максимального срока хранения файлов в резервном хранилище	278
Настройка максимального размера резервного хранилища	279
Восстановление и удаление файлов из резервного хранилища	279

Настройка максимального срока хранения файлов в резервном хранилище

По умолчанию максимальный срок хранения копий файлов в резервном хранилище составляет 30 дней. По истечении максимального срока хранения Kaspersky Endpoint Security удаляет наиболее старые файлы из резервного хранилища. Вы можете отменить ограничение по времени или изменить максимальный срок хранения файлов.

► *Чтобы настроить максимальный срок хранения файлов в резервном хранилище, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Отчеты и хранение**.

3. Выполните одно из следующих действий:

- В правой части окна в блоке **Резервное хранилище** установите флажок **Хранить объекты не более**, если хотите ограничить срок хранения копий файлов в резервном хранилище. В поле справа от флажка **Хранить объекты не более** укажите максимальный срок хранения копий файлов в резервном хранилище. По умолчанию максимальный срок хранения копий файлов в резервном хранилище составляет 30 дней.
- В правой части окна в блоке **Резервное хранилище** снимите флажок **Хранить объекты не более**, если хотите отменить ограничение срока хранения копий файлов в резервном хранилище.

4. Сохраните внесенные изменения.

Настройка максимального размера резервного хранилища

По умолчанию максимальный размер резервного хранилища составляет 100 МБ. После достижения максимального размера Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы из резервного хранилища таким образом, чтобы не превышался его максимальный размер. Вы можете отменить ограничение на максимальный размер резервного хранилища или изменить максимальный размер.

► *Чтобы настроить максимальный размер резервного хранилища, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.

2. В окне параметров программы выберите раздел **Общие параметры** → **Отчеты и хранение**.

3. Выполните одно из следующих действий:

- Если вы хотите ограничить суммарный размер резервного хранилища, установите флажок **Максимальный размер хранилища** в правой части окна в блоке **Резервное хранилище** и укажите максимальный размер резервного хранилища в поле справа от флажка **Максимальный размер хранилища**.

По умолчанию максимальный размер хранилища данных, включающего в себя резервные копии файлов, составляет 100 МБ.

- Если вы хотите отменить ограничение на размер резервного хранилища, снимите флажок **Максимальный размер хранилища** в правой части окна в блоке **Резервное хранилище**.

По умолчанию размер резервного хранилища не ограничен.

4. Сохраните внесенные изменения.

Восстановление и удаление файлов из резервного хранилища

Если в файле обнаружен вредоносный код, Kaspersky Endpoint Security блокирует файл, присваивает ему статус **Заражен**, помещает его копию в резервное хранилище и пытается провести лечение. Если файл удастся вылечить, то статус резервной копии файла изменяется на **Вылечен**. Файл становится доступен в папке исходного размещения. Если файл не удастся вылечить, то Kaspersky Endpoint Security удаляет его из папки исходного размещения. Вы можете восстановить файл из его резервной копии в папку исходного размещения.

Файлы со статусом *Будет вылечен при перезагрузке компьютера* восстановить невозможно. Перезагрузите компьютер и статус файла изменится на *Вылечен* или *Удален*. При этом вы можете восстановить файл из его резервной копии в папку исходного размещения.

Kaspersky Endpoint Security удаляет резервные копии файлов с любым статусом из резервного хранилища автоматически по истечении времени, заданного в параметрах программы. Также вы можете самостоятельно удалить любую копию файла из резервного хранилища.

В случае обнаружения вредоносного кода в файле, который является частью приложения Windows Store, Kaspersky Endpoint Security не помещает копию файла в резервное хранилище, а сразу удаляет его. При этом восстановить целостность приложения Windows Store вы можете средствами операционной системы Microsoft Windows 8 (подробную информацию о восстановлении приложения Windows Store читайте в *Справочной системе к Microsoft Windows 8*).

Набор резервных копий файлов представлен в виде таблицы. Работая с резервным хранилищем, вы можете выполнять следующие действия с резервными копиями файлов:

- Просматривать набор резервных копий файлов.

Для резервной копии файла отображается путь к папке исходного размещения этого файла. Путь к папке исходного размещения файла может содержать персональные данные.

- Восстанавливать файлы из резервных копий в папки их исходного размещения.
- Удалять резервные копии файлов из резервного хранилища.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать резервные копии по графам, в том числе по условиям сложного фильтра;
- использовать функцию поиска резервных копий;
- сортировать резервные копии;
- изменять порядок и набор граф, отображаемых в таблице резервных копий.

Вы можете скопировать информацию о выбранных файлах резервного хранилища в буфер обмена. Чтобы выбрать несколько файлов резервного хранилища, откройте по правой клавише мыши контекстное меню любого файла и выберите пункт **Выделить все**. Далее отметьте те файлы, с которых вы хотите снять выделение, удерживая клавишу **CTRL**.

В этом разделе

Восстановление файлов из резервного хранилища	281
Удаление резервных копий файлов из резервного хранилища	281

Восстановление файлов из резервного хранилища

Если в резервное хранилище помещено несколько расположенных в одной и той же папке файлов с одинаковыми именами и различным содержимым, то для восстановления доступен только тот файл, который был помещен в резервное хранилище последним.

► Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:

1. В главном окне программ нажмите на кнопку **Хранилища**.

Откроется окно **Резервное хранилище**.

2. Если вы хотите восстановить все файлы из резервного хранилища, то в окне **Резервное хранилище** в контекстном меню любого файла выберите пункт **Восстановить все**.

Kaspersky Endpoint Security восстановит все файлы из их резервных копий в папки их исходного размещения.

3. Если вы хотите восстановить один или несколько файлов из резервного хранилища, то выполните следующие действия:

- a. В таблице в окне **Резервное хранилище** выберите один или несколько файлов резервного хранилища.

Чтобы выбрать несколько файлов резервного хранилища, откройте по правой клавише мыши контекстное меню любого файла и выберите пункт **Выделить все**. Далее отметьте те файлы, с которых вы хотите снять выделение, удерживая клавишу **CTRL**.

- b. Восстановите файлы одним из следующих способов:

- Нажмите на кнопку **Восстановить**.
- По правой клавише мыши откройте контекстное меню и выберите пункт **Восстановить**.

Kaspersky Endpoint Security восстановит файлы из выбранных резервных копий в папки их исходного размещения.

Удаление резервных копий файлов из резервного хранилища

► Чтобы удалить резервные копии файлов из резервного хранилища, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Хранилища**.

2. Откроется окно **Резервное хранилище**.

3. Если вы хотите удалить все файлы из резервного хранилища, то выполните одно из следующих действий:

- В контекстном меню любого файла выберите пункт **Удалить все**.
- Нажмите на кнопку **Очистить хранилище**.

Kaspersky Endpoint Security удалит все резервные копии файлов из резервного хранилища.

4. Если вы хотите удалить один или несколько файлов из резервного хранилища, то выполните следующие действия:
 - a. В таблице в окне **Резервное хранилище** выберите один или несколько файлов резервного хранилища.

Чтобы выбрать несколько файлов резервного хранилища, откройте по правой клавише мыши контекстное меню любого файла и выберите пункт **Выделить все**. Далее отметьте те файлы, с которых вы хотите снять выделение, удерживая клавишу **CTRL**.
 - b. Нажмите на кнопку **Удалить**.
- Kaspersky Endpoint Security удалит выбранные резервные копии файлов из резервного хранилища.

Самозащита Kaspersky Endpoint Security

Kaspersky Endpoint Security обеспечивает безопасность компьютера от вредоносных программ, включая и вредоносные программы, которые пытаются заблокировать работу Kaspersky Endpoint Security или удалить программу с компьютера.

Kaspersky Endpoint Security обеспечивает стабильность системы безопасности компьютера за счет следующих технологий:

- Механизм самозащита. Предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.
- AM-PPL (Antimalware Protected Process Light). Защищает процессы Kaspersky Endpoint Security от вредоносных действий. Подробнее о технологии AM-PPL см. на сайте Microsoft (<https://docs.microsoft.com/ru-ru/windows/win32/services/protecting-anti-malware-services-/>).

Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.

- Механизм защиты от внешнего управления. Позволяет блокировать все попытки управления службами программы с удаленного компьютера.

Под управлением 64-разрядных операционных систем доступно только управление механизмом самозащиты Kaspersky Endpoint Security от изменения или удаления файлов программы на жестком диске, а также от изменения или удаления записей в системном реестре.

В этом разделе

Включение и выключение механизма самозащиты.....	283
Включение и выключение поддержки AM-PPL.....	284
Включение и выключение механизма защиты от внешнего управления	285
Обеспечение работы программ удаленного администрирования	285

Включение и выключение механизма самозащиты

По умолчанию механизм самозащиты Kaspersky Endpoint Security включен.

► *Чтобы включить или выключить механизм самозащиты, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры программы**.
3. Выполните одно из следующих действий:
 - Установите флажок **Включить самозащиту**, если вы хотите включить механизм самозащиты.
 - Снимите флажок **Включить самозащиту**, если вы хотите выключить механизм самозащиты.
4. Сохраните внесенные изменения.

Включение и выключение поддержки AM-PPL

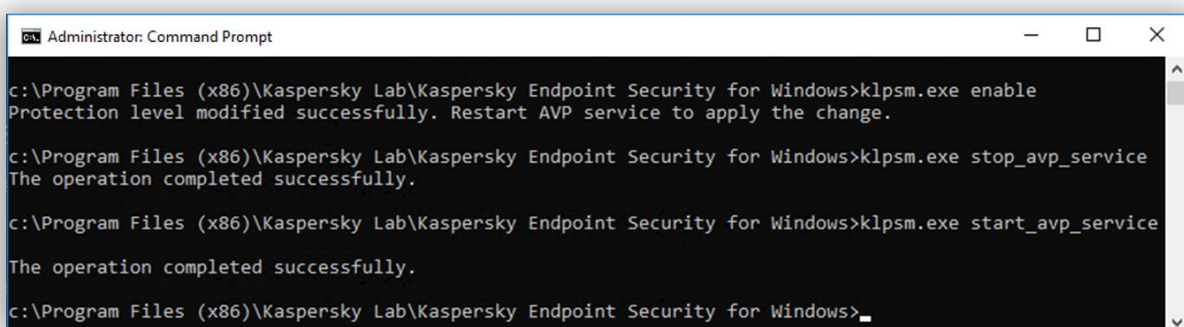
Kaspersky Endpoint Security поддерживает технологию Antimalware Protected Process Light (далее "AM-PPL") от Microsoft. AM-PPL защищает процессы Kaspersky Endpoint Security от вредоносных действий (например, завершение работы программы). AM-PPL разрешает запуск только доверенных процессов. Процессы Kaspersky Endpoint Security подписаны в соответствии с требованиями безопасности Windows, поэтому являются доверенными. Подробнее о технологии AM-PPL см. на сайте Microsoft (<https://docs.microsoft.com/ru-ru/windows/win32/services/protecting-anti-malware-services/>). По умолчанию технология AM-PPL включена.

Kaspersky Endpoint Security также имеет встроенные механизмы защиты процессов программы. Поддержка AM-PPL позволяет делегировать функции защиты процессов операционной системе. Таким образом, вы увеличиваете быстродействие программы и уменьшаете потребление ресурсов компьютера.

Сервис AM-PPL доступен для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.

► Чтобы включить или выключить поддержку технологии AM-PPL, выполните следующие действия:

1. Выключите механизм самозащиты программы (см. раздел "Включение и выключение механизма самозащиты" на стр. [283](#)).
Механизм самозащиты предотвращает изменение и удаление процессов программы в памяти компьютера, в том числе изменение статуса AM-PPL.
2. Запустите интерпретатор командной строки cmd от имени администратора.
3. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
4. В командной строке введите:
 - `klpsm.exe enable` – включение поддержки технологии AM-PPL (см. рис. ниже).
 - `klpsm.exe disable` – выключение поддержки технологии AM-PPL.
5. Перезапустите Kaspersky Endpoint Security (см. раздел "Запуск и остановка программы" на стр. [48](#)).
6. Возобновите работу механизма самозащиты программы (см. раздел "Включение и выключение механизма самозащиты" на стр. [283](#)).



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.

c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.

c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.

c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>
```

Включение и выключение механизма защиты от внешнего управления

По умолчанию механизм защиты от внешнего управления включен.

► *Чтобы включить или выключить механизм защиты от внешнего управления, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры программы**.
3. Выполните одно из следующих действий:
 - Установите флажок **Выключить внешнее управление системными службами**, если вы хотите включить механизм защиты от внешнего управления.
 - Снимите флажок **Выключить внешнее управление системными службами**, если вы хотите выключить механизм защиты от внешнего управления.

Для завершения работы программы из командной строки необходимо, чтобы флажок **Выключить внешнее управление системными службами** был снят.

4. Сохраните внесенные изменения.

Обеспечение работы программ удаленного администрирования

Нередко возникают ситуации, когда при использовании механизма защиты от внешнего управления возникает необходимость применить программы удаленного администрирования.

► *Чтобы обеспечить работу программ удаленного администрирования, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Исключения**.
3. В блоке **Исключения из проверки и доверенные программы** нажмите на кнопку **Настройка**.
Откроется окно **Доверенная зона**.
4. В окне **Доверенная зона** выберите закладку **Доверенные программы**.
5. Нажмите на кнопку **Добавить**.
6. В раскрывшемся контекстном меню выполните одно из следующих действий:
 - Выберите пункт **Программы**, если вы хотите найти программу удаленного администрирования в списке установленных на компьютере программ.
Откроется окно **Выбор программы**.
 - Выберите пункт **Обзор**, если вы хотите указать путь к исполняемому файлу программы удаленного администрирования.
Откроется стандартное окно Microsoft Windows **Открыть**.

7. Выберите программу одним из следующих способов:

- Если на предыдущем шаге вы выбрали пункт **Программы**, выберите программу в списке установленных на компьютере программ и нажмите на кнопку **ОК** в окне **Выбор программы**.
- Если на предыдущем шаге вы выбрали пункт **Обзор**, укажите путь к исполняемому файлу нужной программы и нажмите на кнопку **Открыть** в стандартном окне Microsoft Windows **Открыть**.

В результате выполненных действий откроется окно **Исключения из проверки для программы**.

8. Установите флажок **Не контролировать активность программы**.

9. Сохраните внесенные изменения.

Производительность Kaspersky Endpoint Security и совместимость с другими программами

Производительность Kaspersky Endpoint Security

Под производительностью Kaspersky Endpoint Security подразумевается количество обнаруживаемых типов объектов, которые могут нанести вред компьютеру, а также потребление энергии и ресурсов компьютера.

Выбор типов обнаруживаемых объектов

Kaspersky Endpoint Security позволяет гибко настраивать защиту компьютера и выбирать типы объектов (см. раздел "Выбор типов обнаруживаемых объектов" на стр. [288](#)), которые программа обнаруживает в ходе работы. Kaspersky Endpoint Security всегда проверяет операционную систему на наличие вирусов, червей и троянских программ. Вы не можете выключить проверку этих типов объектов. Такие программы могут нанести значительный вред компьютеру пользователя. Чтобы обеспечить большую безопасность компьютера, вы можете расширить список обнаруживаемых типов объектов, включив контроль действий легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Использование режима энергосбережения

Во время работы на портативных компьютерах потребление программами энергоресурсов имеет особое значение. Зачастую задачи, которые Kaspersky Endpoint Security выполняет по расписанию, требуют значительного количества ресурсов. При питании компьютера от аккумулятора для экономии его заряда вы можете использовать режим энергосбережения.

Режим энергосбережения позволяет автоматически откладывать выполнение задач, для которых установлен запуск по расписанию:

- задача обновления;
- задача полной проверки;
- задача проверки важных областей;
- задача выборочной проверки;
- задача проверки целостности.

Независимо от того, включен режим энергосбережения или нет, Kaspersky Endpoint Security приостанавливает выполнение задач шифрования при переходе портативного компьютера в режим работы от аккумулятора. При выходе портативного компьютера из режима работы от аккумулятора в режим работы от сети программа возобновляет выполнение задач шифрования.

Передача ресурсов компьютера другим программам

Потребление ресурсов компьютера Kaspersky Endpoint Security может сказываться на производительности других программ. Чтобы решить проблему совместной работы при увеличении нагрузки на процессор и дисковые подсистемы, Kaspersky Endpoint Security может приостанавливать выполнение задач по расписанию и уступать ресурсы другим программам.

Однако существует ряд программ, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Чтобы проверка не зависела от работы таких программ, не следует уступать им ресурсы операционной системы.

По мере необходимости вы можете запускать эти задачи вручную.

Применение технологии лечения активного заражения

Современные вредоносные программы могут внедряться на самые нижние уровни операционной системы, что делает их удаление практически невозможным. Обнаружив вредоносную активность в операционной системе, Kaspersky Endpoint Security выполняет расширенную процедуру лечения, применяя специальную технологию лечения активного заражения. *Технология лечения активного заражения* направлена на лечение операционной системы от вредоносных программ, которые уже запустили свои процессы в оперативной памяти и мешают Kaspersky Endpoint Security удалить их с помощью других методов. В результате угроза нейтрализуется. В процессе процедуры лечения активного заражения не рекомендуется запускать новые процессы или редактировать реестр операционной системы. Технология лечения активного заражения требует значительных ресурсов операционной системы, что может замедлить работу других программ.

После окончания процедуры лечения активного заражения на компьютере под управлением операционной системы Microsoft Windows для рабочих станций Kaspersky Endpoint Security запрашивает у пользователя разрешение на перезагрузку компьютера. После перезагрузки компьютера Kaspersky Endpoint Security удаляет файлы вредоносного программного обеспечения и запускает облегченную полную проверку компьютера.

Запрос перезагрузки на компьютере под управлением операционной системы Microsoft Windows для серверов невозможен из-за особенностей программы Kaspersky Endpoint Security. Незапланированная перезагрузка файлового сервера может повлечь за собой проблемы, связанные с временным отказом доступа к данным файлового сервера или потерей несохраненных данных. Перезагрузку файлового сервера рекомендуется выполнять строго по расписанию. Поэтому по умолчанию технология лечения активного заражения для файловых серверов выключена (см. раздел "Включение и выключение технологии лечения активного заражения" на стр. [289](#)).

В случае обнаружения активного заражения на файловом сервере, на Kaspersky Security Center передается событие о необходимости лечения активного заражения. Для лечения активного заражения на сервере требуется включить технологию лечения активного заражения для серверов и запустить групповую задачу *Поиск вирусов* в удобное для пользователей сервера время.

В этом разделе

Выбор типов обнаруживаемых объектов.....	288
Включение и выключение технологии лечения активного заражения.....	289
Включение и выключение режима энергосбережения.....	290
Включение и выключение режима передачи ресурсов другим программам	290

Выбор типов обнаруживаемых объектов

► *Чтобы выбрать типы обнаруживаемых объектов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Исключения**.
3. В блоке **Объекты для обнаружения** нажмите на кнопку **Настройка**.

Откроется окно **Объекты для обнаружения**.

4. Установите флажки для типов объектов, которые должен обнаруживать Kaspersky Endpoint Security:
 - **Вредоносные утилиты.**
 - **Рекламные программы.**
 - **Программы автодозвона.**
 - **Другие.**
 - **Упакованные файлы, которые могут нанести вред.**
 - **Многократно упакованные файлы.**
5. Нажмите на кнопку **ОК**.

Окно **Объекты для обнаружения** закроется. В блоке **Объекты для обнаружения** под надписью **Включено обнаружение объектов следующих типов** отобразятся выбранные вами типы объектов.
6. Сохраните внесенные изменения.

Включение и выключение технологии лечения активного заражения

► *Чтобы включить или выключить технологию лечения активного заражения для рабочих станций, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры программы**.
3. В правой части окна выполните одно из следующих действий:
 - Установите флажок **Применять технологию лечения активного заражения**, если хотите включить технологию лечения активного заражения.
 - Снимите флажок **Применять технологию лечения активного заражения**, если хотите выключить технологию лечения активного заражения.
4. Сохраните внесенные изменения.

При запуске задачи лечения активного заражения через Kaspersky Security Center пользователю не будут доступны большинство функций операционной системы. После завершения задачи рабочая станция будет перезагружена.

► *Чтобы включить технологию лечения активного заражения для серверов, выполните одно из следующих действий:*

- Включите технологию лечения активного заражения в свойствах активной политики Kaspersky Security Center. Для этого выполните следующие действия:
 - a. Откройте раздел **Параметры программы** окна свойств политики.
 - b. Установите флажок **Применять технологию лечения активного заражения**.
 - c. Нажмите на кнопку **ОК** в окне свойств политики, чтобы сохранить внесенные изменения.
- В свойствах групповой задачи Kaspersky Security Center "Поиск вирусов" установите флажок **Выполнять лечение активного заражения немедленно**.

► Чтобы выключить технологию лечения активного заражения для серверов, выполните одно из следующих действий:

- Выключите технологию лечения активного заражения в свойствах политики Kaspersky Security Center. Для этого выполните следующие действия:
 - a. Откройте раздел **Параметры программы** окна свойств политики.
 - b. Снимите флажок **Применять технологию лечения активного заражения**.
 - c. Нажмите на кнопку **ОК** в окне свойств политики, чтобы сохранить внесенные изменения.
- В свойствах групповой задачи Kaspersky Security Center "Поиск вирусов" снимите флажок **Выполнять лечение активного заражения немедленно**.

Включение и выключение режима энергосбережения

► Чтобы включить или выключить режим энергосбережения, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры программы**.
3. В блоке **Производительность** выполните следующие действия:
 - Установите флажок **Откладывать задачи по расписанию при работе от аккумулятора**, если вы хотите включить режим энергосбережения.

Если включен режим энергосбережения, при работе от аккумулятора не запускаются следующие задачи, даже если для них задан запуск по расписанию:

 - задача обновления;
 - задача полной проверки;
 - задача проверки важных областей;
 - задача выборочной проверки;
 - задача проверки целостности.
 - Снимите флажок **Откладывать задачи по расписанию при работе от аккумулятора**, если вы хотите выключить режим энергосбережения. В этом случае Kaspersky Endpoint Security выполняет задачи, для которых задан запуск по расписанию, независимо от источника питания компьютера.
4. Сохраните внесенные изменения.

Включение и выключение режима передачи ресурсов другим программам

► Чтобы включить или выключить режим передачи ресурсов другим программам, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры программы**.
3. В блоке **Производительность** выполните следующие действия:

- Установите флажок **Уступать ресурсы другим программам**, если вы хотите включить режим передачи ресурсов другим программам.

При включенном режиме передачи ресурсов другим программам Kaspersky Endpoint Security откладывает выполнение задач, если для них задан запуск по расписанию и их выполнение замедляет работу других программ:

- задача обновления;
 - задача полной проверки;
 - задача проверки важных областей;
 - задача выборочной проверки;
 - задача проверки целостности.
- Снимите флажок **Уступать ресурсы другим программам**, если вы хотите выключить режим передачи ресурсов другим программам. В этом случае Kaspersky Endpoint Security выполняет задачи, для которых задан запуск по расписанию, независимо от работы других программ.

По умолчанию режим передачи ресурсов другим программам включен.

4. Сохраните внесенные изменения.

Создание и использование конфигурационного файла

Конфигурационный файл с параметрами работы Kaspersky Endpoint Security позволяет решить следующие задачи:

- Выполнить локальную установку Kaspersky Endpoint Security через командную строку с заранее заданными параметрами.

Для этого требуется сохранить конфигурационный файл в той же папке, где находится дистрибутив.

- Выполнить удаленную установку Kaspersky Endpoint Security через Kaspersky Security Center с заранее заданными параметрами.
- Перенести параметры работы Kaspersky Endpoint Security с одного компьютера на другой.

► *Чтобы создать конфигурационный файл, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Управление параметрами**.
3. В блоке **Управление параметрами** нажмите на кнопку **Сохранить**.
Откроется стандартное окно Microsoft Windows **Выбор конфигурационного файла**.
4. Укажите путь, по которому вы хотите сохранить конфигурационный файл, и введите его имя.

Чтобы использовать конфигурационный файл для локальной или удаленной установки Kaspersky Endpoint Security, необходимо назвать его `install.cfg`.

5. Нажмите на кнопку **Сохранить**.

► *Чтобы импортировать параметры работы Kaspersky Endpoint Security из конфигурационного файла, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Управление параметрами**.
3. В блоке **Управление параметрами** нажмите на кнопку **Загрузить**.
Откроется стандартное окно Microsoft Windows **Выбор конфигурационного файла**.
4. Укажите путь к конфигурационному файлу.
5. Нажмите на кнопку **Открыть**.

Все значения параметров Kaspersky Endpoint Security будут установлены в соответствии с выбранным конфигурационным файлом.

Работа с программой из командной строки

Этот раздел содержит описание работы с Kaspersky Endpoint Security из командной строки.

В этом разделе

Команды.....	293
Сообщения об ошибках.....	310
Коды возврата.....	314
Использование профилей задач.....	320
Приложение. Профили программы.....	322

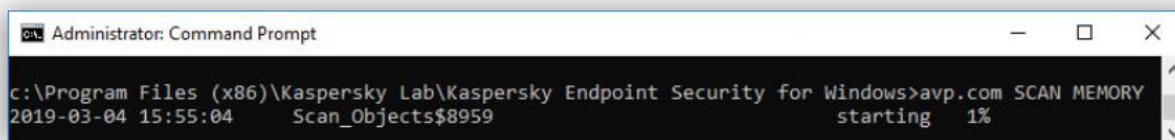
Команды

► Чтобы управлять Kaspersky Endpoint Security из командной строки, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Используйте следующий шаблон для выполнения команды:

```
avp.com <команда> [параметры]
```

В результате Kaspersky Endpoint Security выполнит команду (см. рис. ниже).



В этом разделе

SCAN. Антивирусная проверка	294
UPDATE. Обновление баз и модулей программы	298
ROLLBACK. Откат последнего обновления	300
TRACES. Трассировка	300
START. Запуск профиля	302
STOP. Остановка профиля	302
STATUS. Статус профиля	303
STATISTICS. Статистика выполнения профиля	304
RESTORE. Восстановление файлов	304
EXPORT. Экспорт параметров программы	305
IMPORT. Импорт параметров программы	306
ADDKEY. Применение файла ключа	307
LICENSE. Лицензирование	307
RENEW. Покупка лицензии	308
PBATESTRESET. Сбросить результаты проверки перед шифрованием	309
EXIT. Завершение работы программы	309
EXITPOLICY. Выключение политики	309
STARTPOLICY. Включение политики	310
DISABLE. Выключение защиты	310
SPYWARE. Обнаружение шпионского ПО	310

SCAN. Антивирусная проверка

Запустить задачу антивирусной проверки.

Синтаксис команды

```
SCAN [<область проверки>] [<действие при обнаружении угрозы>] [<типы файлов>]  
[<исключения из проверки>] [/R[A]:<файл отчета>] [<технологии проверки>]  
[/C:<файл с параметрами антивирусной проверки>]
```

Область проверки

<файлы для проверки>

/ALL

/MEMORY

/STARTUP

/MAIL

/REMDRIVES

/FIXDRIVES

/NETDRIVES

/QUARANTINE

/@:<список файлов.lst>

Список файлов и папок через пробел. Длинные пути должны быть заключены в кавычки. Короткие пути (формат MS-DOS) заключать в кавычки не требуется. Например:

- "C:\Program Files (x86)\Example Folder" – длинный путь.
- C:\PROGRA~2\EXAMPL~1 – короткий путь.

Запустить задачу *Полная проверка*. Kaspersky Endpoint Security проверяет следующие объекты:

- память ядра;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- загрузочные секторы;
- резервное хранилище операционной системы;
- все жесткие и съемные диски.

Проверить память ядра.

Проверить объекты, загрузка которых осуществляется при запуске операционной системы.

Проверить почтовый ящик Outlook.

Проверить съемные диски.

Проверить жесткие диски.

Проверить сетевые диски.

Проверить файлы в резервном хранилище Kaspersky Endpoint Security.

Проверить файлы и папки, перечисленные в списке. Каждый файл из списка нужно вводить с новой строки. Длинные пути должны быть заключены в кавычки. Короткие пути (формат MS-DOS) заключать в кавычки не требуется. Например:

- "C:\Program Files (x86)\Example Folder" – длинный путь.
- C:\PROGRA~2\EXAMPL~1 – короткий путь.

Действие при обнаружении угрозы

/i0

Информировать. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.

/i1

Лечить; информировать, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз.

/i2

Лечить; удалять, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет.

Этот вариант действия выбран по умолчанию.

/i3

Лечить обнаруженные зараженные файлы. Если лечение невозможно, удалять зараженные файлы. Также удалять составные файлы (например, архивы), если вылечить или удалить зараженный файл невозможно.

/i4

Удалять зараженные файлы. Также удалять составные файлы (например, архивы), если удалить зараженный файл невозможно.

/i8

Запрашивать действие у пользователя сразу после обнаружения угрозы.

/i9

Запрашивать действие у пользователя после выполнения проверки.

Типы файлов

/fe

Файлы, проверяемые по расширению. Если выбран этот параметр, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.

/fi

Файлы, проверяемые по формату. Если выбран этот параметр, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.

/fa

Все файлы. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений). Параметр выбран по умолчанию.

Исключения из проверки

-e:a

Исключение из проверки архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.

-e:b

Исключение из проверки почтовых баз, входящих и исходящих сообщений электронной почты.

-e:<маска файла>

Исключение из проверки файлов по маске. Например:

- Маска *.exe будет включать все пути к файлам с расширением exe.
- Маска example* будет включать все пути к файлам с именем EXAMPLE.

-e:<секунды>

Исключение из проверки файлов, длительность проверки которых превышает установленное значение в секундах.

-es:<мегабайты>

Исключение из проверки файлов, размер которых превышает установленное значение в мегабайтах.

Режим сохранения событий в файл отчета

/R:<файл отчета>

Сохранять только критические события в файл отчета.

/RA:<файл отчета>

Сохранять все события в файл отчета.

Технологии проверки

`/iChecker=on|off`

Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки.

`/iSwift=on|off`

Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.

Дополнительные параметры

`/C:<файл с параметрами антивирусной проверки>`

Файл с параметрами задачи антивирусной проверки. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: [`<область проверки>`] [`<действие при обнаружении угрозы>`] [`<типы файлов>`] [`<исключения из проверки>`] [`/R[A]:<файл отчета>`] [`<технологии проверки>`].

Пример:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

См. также

Запуск и остановка задачи проверки	52
Работа с активными угрозами	63

UPDATE. Обновление баз и модулей программы

Запустить задачу *Обновление*.

Синтаксис команды

```
UPDATE ["<источник обновления>"] [/R[A]:<файл отчета>] [/C:<файл с параметрами обновления>]
```

Источник обновления

"<источник обновления>"

Адрес HTTP-, FTP-сервера или папки общего доступа с пакетом обновлений. Вы можете указать только один источник обновления. Если источник обновлений не указан, Kaspersky Endpoint Security использует источник, указанный в задаче *Обновление*. Задача *Обновление* создается автоматически после установки программы.

Режим сохранения событий в файл отчета

/R:<файл отчета>

Сохранять только критические события в файл отчета.

/RA:<файл отчета>

Сохранять все события в файл отчета.

Дополнительные параметры

/C:<файл с параметрами обновления>

Файл с параметрами задачи *Обновление*. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: ["<источник обновления>"] [/R[A]:<файл отчета>].

Пример:

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

См. также

Запуск и остановка задачи обновления [81](#)

ROLLBACK. Откат последнего обновления

Откатить последние обновления антивирусных баз. Это позволяет вернуться к использованию предыдущей версии баз и модулей программы при необходимости, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

Синтаксис команды

```
ROLLBACK [/R[A]:<файл отчета>]
```

Режим сохранения событий в файл отчета

/R:<файл отчета>

Сохранять только критические события в файл отчета.

/RA:<файл отчета>

Сохранять все события в файл отчета.

Пример:

```
avp.com ROLLBACK /RA:rollback.txt
```

См. также

Ограничения функциональности восстановления файлов.....	114
Включение и выключение Отката вредоносных действий.....	114

TRACES. Трассировка

Включить / выключить трассировку. Файлы трассировки (см. раздел "О составе и хранении файлов трассировки" на стр. [327](#)) хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы. По умолчанию трассировка выключена.

Синтаксис команды

```
TRACES on|off [<уровень трассировки>] [<дополнительные параметры>]
```

Уровень трассировки

<уровень трассировки>

Уровень детализации трассировки. Возможные значения:

- 100 (критический). Только сообщения о неустранимых ошибках.
- 200 (высокий). Сообщения о всех ошибках, включая неустранимые.
- 300 (диагностический). Сообщения о всех ошибках, а также предупреждения.
- 400 (важный). Сообщения о всех ошибках, предупреждения, а также дополнительная информация.
- 500 (обычный). Сообщения о всех ошибках, предупреждениях, а также подробная информация о работе программы в нормальном режиме (значение по умолчанию).
- 600 (низкий). Все сообщения.

Дополнительные параметры

all	Выполнить команду с параметрами <code>dbg</code> , <code>file</code> и <code>mem</code> .
dbg	Использовать функцию <code>OutputDebugString</code> и сохранять файл трассировки. Функция <code>OutputDebugString</code> отправляет символьную строку отладчику программы для вывода на экран. Подробнее см. на <i>сайте MSDN</i> (https://msdn.microsoft.com/ru-RU/library/windows/desktop/aa363362(v=vs.85).aspx).
file	Сохранить один файл трассировки (без ограничений по размеру).
rot	Сохранить результаты трассировки в ограниченное число файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера.
mem	Записывать результаты трассировки в файлы дампов.

Примеры:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

См. также

Трассировка работы программы	326
О составе и хранении файлов трассировки	327
О составе и хранении файлов дампов	330
Запись дампов.....	330
Защита файлов дампов и трассировок.....	330

START. Запуск профиля

Запустить выполнение профиля (например, запустить обновление баз или включить компонент защиты).

Синтаксис команды

```
START <профиль> [/R[A]:<файл отчета>]
```

Профиль

<профиль>

Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей (см. раздел "Приложение. Профили программы" на стр. [322](#)) вы можете узнать по команде `HELP START`.

Режим сохранения событий в файл отчета

/R:<файл отчета>

Сохранять только критические события в файл отчета.

/RA:<файл отчета>

Сохранять все события в файл отчета.

Пример:

```
avp.com START Scan_Objects
```

STOP. Остановка профиля

Остановить выполняемый профиль (например, остановить проверку съемных дисков или выключить компонент защиты).

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. [200](#)). Пользователь должен иметь разрешения **Выключение компонентов защиты, Выключение компонентов контроля**.

Синтаксис команды

```
STOP <профиль> /login=<имя пользователя> /password=<пароль>
```

Профиль

<профиль>

Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей (см. раздел "Приложение. Профили программы" на стр. [322](#)) вы можете узнать по команде `HELP STOP`.

Авторизация

```
/login=<имя пользователя>  
/password=<пароль>
```

Данные учетной записи пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. [201](#)).

STATUS. Статус профиля

Показать информацию о состоянии профилей программы (см. раздел "Приложение. Профили программы" на стр. [322](#)) (например, `running` или `completed`). Список доступных профилей вы можете узнать по команде `HELP STATUS`.

Также Kaspersky Endpoint Security показывает информацию о состоянии служебных профилей. Информация о состоянии служебных профилей может понадобиться при обращении в Службу технической поддержки "Лаборатории Касперского".

Синтаксис команды

```
STATUS [<профиль>]
```

STATISTICS. Статистика выполнения профиля

Показать статистическую информацию о профиле программы (см. раздел "Приложение. Профили программы" на стр. [322](#)) (например, время проверки или количество обнаруженных угроз). Список доступных профилей вы можете узнать по команде `HELP STATISTICS`.

Синтаксис команды

```
STATISTICS <профиль>
```

RESTORE. Восстановление файлов

Восстановить файл из резервного хранилища в папку его исходного размещения. Если по указанному пути уже существует файл с таким же именем, к имени файла добавляется суффикс "-copy". Восстанавливаемый файл копируется с исходным именем.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. [200](#)). Пользователь должен иметь разрешение **Восстановление из резервного хранилища**.

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES\QB`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security.

В Kaspersky Endpoint Security отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Синтаксис команды

```
RESTORE [/REPLACE] <имя файла> /login=<имя пользователя> /password=<пароль>
```

Дополнительные параметры

`/REPLACE`

Переписать существующий файл.

`<имя файла>`

Имя восстанавливаемого файла.

Авторизация

```
/login=<имя пользователя>  
/password=<пароль>
```

Данные учетной записи пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. [201](#)).

Пример:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

См. также

Восстановление и удаление файлов из резервного хранилища [279](#)

EXPORT. Экспорт параметров программы

Экспортировать параметры Kaspersky Endpoint Security в файл. Файл будет размещен в папке C:\Windows\SysWOW64.

Синтаксис команды

```
EXPORT <профиль> <имя файла>
```

Профиль

<профиль>

Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей (см. раздел "Приложение. Профили программы" на стр. [322](#)) вы можете узнать по команде `HELP EXPORT`.

Файл для экспорта

<имя файла>

Имя файла, в который должны быть экспортированы параметры профиля. Вы можете экспортировать параметры профиля в конфигурационный файл в формате DAT или CFG, в текстовый файл в формате TXT или в документ в формате XML.

Примеры:

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

См. также

Создание и использование конфигурационного файла..... [292](#)

IMPORT. Импорт параметров программы

Импортировать параметры Kaspersky Endpoint Security из файла, который был создан с помощью команды EXPORT.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. [200](#)). Пользователь должен иметь разрешение **Настройка параметров программы**.

Синтаксис команды

```
IMPORT <имя файла> /login=<имя пользователя> /password=<пароль>
```

Файл для импорта

<имя файла>

Имя файла, из которого должны быть импортированы параметры программы. Вы можете импортировать параметры Kaspersky Endpoint Security из конфигурационного файла в формате DAT или CFG, текстового файла в формате TXT или документа в формате XML.

Авторизация

```
/login=<имя пользователя>  
/password=<пароль>
```

Данные учетной записи пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. [201](#)).

Пример:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

См. также

Создание и использование конфигурационного файла..... [292](#)

ADDKEY. Применение файла ключа

Применить файл ключа для активации Kaspersky Endpoint Security. Если программа уже активирована, ключ будет добавлен в качестве резервного.

Синтаксис команды

```
ADDKEY <имя файла> [/login=<имя пользователя> /password=<пароль>]
```

Файл ключа

<имя файла>

Имя файла ключа.

Авторизация

```
/login=<имя пользователя>  
/password=<пароль>
```

Данные учетной записи пользователя. Данные учетные записи нужно вводить, только если включена Защита паролем (на стр. [197](#)).

Пример:

```
avp.com ADDKEY file.key
```

LICENSE. Лицензирование

Выполнить операции с лицензионными ключами программы Kaspersky Endpoint Security.

Для выполнения команды удаления лицензионного ключа должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. [200](#)). Пользователь должен иметь разрешение **Удаление ключа**.

Синтаксис команды

```
LICENSE <операция> [/login=<имя пользователя> /password=<пароль>]
```

Операция

`/CHECK`

Показать информацию о лицензии, по которой активирована программа.

`/ADD <имя файла>`

Применить файл ключа для активации Kaspersky Endpoint Security. Если программа уже активирована, ключ будет добавлен в качестве резервного.

`/ADD <код активации>`

Активировать Kaspersky Endpoint Security с помощью кода активации. Если программа уже активирована, ключ будет добавлен в качестве резервного.

`/REFRESH <имя файла>`

Продлить срок действия лицензии с помощью файла ключа. В результате будет добавлен резервный ключ, который станет активным по истечении срока действия лицензии. Добавить активный ключ с помощью этой команды невозможно.

`/REFRESH <код активации>`

Продлить срок действия лицензии с помощью кода активации. В результате будет добавлен резервный ключ, который станет активным по истечении срока действия лицензии. Добавить активный ключ с помощью этой команды невозможно.

`/DEL /login=<имя пользователя>`

`/password=<пароль>`

Удалить лицензионный ключ. Также будет удален резервный ключ.

Авторизация

`/login=<имя пользователя>`

`/password=<пароль>`

Данные учетной записи пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. [201](#)).

Пример:

- `avp.com LICENSE /ADD file.key`
- `avp.com LICENSE /ADD AAAAAA-BBBBBB-CCCCC-DDDDD`
- `avp.com LICENSE /DEL /login=KLAdmin /password=!Password1`

RENEW. Покупка лицензии

Перейти на веб-сайт "Лаборатории Касперского" для покупки лицензии или продления ее срока действия.

РВАТРЕТРЕТРЕТ. Сбросить результаты проверки перед шифрованием

Сбросить результаты проверки поддержки полнодискового шифрования по технологии BitLocker. Также результаты включают в себя проверку совместимости компьютера с Агентом аутентификации.

Перед запуском полнодискового шифрования программа выполняет ряд проверок на возможность шифрования компьютера по технологии BitLocker. Если шифрование компьютера невозможно, Kaspersky Endpoint Security сохраняет информацию о несовместимости. При следующей попытке шифрования программа не выполняет проверки и предупреждает о том, что шифрование невозможно. Если аппаратная конфигурация компьютера изменилась, то для проверки системного жесткого диска на совместимость с Агентом аутентификации и поддержку технологии BitLocker требуется сбросить информацию о несовместимости, полученную программой при предыдущей проверке.

См. также

Полнодисковое шифрование с помощью технологии Шифрование диска BitLocker [214](#)

EXIT. Завершение работы программы

Завершить работу Kaspersky Endpoint Security. Программа будет выгружена из оперативной памяти компьютера.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. [200](#)). Пользователь должен иметь разрешение **Завершение работы программы**.

Синтаксис команды

```
EXIT /login=<имя пользователя> /password=<пароль>
```

EXITPOLICY. Выключение политики

Выключает политику Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком (🔒).

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. [200](#)). Пользователь должен иметь разрешение **Выключение политики Kaspersky Security Center**.

Синтаксис команды

```
EXITPOLICY /login=<имя пользователя> /password=<пароль>
```

STARTPOLICY. Включение политики

Включить политику Kaspersky Security Center на компьютере. Параметры программы будут настроены в соответствии с политикой.

DISABLE. Выключение защиты

Выключить Защиту от файловых угроз на компьютере с истекшей лицензией на Kaspersky Endpoint Security. Выполнить команду на компьютере с неактивированной программой или с действующей лицензией невозможно.

SPYWARE. Обнаружение шпионского ПО

Включить / выключить обнаружение шпионского ПО. По умолчанию обнаружение шпионского ПО включено.

Синтаксис команды

```
SPYWARE on|off
```

Сообщения об ошибках

Сообщение об ошибке в командной строке	Код возврата в Shell
Error %d getting thread's context	
Error %d loading QueryInformationThread function	
Error %d opening thread	
Error %d querying thread information	
Error %d suspending thread	
Error in UpdateKSNConfig	
Error in thread safety code: could not acquire a lock	
Error: %S (err 0x%x)	
Error: %S: %s (err 0x%x)	
Error: '%S' has not been completed due to execution timeout	_Shell::_E_TIMEOUT
Error: '%S' is disabled	
Error: Cannot change state for '%S' (%S), task already in state?	SHELL_RET_FAILED
Error: Cannot change state for '%S' (%S), task disabled?	SHELL_RET_FAILED
Error: Cannot create message receiver	
Error: Cannot create task, err=%08X	SHELL_RET_FAILED
Error: Cannot find task '%S'	SHELL_RET_FAILED /SHELL_RET_PARAMETER_INVALID
Error: Cannot get product settings	
Error: Cannot get tasks list	SHELL_RET_FAILED
Error: Cannot initialize task parameters block	SHELL_RET_PARAMETER_INVALID
Error: Cannot open configuration file '%S'	
Error: Cannot open list file '%S'	
Error: Cannot set report handler	
Error: Cannot start task '%S', error=%08X	SHELL_RET_NO_LICENCE

Сообщение об ошибке в командной строке	Код возврата в Shell
Error: Cannot start task '%S', no licence	_Shell::_S_NO_LICENSE
Error: Cannot start task '%S', parameters invalid	SHELL_RET_PARAMETER_INVALID
Error: Cannot verify task parameters block	
Error: Change state failed for task '%S' (%S), error=%08X	SHELL_RET_FAILED
Error: Command unavailable due to password protection disabled	
Error: Configuration file not specified (/C)	
Error: Credential is not obtained, access denied	
Error: Duplicate taskid '%S'	
Error: Failed to flush cached data	
Error: File list not specified	
Error: File list not specified (/@)	
Error: Internal error %08X	SHELL_RET_FAILED
Error: Invalid command '%S'	
Error: Invalid parameter '%S'	
Error: Local task control is denied by policy	
Error: NOT IMLEMENTED	SHELL_RET_FAILED
Error: Not enough memory	
Error: Nothing to scan	
Error: Parameter '%S' must contain exclusion specification	
Error: Parameter '%S' must specify size in megabytes	
Error: Parameter not supported by task '%S'	
Error: Password or login is invalid, access denied	
Error: Profile name must be specified	SHELL_RET_PARAMETER_INVALID
Error: Task '%S' not found	SHELL_RET_TASK_FAILED
Error: Unknown parameter '%S'	

Сообщение об ошибке в командной строке	Код возврата в Shell
Error: Usage parameter /APP=<on off>	
Error: Usage parameter /iChecker=<on off>	
Error: Usage parameter /iSwift=<on off>	
Error: cannot open report file %S, error=%d %s	
Error: control of this task is not allowed	
Error: failed to register message handlers	
Error: failed to set INetSwift state	
Error: failed to unregister message handlers	
Error: Local task control is denied by policy	
Scan_Quarantine failed: %	SHELL_RET_FAILED
Scan_Quarantine completed successfully	SHELL_RET_OK
Failed to get AVP_SERVICE_PRODUCT. Error	SHELL_RET_FAILED
Disable command cannot be elevated. Error	SHELL_RET_FAILED
Failed to disable product from command line. Error	SHELL_RET_FAILED
Failed to get AVP_SERVICE_PRODUCT. Error	
Failed to get TaskManager service. Error	
Failed to get service locator. Error	
Invalid parameters	SHELL_RET_PARAMETER_INVALID
Failed while activating Global KSN	SHELL_RET_FAILED
Failed to execute command set silent detect. Error	_Shell::_E_FAIL
Failed to execute command silent detect check. Error	_Shell::_E_FAIL
Path not exist	
Cannot write to file, no permission	
Cannot add key file	SHELL_RET_TASK_FAILED
INetSwift state set to	SHELL_RET_OK

Сообщение об ошибке в командной строке	Код возврата в Shell
Internal error	SHELL_RET_FAILED
Fail to terminate command on user's request	_Shell::_E_BREAK_FAIL
Command is terminated on user's request	_Shell::_E_BREAK_OK

Коды возврата

Любая команда, выполняемая администратором в командной строке, может возвращать код возврата. Коды возврата бывают general или специфичные для отдельных задач.

Доступны следующие коды возврата:

- General коды возврата:
 - 0 - задача выполнена успешно;
 - 1 - некорректное значение параметра;
 - 2 - неизвестная ошибка;
 - 3 - ошибка во время выполнения задачи;
 - 4 - выполнение задачи прервано.
- Коды возврата задач антивирусной проверки:
 - 101 - все опасные объекты обработаны;
 - 102 - обнаружены опасные объекты.
- Коды возврата других задач:
 - -14 - истекло время ожидания.
 - 239 - ошибка во время приостановки задачи.
 - 240 - задача отменена пользователем.
 - -15 - файл заблокирован другим процессом и недоступен для обработки программой.
 - -10 - указан неверный путь к объекту.
 - -8 - ключ недействителен.
 - -7 - ключ находится в черном списке.
 - -13 - ключ предназначен для другого продукта.
 - [1-127] - дни до истечения срока действия лицензии.

Если до истечения срока действия лицензии осталось более 127 дней, код возврата 127. Если до истечения срока действия лицензии осталось менее 127 дней, код возврата соответствует реальному количеству дней. Если лицензия уже истекла, код возврата 1.

- 8000045 - недостаточно прав.
- 102 - есть необработанные угрозы.

Таблица 3. Символьные и числовые значения кодов возврата

Символьные значения	Числовые значения	Доступно для команд
_Shell::_E_TIMEOUT	-14	START UPDATE ROLLBACK SCAN
_Shell::_E_BREAK_FAIL	239	UPDATE ROLLBACK SCAN
_Shell::_E_BREAK_OK	240	UPDATE ROLLBACK SCAN
_Shell::_E_FAIL	-3	MESSAGES LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket /DeleteKey /Refresh
_Shell::_E_FILE_BLOCKED	-15	UPDATE ROLLBACK SCAN
_Shell::_E_INVALID_PATH	-10	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_Shell::_E_INVALID_SYNTAX	-2	UPDATE ROLLBACK MESSAGES SCAN
_Shell::_E_KEY_CORRUPTED	-8	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_Shell::_E_KEY_IN_BLST	-7	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket

Символьные значения	Числовые значения	Доступно для команд
_Shell::_E_KEY_NOT_MATCH	-13	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_Shell::_S_ALL_DETECTION	2	UPDATE ROLLBACK SCAN
_Shell::_S_NO_LICENSE	0	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket /DeleteKey
_Shell::_S_OK	0	UPDATE ROLLBACK SCAN LICENSE: /Add (ActivateByKeyEx) /AddTicket /Refresh
_Shell::_S_PARTIAL_DETECTION	3	UPDATE ROLLBACK SCAN
[1-127]	[1-127]	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket
errACCESS_DENIED	8000045	STOP EXITPOLICY

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_FAILED	2	START STOP STATUS STATISTICS MODE HELP EXPORT IMPORT EXIT ADDKEY INETSWIFT EXITPOLICY STARTPOLICY UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SPYWARE MESSAGES RESTORE PBATESTRESET PATCHCOMPATIBILITYRESET SCAN
-SHELL_RET_FAILED	-2	LICENSE: /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_NO_LICENCE	2	START UPDATE ROLLBACK SCAN

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_OK	0	START STOP STATUS STATISTICS HELP EXPORT IMPORT EXIT ADDKEY INETSWIFT EXITPOLICY STARTPOLICY UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SLC SPYWARE LETSDUMP MESSAGES RESTORE PBATESTRESET PATCHCOMPATIBILITYRESET SCAN LICENSE: /Add (ActivateByCode)

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_PARAMETER_INVALID	1	START STOP STATUS STATISTICS EXPORT IMPORT ADDKEY INETSWIFT UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SPYWARE RESTORE PATCHCOMPATIBILITYRESET SCAN
-SHELL_RET_PARAMETER_INVALID	-1	LICENSE: /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_SCAN_ALL_THREATS	101	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_NO_THREATS	0	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_SUSPICIOUS_UNTREATED	0	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_THREATS	102	UPDATE ROLLBACK SCAN

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_TASK_FAILED	3	STOP EXPORT IMPORT ADDKEY UPDATE ROLLBACK RESTORE SCAN
-SHELL_RET_TASK_FAILED	-3	LICENSE: /Add (ActivateByKey) /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_TASK_STOPPED	4	UPDATE ROLLBACK SCAN

Использование профилей задач

Профиль задачи (далее также "профиль") – это набор параметров в текстовом или бинарном виде для создания задачи Kaspersky Endpoint Security.

Профили определяются в реестре операционной системы Windows в ветке `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES10SP2\profiles` или `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES10SP2\profiles`.

Профили имеют иерархическую структуру. Изменения, внесенные в родительский профиль, отражаются и на профилях, входящих в его состав. Например, при удалении родительского профиля все профили, входящие в его состав, также будут удалены.

Профиль может содержать следующие параметры:

- `flags` – внутренний механизм, описывающий доступные операции с задачей;
- `enabled` – параметр, разрешающий или запрещающий запуск задачи;
- `installed` – внутренний механизм, определяющий, установлены ли модули для данного профиля;
- `level` – внутренний механизм, используемый для разделения параметров по уровням;
- `type` – текстовое описание типа задачи;
- `remote` – параметр, позволяющий запустить задачу в отдельном процессе;

- `admflags` - параметры управления задачей с помощью Kaspersky Security Center;
- `pid` – идентификатор бинарного модуля, который содержит реализацию задачи;
- `iid` – идентификатор интерфейса задачи, определяющий класс, который содержит исполняемый код для работы задачи;
- `persistent` – параметр, определяющий количество задач одного типа, которые можно создать в программе Kaspersky Endpoint Security;
- `idSettings` – идентификатор структуры параметров;
- `idStatistics` – идентификатор структуры статистики выполнения задачи;
- `schedule` – параметры расписания задачи;
- `runas` – параметры прав запуска задачи (используется только при значении параметра `persistent = 0`);
- `smode` – параметр, используемый для отложенного выполнения задачи;
- `settings` – дополнительные параметры задачи;
- `def` – параметры задачи, установленные по умолчанию.

Kaspersky Endpoint Security выполняет задачи на основе заданных параметров профиля. При создании задачи программа считывает все профили из реестра и для каждого профиля выполняет следующие действия:

1. Создает пустую структуру параметров с типом `idSettings`.
2. Десериализует значения параметра `settings` в подготовленную структуру.

Если значения параметра `settings` не заданы, то программа использует значения параметра `def` и десериализует их в структуру. При отсутствии значений параметра `def` используются системные значения, заданные по умолчанию для пустой структуры параметров.

3. Создает пустую структуру с типом `idStatistics`, если этот параметр был указан в профиле для создаваемой задачи.
4. Находит бинарный модуль по идентификатору `pid`.
5. Создает экземпляр задачи по идентификатору `iid` из бинарного модуля.
6. Передает структуру параметров и статистики полученному экземпляру задачи.
7. Если указаны значения параметров `installed = 1` и `persistent = 1`, то программа запускает задачу.
8. Если указано значение параметра `persistent = 0`, то программа проверяет параметры `schedule` и `smode` и планирует запуск задачи в соответствии с заданными значениями.

Консоль администрирования Kaspersky Security Center позволяет создавать несколько групповых задач одного типа с различными параметрами. Для каждой такой задачи в реестре создается профиль с названием вида `<profile name>${unique id}`, где `unique id` - уникальный идентификатор для задачи.

Профили программы

Профиль – компонент, задача или функция Kaspersky Endpoint Security. Профили предназначены для управления программой из командной строки. Вы можете использовать профили для выполнения команд `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT` и `IMPORT`. С помощью профилей вы можете настроить параметры программы (например, `STOP DeviceControl`) или запустить задачу (например, `START Scan_My_Computer`).

Доступны следующие профили:

- `AdaptiveAnomaliesControl` – Адаптивный контроль аномалий.
- `AMSI` – Поставщик AMSI-защиты.
- `BehaviorDetection` – Анализ поведения.
- `DeviceControl` – Контроль устройств.
- `EntAppControl` – Контроль программ.
- `File_Monitoring` или `FM` – Защита от файловых угроз.
- `Firewall` или `FW` – Сетевой экран.
- `HIPS` – Предотвращение вторжений.
- `IDS` – Защита от сетевых угроз.
- `IntegrityCheck` – Проверка целостности.
- `Mail_Monitoring` или `EM` – Защита от почтовых угроз.
- `Rollback` – Откат обновления.
- `Scan_ContextScan` – Проверка из контекстного меню.
- `Scan_IdleScan` – Фоновая проверка.
- `Scan_Memory` – Проверка памяти ядра.
- `Scan_My_Computer` – Полная проверка.
- `Scan_Objects` – Выборочная проверка.
- `Scan_Qscan` – Проверка объектов, загрузка которых осуществляется при запуске операционной системы.
- `Scan_Removable_Drive` – Проверка съемных дисков.
- `Scan_Startup` или `STARTUP` – Проверка важных областей.
- `Updater` – Обновление.
- `Web_Monitoring` или `WM` – Защита от веб-угроз.
- `WebControl` – Веб-Контроль.

Также Kaspersky Endpoint Security поддерживает работу служебных профилей. Служебные профили могут понадобиться при обращении в Службу технической поддержки "Лаборатории Касперского".

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. [324](#)).

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением 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:

- позвонить в Службу технической поддержки по телефону (<https://support.kaspersky.ru/b2b>) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (<https://support.kaspersky.ru/b2b>).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) – это портал для организаций, использующих программы "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 информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас создать *файл трассировки*. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на компьютере, подробные отчеты работы компонентов программы.

Во время работ по диагностике специалисты Службы технической поддержки могут попросить вас изменить параметры программы:

- Активировать функциональность получения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения полученной диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав полученных в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в Руководстве администратора или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

В этом разделе

Трассировка работы программы	326
О составе и хранении файлов трассировки	327
О составе и хранении файлов дампов	330
Запись дампов.....	330
Защита файлов дампов и трассировок.....	330

Трассировка работы программы

Трассировка программы – это подробная запись действий, выполняемых программой, и сообщений о событиях, происходящих во время работы программы.

Выполняйте трассировку программы под руководством Службы технической поддержки "Лаборатории Касперского".

► *Чтобы создать файл трассировки программы, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Поддержка**.
Откроется окно **Поддержка**.
2. В окне **Поддержка** нажмите на кнопку **Трассировка системы**.
Откроется окно **Информация для поддержки**.
3. Чтобы запустить процесс трассировки, выберите один из следующих элементов в раскрывающемся списке **Трассировка программы**:
 - **Включена**.
Выберите этот элемент, чтобы включить трассировку.
 - **С ротацией**.
Выберите этот элемент, чтобы включить трассировку и ограничить максимальное количество файлов трассировки и максимальный размер каждого из файлов трассировки. Если записано максимальное количество файлов трассировки максимального размера, то удаляется наиболее старый файл трассировки и начинается запись нового файла трассировки.
Если выбран этот элемент, вы можете указать значение для следующих полей:
 - **Максимальное количество файлов для ротации**.
 - **Максимальный размер каждого файла**.

4. В раскрываемом списке **Уровень** выберите уровень трассировки.
Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки. Если указания Службы технической поддержки отсутствуют, рекомендуется устанавливать уровень трассировки **Обычный (500)**.
5. Перезапустите Kaspersky Endpoint Security.
6. Чтобы остановить процесс трассировки, вернитесь в окно **Информация для поддержки** и выберите **Выключена** в раскрываемом списке **Трассировка программы**.

Вы также можете создать файлы трассировки во время установки программы из командной строки, в том числе с помощью файла `setup.ini`.

О составе и хранении файлов трассировки

Вы сами несете ответственность за обеспечение безопасности полученной информации и, в частности, за контроль и ограничение доступа к полученной информации, хранимой на компьютере, до ее передачи в "Лабораторию Касперского".

Файлы трассировки хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы.

Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке `%ProgramData%\Kaspersky Lab`.

Файлы трассировки называются следующим образом: `KES<номер версии>_dateXX.XX_timeXX.XX_pidXXX.><тип файла трассировки>.log`.

Вы можете просмотреть данные, записанные в файлы трассировки.

Все файлы трассировки содержат следующие общие данные:

- Время события.
- Номер потока выполнения.

Эту информацию не содержит файл трассировки Агента аутентификации.

- Компонент программы, в результате работы которого произошло событие.
- Степень важности события (информационное, предупреждение, критическое, ошибка).
- Описание события выполнения команды компонента программы и результата выполнения этой команды.

Kaspersky Endpoint Security сохраняет пароли пользователя в файл трассировки только в зашифрованном виде.

Содержание файлов трассировки SRV.log, GUI.log и ALL.log

В файлы трассировки `SRV.log`, `GUI.log` и `ALL.log`, помимо общих данных, может записываться следующая информация:

- Персональные данные, в том числе фамилия, имя и отчество, если эти данные являются частью пути к файлам на локальном компьютере.
- Данные об установленном на компьютере аппаратном обеспечении (например, данные о прошивке BIOS / UEFI). Эти данные записываются в файлы трассировки при выполнении полнодискового шифрования по технологии Шифрование диска Kaspersky.
- Имя пользователя и пароль, если они передавались в открытом виде. Эти данные могут записываться в файлы трассировки при проверке интернет-трафика.
- Имя пользователя и пароль, если они содержатся в заголовках протокола HTTP.
- Имя учетной записи для входа в Microsoft Windows, если имя учетной записи является частью имени файла.
- Адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта.
- Веб-сайты, которые вы посещаете, а также ссылки с этих веб-сайтов. Эти данные записываются в файлы трассировки, когда программа проверяет веб-сайты.
- Адрес прокси-сервера, имя компьютера, порт, IP-адрес, имя пользователя, используемое при авторизации на прокси-сервере. Эти данные записываются в файлы трассировки, если программа использует прокси-сервер.
- Внешние IP-адреса, с которыми было установлено соединение с вашего компьютера.
- Тема сообщения, идентификатор, имя отправителя и адрес веб-страницы отправителя сообщения в социальной сети. Эти данные записываются в файлы трассировки, если включен компонент Веб-Контроль.
- Данные о сетевом трафике. Эти данные записываются в файлы трассировки, если включены компоненты мониторинга трафика (например, Веб-Контроль).
- Данные, полученные с серверов "Лаборатории Касперского" (например, версия антивирусных баз).
- Статусы компонентов Kaspersky Endpoint Security и сведения об их работе.
- Данные о действиях пользователя в программе.
- События операционной системы.

Содержание файлов трассировки HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Файл трассировки `HST.log`, помимо общих данных, содержит информацию о выполнении задачи обновления баз и программных модулей.

Файл трассировки `BL.log`, помимо общих данных, содержит информацию о событиях, возникающих во время работы программы, а также данные, необходимые для устранения неполадок в работе программы. Этот файл создается, если программа запускается с параметром `avr.exe -bl`.

Файл трассировки `Dumpwriter.log`, помимо общих данных, содержит служебную информацию, необходимую для устранения неполадок, возникающих при записи файла дампа программы.

Файл трассировки `WD.log`, помимо общих данных, содержит информацию о событиях, возникающих в процессе работы службы `avrsus`, в том числе события обновления программных модулей.

Файл трассировки `AVPCon.dll.log`, помимо общих данных, содержит информацию о событиях, возникающих при работе модуля связи с Kaspersky Security Center.

Содержание файлов трассировки производительности

Файлы трассировки производительности называются следующим образом: KES<номер версии_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl.

Файлы трассировки производительности, помимо общих данных, содержат информацию о нагрузке на процессор, о времени загрузки операционной системы и программ, о запущенных процессах.

Содержание файла трассировки компонента Поставщик AMSI-защиты

Файл трассировки AMSI.log, помимо общих данных, содержит информацию о результатах проверок, запрошенных сторонними приложениями.

Содержание файла трассировки компонента Защита от почтовых угроз

Файл трассировки mcou.OUTLOOK.EXE.log, помимо общих данных, может содержать части сообщений электронной почты, в том числе адреса электронной почты.

Содержание файла трассировки компонента Проверка из контекстного меню

Файл трассировки shellex.dll.log, помимо общих данных, содержит информацию о выполнении задачи проверки и данные, необходимые для устранения неполадок в работе программы.

Содержание файлов трассировки веб-плагина программы

Файлы трассировки веб-плагина программы хранятся на компьютере, на котором развернута Kaspersky Security Center 11 Web Console, в папке Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 11\logs.

Файлы трассировки веб-плагина программы называются следующим образом:

logs-kes_windows-<тип файла трассировки>.DESKTOP-<дата обновления файла>.log. Web Console начинает записывать данные после установки и удаляет файлы трассировки после удаления Web Console.

Файлы трассировки веб-плагина программы, помимо общих данных, содержат следующую информацию:

- Пароль пользователя KAdmin для разблокировки интерфейса Kaspersky Endpoint Security (Защита паролем).
- Временный пароль для разблокировки интерфейса Kaspersky Endpoint Security (Защита паролем).
- Имя пользователя и пароль для почтового SMTP-сервера (Уведомления по электронной почте).
- Имя пользователя и пароль для прокси-сервера сети интернет (Прокси-сервер).
- Имя пользователя и пароль для задачи *Изменение состава компонентов программы*.
- Учетные данные и пути, указанные в свойствах политики и в задачах Kaspersky Endpoint Security.

Содержание файла трассировки Агента аутентификации

Файл трассировки Агента аутентификации хранится в папке System Volume Information и называется следующим образом: KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBLOG.bin.

Файл трассировки Агента аутентификации, помимо общих данных, содержит информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации.

О составе и хранении файлов дампов

Сохраненные дампы могут содержать конфиденциальные данные. Для контроля доступа к данным вам нужно самостоятельно обеспечить защиту файлов дампов.

Файлы дампов хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы. Файлы дампов хранятся в папке %ProgramData%\Kaspersky Lab.

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security на момент создания этого файла дампа.

Запись дампов

Сохраненные дампы могут содержать конфиденциальные данные. Для контроля доступа к данным вам нужно самостоятельно обеспечить защиту файлов дампов.

Файлы дампов хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы. Файлы дампов хранятся в папке %ProgramData%\Kaspersky Lab.

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security на момент создания этого файла дампа.

► *Чтобы включить или выключить запись дампов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Настройка**.
2. В окне параметров программы выберите раздел **Общие параметры** → **Параметры программы**.
3. В блоке **Отладочная информация** нажмите на кнопку **Настройка**.
Откроется окно **Отладочная информация**.
4. Выполните одно из следующих действий:
 - Установите флажок **Включить запись дампов**, если вы хотите чтобы программа записывала дампы программы.
 - Снимите флажок **Включить запись дампов**, если вы не хотите чтобы программа записывала дампы программы.
5. Нажмите на кнопку **ОК** в окне **Отладочная информация**.
6. Нажмите на кнопку **Сохранить** в главном окне программы, чтобы сохранить внесенные изменения.

Защита файлов дампов и трассировок

Файлы дампов и файлы трассировки содержат информацию об операционной системе, а также могут содержать данные пользователя (см. раздел "О составе и хранении файлов трассировки" на стр. [327](#)). Чтобы предотвратить несанкционированный доступ к этим данным, вы можете включить защиту файлов дампов и файлов трассировки.

Если защита файлов дампов и файлов трассировки включена, доступ к файлам имеют следующие пользователи:

- К файлам дампов имеют доступ системный и локальный администраторы, а также пользователь, включивший запись файлов дампов и файлов трассировки.
 - К файлам трассировки имеют доступ только системный и локальный администраторы.
- *Чтобы включить или выключить защиту файлов дампов и файлов трассировки, выполните следующие действия:*
1. В главном окне программы нажмите на кнопку **Настройка**.
 2. В окне параметров программы выберите раздел в разделе **Общие параметры** → **Параметры программы**.
 3. В блоке **Отладочная информация** нажмите на кнопку **Настройка**.
Откроется окно **Отладочная информация**.
 4. Выполните одно из следующих действий:
 - Установите флажок **Включить защиту файлов дампов и файлов трассировки**, если вы хотите включить защиту.
 - Снимите флажок **Включить защиту файлов дампов и файлов трассировки**, если вы хотите выключить защиту.
 5. Нажмите на кнопку **ОК** в окне **Отладочная информация**.
 6. Нажмите на кнопку **Сохранить** в главном окне программы, чтобы сохранить внесенные изменения.
- Файлы дампов и файлы трассировки, записанные при включенной защите, остаются защищенными после отключения этой функции.

Глоссарий

О

OLE-объект

Файл, присоединенный или встроенный в другой файл. Программы "Лаборатории Касперского" позволяют проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel® в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

А

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и программами "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех программ "Лаборатории Касперского", работающих в операционной системе Windows. Для программ, работающих в других операционных системах, предназначены 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.

Активный ключ

Ключ, используемый в текущий момент для работы программы.

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.

Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

Б

База вредоносных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как опасное. Список сформирован специалистами "Лаборатории Касперского", регулярно обновляется и входит в поставку программы "Лаборатории Касперского".

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами "Лаборатории Касперского" как фишинговые. База регулярно обновляется и входит в поставку программы "Лаборатории Касперского".

Г

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

Д

Доверенный платформенный модуль

Микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины.

З

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Зараженный файл

Файл, внутри которого содержится вредоносный код (при проверке файла был обнаружен код известной программы, представляющей угрозу). Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими файлами, поскольку это может привести к заражению вашего компьютера.

И

Издатель сертификата

Центр сертификации, выдавший сертификат.

К

Коннектор к Агенту администрирования

Функциональность программы, обеспечивающая связь программы с Агентом администрирования. Агент администрирования предоставляет возможность удаленного управления программой через Kaspersky Security Center.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

Ложное срабатывание

Ситуация, когда незараженный файл определяется программой "Лаборатории Касперского" как зараженный ввиду того, что его код напоминает код вируса.

М

Маска файла

Представление названия и расширения файла общими символами.

Для формирования маски файла можно использовать любые символы, допустимые в названиях файлов, в том числе специальные:

- * – символ, заменяющий нуль или более нуль любых символов;
- ? – символ, заменяющий любой один символ.

Следует иметь в виду, что название и расширение файла всегда пишутся через точку.

Н

Настройки задачи

Настройки работы программы, специфичные для каждого типа задач.

Нормализованная форма адреса веб-ресурса

Нормализованной формой адреса веб-ресурса называется текстовое представление адреса веб-ресурса, полученное в результате применения нормализации. Нормализация – процесс, в результате которого текстовое представление адреса веб-ресурса изменяется в соответствии с определенными правилами (например, исключение из текстового представления адреса веб-ресурса имени пользователя, пароля и порта соединения, понижение верхнего регистра символов адреса веб-ресурса до нижнего регистра).

В контексте работы компонентов защиты цель нормализации адресов веб-ресурсов заключается в том, чтобы проверять синтаксически различные, но физически эквивалентные адреса веб-ресурсов один раз.

Пример:

Ненормализованная форма адреса: `www.Example.com\.`

Нормализованная форма адреса: `www.example.com.`

О

Область защиты

Объекты, которые компонент базовой защиты постоянно проверяет во время своей работы. Область защиты разных компонентов имеет разные свойства.

Область проверки

Объекты, которые Kaspersky Endpoint Security проверяет во время выполнения задачи проверки.

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Отпечаток сертификата

Информация, по которой можно проверить подлинность сертификата сервера. Отпечаток создается путем применения криптографической хеш-функции к содержанию сертификата сервера.

П

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

Портативный файловый менеджер

Программа, предоставляющая интерфейс для работы с зашифрованными файлами на съемных дисках при недоступности функциональности шифрования на компьютере.

Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe, dll и др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

Программные модули

Файлы, входящие в состав дистрибутива программы "Лаборатории Касперского" и отвечающие за реализацию его основных задач. Каждому типу задач, реализуемых программой (Постоянная защита, Проверка по требованию, Обновление), соответствует свой исполняемый модуль. Запуская из главного окна полную проверку вашего компьютера, вы инициируете запуск модуля этой задачи.

Р

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их лечением или удалением.

Резервный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

С

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского" и управления ими.

Сертификат

Электронный документ, содержащий открытый ключ, информацию о владельце ключа и области применения ключа, а также подтверждающий принадлежность открытого ключа владельцу. Сертификат должен быть подписан выдавшим его центром сертификации.

Сетевая служба

Набор параметров, характеризующих сетевую активность. Для этой сетевой активности вы можете создать сетевое правило, регулирующее работу Сетевого экрана.

Сигнатурный анализ

Технология обнаружения угроз, которая использует базы Kaspersky Endpoint Security, содержащие описания известных угроз и методы их устранения. Защита с помощью сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" этот метод анализа всегда включен.

Субъект сертификата

Держатель закрытого ключа, связанного с сертификатом. Это может быть пользователь, программа, любой виртуальный объект, компьютер или служба.

Ф

Фишинг

Вид интернет-мошенничества, заключающийся в рассылке сообщений электронной почты с целью кражи конфиденциальных данных, как правило, финансового характера.

Ч

Черный список адресов

Список адресов электронной почты, входящие сообщения с которых блокируются программой "Лаборатории Касперского" независимо от их содержания.

Э

Эвристический анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

Эксплойт

Программный код, который использует какую-либо уязвимость в системе или программном обеспечении. Эксплойты часто используются для установки вредоносного программного обеспечения на компьютере без ведома пользователя.

Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в папке установки программы.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 4. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	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 программы	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

Приложение 1. Значения параметров программы в сертифицированной конфигурации

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, 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 5. Параметры и их безопасные значения для программы в сертифицированной конфигурации

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Продвинутая защита		
Kaspersky Security Network	Kaspersky Security Network	Флажок снят. Допускается устанавливать флажок только при использовании Локального KSN (Kaspersky Private Security Network – KPSN).
Откат вредоносных действий	Откат вредоносных действий	Флажок установлен.
Базовая защита		
Защита от файловых угроз	Защита от файловых угроз	Флажок установлен.
Защита от файловых угроз	Уровень безопасности	Одно из следующих значений: <ul style="list-style-type: none"> • Рекомендуемый. • Высокий.
Защита от файловых угроз	Действие при обнаружении угрозы	Лечить; удалять, если лечение невозможно.
Защита от файловых угроз → Настройка (Общие)	Типы файлов	Все файлы.
Защита от файловых угроз → Настройка (Общие)	Область защиты	Все съемные диски, Все жесткие диски, Все сетевые диски.
Защита от файловых угроз → Настройка (Производительность)	Эвристический анализ	Флажок установлен.
Защита от файловых угроз → Настройка (Производительность)	Проверять архивы	Флажок установлен.
Защита от почтовых угроз	Защита от почтовых угроз	Флажок установлен.
Защита от почтовых угроз	Уровень безопасности	Одно из следующих значений: <ul style="list-style-type: none"> • Рекомендуемый. • Высокий.
Защита от почтовых угроз	Действие при обнаружении угрозы	Лечить; удалять, если лечение невозможно.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Защита от сетевых угроз	Защита от сетевых угроз	Флажок установлен.
Защита от сетевых угроз	Добавить атакующий компьютер в список блокирования на N минут	Флажок установлен. Время блокирования – 60 мин.
Защита от сетевых угроз	Исключения	Пустой список IP-адресов. Добавление некоторых исключений может вести к выходу из безопасного состояния. Администратору безопасности следует осторожно подходить к выбору исключений. Для минимизации риска рекомендуется оставить значения по умолчанию.
Контроль безопасности		
Контроль программ	Контроль программ	Флажок установлен.
Задачи		
Обновление	Загружать обновления модулей программы	Флажок снят.
Общие параметры		
Параметры программы	Запускать Kaspersky Endpoint Security для Windows при включении компьютера	Флажок установлен.
Параметры программы	Применять технологию лечения активного заражения	Флажок установлен.
Параметры программы	Включить самозащиту	Флажок установлен.
Параметры программы	Выключить внешнее управление системными службами	Флажок установлен.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Исключения	Объекты для обнаружения	Вирусы, черви; Троянские программы; Вредоносные утилиты; Упакованные файлы, которые могут нанести вред; Многократно упакованные файлы
Исключения	Исключения из проверки и доверенные программы	Список исключений пуст. Добавление некоторых исключений может вести к выходу из безопасного состояния. Администратору безопасности следует осторожно подходить к выбору исключений. Для минимизации риска рекомендуется оставить значения по умолчанию.
Интерфейс → Настройка (Защита паролем)	Включить защиту паролем	Флажок установлен. Администратор безопасности должен установить надежный пароль и область действия (все опции).

Приложение 2. Категории содержания веб-ресурсов

Категории содержания веб-ресурсов (далее также "категории") в приведенном ниже списке подобраны таким образом, чтобы максимально полно описать блоки информации, размещенные на веб-ресурсах, с учетом их функциональных и тематических особенностей. Порядок категорий в списке не отражает относительной важности или распространенности категорий в сети Интернет. Названия категорий являются условными и используются лишь для целей программ и веб-сайтов "Лаборатории Касперского". Названия не обязательно соответствуют значению, которое им придает применимое законодательство. Один веб-ресурс может относиться к нескольким категориям одновременно.

Для взрослых

В общем определении категория включает в себя веб-ресурсы, относящиеся к сексуальной стороне человеческих отношений, философий, секс магазинов и т.д. Это может быть содержимое в любом формате и виде.

Алкоголь, табак, наркотики и психотропы

В общем определении категория включает в себя веб ресурсы, на которых есть упоминание алкоголя, наркотиков, табака в любых видах, в том числе рекламные, исторические, медицинские и обучающие ресурсы. А также веб ресурсы, где описаны или продаются приспособления для употребления указанных веществ.

Насилие

Данная категория включает веб-ресурсы, содержащие фото-, видео- и текстовые материалы, описывающие акты физического или психического насилия над людьми, а также жестокого отношения к животным как цель существования этого контента.

Произведения искусства могут быть исключениями в этой категории.

Нецензурная лексика

Категория включает веб-ресурсы, на которых обнаружены элементы нецензурной брани.

В данную категорию так же попадают веб-ресурсы с лингвистическими и филологическими материалами, содержащими нецензурную лексику в качестве предмета рассмотрения.

Оружие, взрывчатые вещества, пиротехника

Данная категория включает веб-ресурсы, содержащие информацию об оружии, взрывчатых веществах и пиротехнической продукции.

Под "оружием" понимаются устройства, предметы и средства, конструктивно предназначенные для нанесения вреда жизни и здоровью людей и животных и / или выведения из строя техники и сооружений.

Поиск работы

Данная категория включает веб-ресурсы, предназначенные для установления контактов между работодателем и соискателем работы. К ним в частности относятся:

- Веб-сайты кадровых агентств (агентств по трудоустройству и/или агентств по подбору персонала).
- Веб-страницы работодателей, содержащие описание имеющихся вакансий и их преимуществ.
- Независимые порталы, содержащие предложения трудоустройства от работодателей и кадровых агентств.
- Социальные сети профессионального характера, которые в том числе позволяют размещать/находить данные о специалистах, которые не находятся в активном поиске работы.

Средства анонимного доступа

Данная категория включает веб-ресурсы, выступающие в роли посредника для загрузки контента прочих веб-ресурсов с помощью специальных веб-приложений для:

- обхода ограничений администратора локальной сети на доступ к веб-адресам или IP-адресам;
- анонимного доступа к веб-ресурсам, в том числе к веб-ресурсам, которые преднамеренно не принимают HTTP-запросы с определённых IP-адресов или их групп (например, по стране происхождения).

Программное обеспечение, аудио, видео

В общем определении категория включает в себя веб-ресурсы, предоставляющие возможность скачивания соответствующих файлов.

- **Торренты**
Торрент трекеры и веб ресурсы, помогающие организовать их работу.
- **Файловые обменники**
Веб-ресурсы, предоставляющие возможность обмена файлами.
- **Аудио, видео**
Веб-ресурсы, с которых можно загрузить или просмотреть/прослушать аудио или видео файлы.

Азартные игры, лотереи, тотализаторы

Категория охватывает веб-ресурсы, содержащие:

- Азартные игры, предусматривающие денежные взносы за участие.
- Тотализаторы, предусматривающие денежные ставки.
- Лотереи, предусматривающие приобретение лотерейных билетов/номеров.

Общение в сети

В общем определении категория включает в себя веб-ресурсы, позволяющие тем или иным пользователям (зарегистрированным или нет) отправлять персональные сообщения другим пользователям. Существует ряд веб-ресурсов рассчитанных на общение.

- **Веб-почта**
Веб-почта - исключительно страницы авторизации в почтовом сервисе и страницы почтового ящика, содержащего почтовые сообщения и сопутствующие данные (например, личные контакты). Для остальных веб-страниц интернет-провайдера, предлагающего почтовый сервис, данная категория не назначается.

- **Социальные сети**

Социальные сети – веб-сайты, предназначенные для построения, отражения и организации контактов между людьми, организациями, государством, требующие в качестве условия участия регистрацию учётной записи пользователя.

- **Чаты, форумы**

В данную категорию следует относить веб-чаты, а также веб-ресурсы, предназначенные для распространения и поддержки приложений для мгновенного обмена сообщениями, предоставляющих возможность коммуникации в реальном времени. А также форумы – специальные веб сервисы для публичного обсуждения различных тем с сохранением переписки.

- **Блоги**

Блоги – веб-ресурсы, предназначенные для публичного обсуждения различных тем с помощью специальных веб-приложений, включая блог-платформы (веб-сайты, предоставляющие платные или бесплатные услуги по созданию и обслуживанию блогов).

- **Сайты знакомств**

Веб ресурсы знакомств, которые помогают организовать знакомства между людьми, в том числе без сексуального подтекста.

Интернет-магазины, банки, платежные системы

В общем определении категория включает в себя веб-ресурсы, предназначенные для проведения любых операций с безналичными денежными средствами в режиме онлайн с помощью специальных веб-приложений. А также веб ресурсы, помогающие снять, сдать, купить или продать недвижимость.

- **Интернет-магазины**

Интернет-магазины и интернет-аукционы, предназначенные для реализации любых товаров, работ или услуг физическим и/или юридическим лицам, в том числе как веб-сайты магазинов, осуществляющих реализацию исключительно в интернете, так и интернет-представительства обычных магазинов, характерной особенностью которых является возможность оплаты в режиме онлайн.

- **Банки**

Веб-ресурсы банков.

- **Платежные системы**

К данной категории относятся следующие веб страницы:

- Специальные веб-страницы банков, предусматривающие услуги интернет-банкинга, включающие безналичные (электронные) переводы между банковскими счетами, открытие банковских вкладов, конвертацию денежных средств, оплату услуг сторонних организаций и т.д.
- Веб-страницы электронных платёжных систем, предоставляющие доступ к персональной учётной записи пользователя.

- **Криптовалюты и майнинг**

Подкатегория включает веб-сайты, предоставляющие сервисы покупки и продажи криптовалют, сервисы информирования о криптовалютах и майнинге.

Компьютерные игры

Данная категория включает веб-ресурсы, посвящённые компьютерным играм разнообразных жанров. А также игровые сообщества и сервисы.

Религии, религиозные объединения

Данная категория включает веб-ресурсы, содержащие материалы об общественных течениях (движениях), объединениях (сообществах) и организациях, подразумевающих наличие религиозной идеологии и/или культа в любых проявлениях.

Новостные ресурсы

Новостные порталы на любые темы, в том числе социальные новости агрегаторы новостей, rss рассылки.

Баннеры

Категория включает веб-ресурсы, содержащие баннеры. Рекламная информация на баннерах может отвлекать пользователей от дел, а загрузка баннеров увеличивает объем трафика.

Региональные ограничения законодательства

- **Запрещено законодательством Российской Федерации**
- **Запрещено законодательством Бельгии**
- **Запрещено полицией Японии**

Веб-ресурсы, предоставляемые по соглашению с японской полицией, только для продуктов японского рынка.