

kaspersky

Kaspersky Industrial CyberSecurity for Linux Nodes

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 1.5.0.2430

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: 12.08.2024

© 2024 АО "Лаборатория Касперского"

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

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

Содержание

Об этом документе	15
Источники информации о приложении	16
О приложении.....	17
О режимах работы приложения.....	19
Требования.....	21
Указания по эксплуатации и требования к среде	21
Аппаратные требования.....	22
Программные требования.....	22
Поддерживаемые версии Kaspersky Security Center	25
Поддерживаемые версии Kaspersky Industrial CyberSecurity for Networks	26
Подготовка к установке приложения.....	27
Установка и первоначальная настройка приложения	28
Установка и первоначальная настройка Агента администрирования Kaspersky Security Center	29
Об установке Агента администрирования с помощью Kaspersky Security Center	29
Об установке Агента администрирования с помощью командной строки	30
Установка плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes.....	31
Установка веб-плагина Kaspersky Industrial CyberSecurity for Linux Nodes	32
Установка mmc-плагина Kaspersky Industrial CyberSecurity for Linux Nodes	33
Установка и первоначальная настройка приложения с помощью Kaspersky Security Center	34
Создание инсталляционного пакета в Web Console	35
Создание инсталляционного пакета в Консоли администрирования	40
Подготовка архива с базами приложения для создания инсталляционного пакета с интегрированными базами	42
Параметры конфигурационного файла autoinstall.ini	42
Подготовка приложения к работе с помощью Kaspersky Security Center	48
Активация приложения с помощью Kaspersky Security Center	49
Установка и первоначальная настройка приложения с помощью командной строки.....	52
Установка приложения с помощью командной строки.....	53
Первоначальная настройка приложения в интерактивном режиме	54
Первоначальная настройка приложения в автоматическом режиме	59
Параметры конфигурационного файла первоначальной настройки	60
Настройка разрешающих правил в системе SELinux.....	66
Запуск приложения в ОС Astra Linux в режиме замкнутой программной среды	68
Установка и удаление приложения на устройстве с ОС TeNIX WS.....	70
Удаление приложения	71
Об удалении приложения и Агента администрирования с помощью Kaspersky Security Center	72
Удаление приложения с помощью командной строки.....	72
Удаление Агента администрирования с помощью командной строки.....	73

Об удалении плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes	74
Процедура приемки	75
Безопасное состояние приложения	75
Проверка работоспособности. Тестовый файл EICAR	75
Разделение доступа к функциям приложения по пользовательским ролям	77
Просмотр списка пользователей и ролей.....	78
Назначение роли пользователю	79
Отзыв роли у пользователя	79
Лицензирование приложения	80
О Лицензионном соглашении	80
О лицензии	81
О лицензионном сертификате	81
О лицензионном ключе	82
Предоставление данных	84
Данные, предоставляемые при загрузке обновлений с серверов обновлений "Лаборатории Касперского"	84
Данные, передаваемые приложению Kaspersky Security Center	85
Данные, предоставляемые при переходе по ссылкам из интерфейса приложения	88
Данные, предоставляемые при использовании Kaspersky Security Network	88
Данные, передаваемые приложению Kaspersky Industrial CyberSecurity for Networks.....	89
Данные, предоставляемые при использовании Kaspersky Endpoint Detection and Response Optimum	92
Интерфейсы управления приложением	96
Концепция управления приложением	97
Управление приложением через Kaspersky Security Center	97
О плагинах управления Kaspersky Industrial CyberSecurity for Linux Nodes	99
О политиках Kaspersky Security Center	99
О задачах для Kaspersky Industrial CyberSecurity for Linux Nodes, созданных в Kaspersky Security Center	100
Вход и выход из Web Console.....	101
Управление политиками в Web Console	102
Управление политиками в Консоли администрирования	107
Управление задачами в Web Console.....	112
Управление задачами в Консоли администрирования	115
Управление приложением через командную строку	118
Включение автоматического дополнения команды kics-control (bash completion)	119
Управление задачами в командной строке	119
Вывод параметров задачи в командной строке.....	129
Изменение параметров задачи в командной строке	129
Настройка расписания задачи в командной строке	135
Управление общими параметрами приложения в командной строке	137
Использование фильтра для ограничения результатов запросов	140

Экспорт и импорт параметров приложения	142
Запуск и остановка приложения	144
Запуск и остановка приложения с помощью Web Console	144
Запуск и остановка приложения с помощью Консоли администрирования	145
Запуск и остановка приложения с помощью командной строки	145
Просмотр состояния защиты устройства и параметров приложения	147
Просмотр состояния защиты устройства в Web Console	148
Просмотр состояния защиты устройства в Консоли администрирования	149
Просмотр информации о работе приложения в Web Console	149
Просмотр информации о работе приложения в Консоли администрирования	150
Просмотр информации о работе приложения в командной строке	152
Активация приложения и управление лицензионными ключами	154
Просмотр информации о лицензии и ключе в командной строке	155
Управление лицензионными ключами в командной строке	157
Обновление баз и модулей приложения	158
Об обновлении баз и модулей	159
Об источниках и схемах обновления	160
Обновление баз и модулей приложения в Web Console	161
Обновление баз и модулей приложения в Консоли администрирования	163
Обновление баз и модулей приложения в командной строке	166
Обновление с помощью Kaspersky Update Utility	169
Откат обновления баз и модулей приложения	170
Защита от файловых угроз	172
Настройка защиты от файловых угроз в Web Console	173
Окно Области защиты	178
Окно добавления области защиты	178
Исключения Защиты от файловых угроз	182
Настройка защиты от файловых угроз в Консоли администрирования	190
Окно Области проверки	191
Окно <Новая область проверки>	192
Окно Параметры проверки	196
Окно Действие при обнаружении угрозы	200
Исключения Защиты от файловых угроз	201
Настройка защиты от файловых угроз в командной строке	210
Параметры задачи Защита от файловых угроз	210
Оптимизация проверки сетевых директорий	222
Особенности проверки символических и жестких ссылок	223
Поиск вредоносного ПО	225
Поиск вредоносного ПО в Web Console	226
Окно добавления области проверки	230

Раздел Области проверки	233
Окно Области проверки	234
Раздел Области исключения	234
Окно Области исключения	235
Окно добавления области исключения	235
Окно Исключения по маске	238
Окно Исключения по названию угрозы	238
Поиск вредоносного ПО в Консоли администрирования	238
Окно Области проверки	239
Окно <Новая область проверки>	240
Окно Параметры области проверки	243
Окно Области проверки	244
Окно Параметры проверки	245
Окно Действие при обнаружении угрозы	249
Раздел Исключения	249
Окно Области исключения	250
Окно <Новая область исключения>	250
Окно Исключения по маске	254
Окно Исключения по названию угрозы	254
Поиск вредоносного ПО в командной строке	254
Параметры предустановленной задачи Поиск вредоносного ПО	255
Выборочная проверка файлов и директорий	265
Проверка важных областей	274
Проверка важных областей в Web Console	274
Окно добавления области проверки	278
Раздел Области проверки	282
Окно Области проверки	282
Раздел Области исключения	282
Окно Области исключения	283
Окно добавления области исключения	283
Окно Исключения по маске	287
Окно Исключения по названию угрозы	287
Проверка важных областей в Консоли администрирования	287
Окно Области проверки	288
Окно <Новая область проверки>	289
Окно Параметры области проверки	293
Окно Области проверки	295
Окно Параметры проверки	295
Окно Действие при обнаружении угрозы	299
Раздел Исключения	299

Окно Области исключения	300
Окно <Новая область исключения>	300
Окно Исключения по маске	304
Окно Исключения по названию угрозы	304
Проверка важных областей в командной строке	304
Проверка съемных дисков	314
Настройка проверки съемных дисков в Web Console.....	314
Настройка проверки съемных дисков в Консоли администрирования	316
Настройка проверки съемных дисков в командной строке	318
Проверка контейнеров.....	322
Мониторинг контейнеров.....	322
Настройка мониторинга контейнеров в Web Console.....	323
Настройка мониторинга контейнеров в Консоли администрирования	325
Настройка мониторинга контейнеров в командной строке	326
Проверка контейнеров и образов по требованию	328
Проверка контейнеров в Web Console.....	329
Проверка контейнеров в Консоли администрирования	334
Проверка контейнеров в командной строке	342
Управление сетевым экраном	356
О сетевых пакетных правилах.....	357
О динамических правилах	358
О предустановленных именах сетевых зон	358
Управление сетевым экраном в Web Console	359
Окно Сетевые пакетные правила.....	359
Окно Сетевое пакетное правило	360
Окно Доступные сети.....	363
Окно Сетевое соединение	364
Управление сетевым экраном в Консоли администрирования	364
Окно Сетевые пакетные правила.....	365
Окно Добавление сетевого пакетного правила	366
Окно Доступные сети.....	369
Окно Сетевое соединение	370
Управление сетевым экраном в командной строке	370
Настройка списка сетевых пакетных правил в командной строке	376
Настройка сетевых зон в командной строке	377
Защита от веб-угроз.....	378
Настройка защиты от веб-угроз в Web Console	379
Окно Веб-адрес.....	381
Настройка защиты от веб-угроз в Консоли администрирования	381
Окно Доверенные веб-адреса	381

Окно Веб-адрес.....	382
Окно Параметры проверки	382
Настройка защиты от веб-угроз в командной строке	383
Проверка защищенных соединений.....	388
Настройка проверки защищенных соединений в Web Console	388
Окно Доверенные корневые сертификаты	390
Окно добавления доверенного сертификата	390
Окно Доверенные домены	390
Окно Контролируемые порты	390
Настройка проверки защищенных соединений в Консоли администрирования	391
Окно Доверенные домены	392
Окно Доверенные корневые сертификаты	393
Окно Добавление сертификата	393
Окно Контролируемые порты	394
Настройка проверки защищенных соединений в командной строке	394
Просмотр и изменение параметров проверки защищенных соединений	395
Просмотр исключений из проверки защищенных соединений.....	396
Управление списком доверенных сертификатов.....	397
Защита от сетевых угроз	398
Настройка защиты от сетевых угроз в Web Console	399
Окно IP-адрес	399
Настройка защиты от сетевых угроз в Консоли администрирования	400
Окно Исключения.....	400
Окно IP-адрес	401
Настройка защиты от сетевых угроз в командной строке.....	401
Защита от удаленного вредоносного шифрования	404
Настройка защиты от шифрования в Web Console	405
Окно Области защиты	406
Окно добавления области защиты.....	407
Окно Области исключения	410
Окно добавления области исключения	410
Окно Исключения по маске	414
Настройка защиты от шифрования в Консоли администрирования.....	414
Окно Области проверки	415
Окно <Новая область проверки>.....	415
Окно Параметры защиты	419
Окно Области исключения	419
Окно <Новая область исключения>	419
Окно Исключения по маске	423
Настройка защиты от шифрования в командной строке	423

Управление заблокированными устройствами	429
Контроль приложений.....	431
О правилах контроля приложений	432
Настройка контроля приложений в Web Console.....	433
Окно Правила Контроля приложений	434
Окно Правило Контроля приложений	435
Окно Категории приложений.....	436
Окно Выбор пользователя или группы	436
Настройка контроля приложений в Консоли администрирования	436
Окно Правила Контроля приложений	437
Окно Добавление правила	438
Окно Категории приложений.....	439
Окно Пользователь или группа	439
Экспорт и импорт параметров и категорий через Kaspersky Security Center	439
Настройка контроля приложений в командной строке	440
Параметры задачи Контроль приложений	441
Создание и изменение списка категорий	446
Просмотр списка созданных категорий	447
Настройка списка правил контроля приложений.....	448
Инвентаризация	450
Инвентаризация в Web Console	450
Окно добавления области проверки	451
Раздел Области исключения.....	452
Окно Области исключения.....	452
Окно добавления области исключения	453
Инвентаризация в Консоли администрирования	454
Окно Области проверки	455
Окно <Новая область проверки>.....	456
Раздел Исключения.....	457
Окно Области исключения.....	457
Окно <Новая область исключения>	457
Инвентаризация в командной строке.....	458
Параметры задачи Инвентаризация.....	459
Просмотр списка обнаруженных приложений.....	462
Контроль устройств.....	464
Настройка контроля устройств в Web Console	466
Окно Доверенные устройства.....	466
Окно Доверенное устройство (Идентификатор устройства)	467
Окно Доверенное устройство (Список обнаруженных устройств)	467
Окно Типы устройств.....	468

Окно Параметры доступа к устройствам	469
Окно Правило доступа к устройствам	469
Окно Выбор пользователя или группы	470
Окно Расписания	470
Окно Расписание доступа	471
Окно Шины подключения	471
Настройка контроля устройств в Консоли администрирования	471
Окно Доверенные устройства	472
Окно Доверенное устройство	473
Окно Устройства на клиентских устройствах	473
Окно Тип устройства	474
Окно Настройка правила доступа к устройствам	474
Окно Пользователь или группа	475
Окно Расписание доступа	475
Окно Шины подключения	476
Настройка Контроля устройств в командной строке	476
Параметры задачи Контроль устройств	477
Просмотр списка подключенных устройств в командной строке	488
Веб-Контроль	489
О правилах доступа к веб-ресурсам	490
Настройка Веб-Контроля в Web Console	491
Окно Правило Веб-Контроля	494
Окно Группы адресов	497
Окно Группа	497
Окно Выбор пользователя или группы	497
Окно Расписания	498
Окно Расписание доступа	498
Настройка Веб-Контроля в Консоли администрирования	498
Окно Правило Веб-Контроля	501
Окно Выбор категории содержания	504
Окно Выбор категории типов данных	504
Окно Выбор адресов	504
Окно Выбор групп адресов	505
Окно Добавление группы адресов	505
Окно Выбор пользователей	505
Окно Пользователь или группа	505
Окно Расписание доступа	505
Настройка шаблонов сообщений Веб-Контроля	506
Настройка Веб-Контроля в командной строке	508
Параметры задачи Веб-Контроль	508

Просмотр и изменение параметров Веб-Контроля	513
Правила формирования масок адресов веб-ресурсов	514
Контроль целостности системы	516
Контроль целостности системы в реальном времени	516
Настройка контроля целостности системы в Web Console	517
Настройка контроля целостности системы в Консоли администрирования	522
Настройка контроля целостности системы в командной строке	525
Проверка целостности системы	528
Проверка целостности системы в Web Console	529
Проверка целостности системы в Консоли администрирования	534
Проверка целостности системы в командной строке	539
Анализ поведения	544
Настройка анализа поведения в Web Console	544
Окно Исключения по процессам	545
Окно добавления области исключения по процессам	546
Настройка анализа поведения в Консоли администрирования	546
Окно Исключения по процессам	547
Окно Доверенный процесс	548
Настройка анализа поведения в командной строке	548
Использование Kaspersky Security Network	550
Настройка использования Kaspersky Security Network в Web Console	552
Положение о Kaspersky Security Network	553
Положение о Kaspersky Private Security Network	553
Настройка использования Kaspersky Security Network в Консоли администрирования	554
Параметры Kaspersky Security Network	555
Положение о Kaspersky Security Network	555
Положение о Kaspersky Private Security Network	556
Настройка использования Kaspersky Security Network в командной строке	556
Проверка подключения к Kaspersky Security Network с помощью командной строки	557
Дополнительные параметры работы приложения	559
Настройка прокси-сервера	560
Настройка параметров прокси-сервера в Web Console	560
Настройка параметров прокси-сервера в Консоли администрирования	563
Настройка параметров прокси-сервера в командной строке	566
Настройка глобальных исключений	566
Настройка глобальных исключений в Web Console	567
Настройка глобальных исключений в Консоли администрирования	570
Настройка глобальных исключений в командной строке	571
Исключение памяти процессов из проверки	572
Выбор режима перехвата файловых операций	574

Настройка обнаружения приложений, которые злоумышленники могут использовать для нанесения вреда	575
Включение мониторинга стабильности работы приложения.....	576
Настройка параметров запуска приложения.....	577
Ограничение на использование памяти и ресурсов процессора	578
Ограничение на использование резидентной памяти приложением.....	580
Ограничение на количество задач выборочной проверки	583
Настройка отправки информации в хранилище Kaspersky Security Center.....	583
Настройка разрешений на управление задачами	584
Резервное хранилище	586
Настройка параметров резервного хранилища в Web Console	587
Настройка параметров резервного хранилища в Консоли администрирования	587
Настройка параметров резервного хранилища в командной строке	588
Работа с объектами резервного хранилища в командной строке.....	589
Интеграция с Kaspersky Industrial CyberSecurity for Networks	592
Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в Web Console	594
Окно настройки параметров подключения к серверу интеграции	595
Окно подключения к серверу интеграции.....	598
Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в Консоли администрирования.....	598
Окно Серверы интеграции KICS for Networks	599
Окно Сервер интеграции KICS for Networks	600
Окно Параметры подключения к серверам интеграции.....	600
Окно Добавление сертификата	602
Окно Добавление сертификата	602
Окно Параметры передачи данных	602
Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в командной строке	603
Параметры задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks	604
Управление сертификатами для подключения к серверу интеграции	607
Интеграция с Kaspersky Endpoint Detection and Response Optimum	610
Об ответных действиях по командам	612
Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum.....	614
Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console	614
Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в командной строке	615
Просмотр статуса интеграции с Kaspersky Endpoint Detection and Response Optimum	616
Просмотр информации об обнаруженной угрозе и действиях по реагированию	617
Поиск индикаторов компрометации	617
Требования к IOC-файлам.....	619
Включение и выключение сетевой изоляции устройства	622
Включение и выключение сетевой изоляции устройства вручную в Web Console	623

Настройка автоматического выключения сетевой изоляции	623
Выключение сетевой изоляции устройства в командной строке	625
Настройка исключений из сетевой изоляции	626
Добавление и удаление исключений из сетевой изоляции в свойствах политики в Web Console ..	627
Добавление и удаление исключения из сетевой изоляции в свойствах устройства	627
Окно добавления исключения из сетевой изоляции	628
Окно Словарь сетевых профилей	628
Запуск процесса	629
Завершение процесса	631
Получение файла с устройства	634
Удаление файла с устройства	635
Просмотр событий и отчетов	638
Настройка записи событий в журнал операционной системы	641
Настройка параметров журнала событий приложения	642
Просмотр событий в Kaspersky Security Center	642
Просмотр событий в командной строке	642
Управление приложением через графический пользовательский интерфейс	645
Графический пользовательский интерфейс	646
Включение и выключение компонентов приложения	648
Запуск и остановка задач проверки	648
Запуск и остановка задачи обновления	649
Настройка использования Kaspersky Security Network	649
Просмотр отчетов	650
Просмотр объектов резервного хранилища	652
Управление лицензионными ключами	652
Добавление лицензионного ключа	653
Удаление лицензионного ключа	654
Просмотр информации о лицензии	654
Создание файла трассировки	655
Проверка целостности компонентов приложения	656
Обновление баз приложения в изолированном сегменте сети	658
Устранение уязвимостей и установка критических обновлений в приложении	659
Действия после сбоя или неустранимой ошибки в работе приложения	660
Обращение в Службу технической поддержки	661
Техническая поддержка через Kaspersky CompanyAccount	661
Получение информации для Службы технической поддержки	662
О файлах трассировки приложения	663
Настройка параметров трассировки приложения	664
О файлах трассировки плагинов управления приложением	666
О файлах дампа	667

Включение и выключение записи дампов	667
Об удаленной диагностике устройства с помощью Kaspersky Security Center	669
Приложения	671
Приложение 1. Оптимизация потребления ресурсов	671
Определение задачи, которая занимает ресурсы	672
Настройка задачи Защита от файловых угроз	674
Настройка задачи проверки по требованию	675
Установка ограничения на использование памяти приложением	675
Приложение 2. Команды управления Kaspersky Industrial CyberSecurity for Linux Nodes	676
Команды управления параметрами и задачами приложения	677
Команды статистики	688
Команды вывода событий	688
Команды управления событиями приложения	689
Команды управления лицензионными ключами	690
Команды управления сетевым экраном	691
Команды управления заблокированными устройствами	693
Команды управления Контролем устройств	694
Команды управления Контролем приложений	694
Команды управления Веб-Контролем	696
Команды управления резервным хранилищем	696
Команды управления пользователями и ролями	698
Команды управления параметрами интеграции с Kaspersky Industrial CyberSecurity for Networks	698
Команды управления параметрами интеграции с Kaspersky Endpoint Detection and Response Optimum	699
Приложение 3. Конфигурационные файлы и параметры приложения по умолчанию	700
Правила редактирования конфигурационных файлов задач приложения	701
Предустановленные конфигурационные файлы	702
Параметры задач командной строки по умолчанию	711
Общие параметры приложения	721
Общие параметры проверки контейнеров	728
Параметры проверки защищенных соединений	731
Параметры расписания задач	734
Приложение 4. Коды возврата командной строки	735
Приложение 5. Настройка совместной работы с SIEM-системами	735
Приложение 6. Значения параметров приложения в сертифицированной конфигурации	737
Соответствие терминов	744
Информация о стороннем коде	745
Уведомления о товарных знаках	746

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Industrial CyberSecurity for Linux Nodes" (далее также "Kaspersky Industrial CyberSecurity for Linux Nodes", "приложение").

Подготовительные процедуры изложены в разделах "Подготовка к установке приложения (см. стр. [27](#))", "Установка и первоначальная настройка приложения (см. стр. [28](#))" и "Процедура приемки (см. стр. [75](#))" и содержат процедуры безопасной установки и первоначальной настройки приложения, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования (см. стр. [21](#))" приведены минимально необходимые системные требования для безопасной установки приложения.

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

В документе также содержатся разделы с дополнительной информацией о приложении.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Industrial CyberSecurity for Linux Nodes, а также поддержка организаций, использующих Kaspersky Industrial CyberSecurity for Linux Nodes.

Руководство предназначено специалистам, которые знакомы с операционными системами и Linux® и владеют основными приемами работы в них, а также имеют опыт работы с системой удаленного централизованного управления приложениями "Лаборатории Касперского" Kaspersky Security Center.

Источники информации о приложении

Этот раздел содержит описание источников информации о приложении.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

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

Вы можете использовать следующие источники для самостоятельного поиска информации о приложении:

- страница приложения на веб-сайте "Лаборатории Касперского";
- страница приложения на веб-сайте Службы технической поддержки (База знаний);
- онлайн-справка;
- форум "Лаборатории Касперского".

Страница Kaspersky Industrial CyberSecurity for Linux Nodes на веб-сайте "Лаборатории Касперского"

На странице приложения (<https://www.kaspersky.ru/enterprise-security/industrial>) вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница приложения содержит ссылку на интернет-магазин. В нем вы можете приобрести приложение или продлить право пользования приложением.

Страница Kaspersky Industrial CyberSecurity for Linux Nodes в Базе знаний

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

На странице приложения в Базе знаний (<https://support.kaspersky.ru/kics-for-linux-nodes/1.5?page=kb>) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к приложению Kaspersky Industrial CyberSecurity for Linux Nodes, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Онлайн-справка

В онлайн-справке вы можете найти информацию о настройке и использовании приложения Kaspersky Industrial CyberSecurity for Linux Nodes, а также об окнах графического пользовательского интерфейса и окнах плагинов управления приложением: перечень и описание параметров.

Обсуждение приложений "Лаборатории Касперского" на Форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме (<https://forum.kaspersky.com>).

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

О приложении

Программное изделие Kaspersky Industrial CyberSecurity for Linux Nodes (далее также "Kaspersky Industrial CyberSecurity for Linux Nodes", "приложение") представляет собой средство антивирусной защиты и средство контроля подключения съемных машинных носителей информации, предназначенное для применения на серверах и автоматизированных рабочих местах информационных систем, а также на автономных автоматизированных рабочих местах на аппаратных платформах x86 и x64 под управлением ОС семейства Linux.

Приложение реализует 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. Также в программном изделии реализованы функции для обеспечения контроля использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации для конкретных пользователей информационной системы.

Основными угрозами, для противостояния которым используется Kaspersky Industrial CyberSecurity for Linux Nodes, 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) (KB);
- угрозы, связанные с установкой на узлы информационной системы внутренними и внешними нарушителями незарегистрированного (неучтенного) потенциально вредоносного программного обеспечения;
- угрозы, связанные с подключением к информационной системе внутренними и внешними нарушителями незарегистрированных (неучтенных) съемных машинных носителей информации с последующей несанкционированной записью (передачей) на эти носители защищаемой информации из информационной системы или загрузкой в информационную систему с этих съемных машинных носителей информации вредоносного программного обеспечения.

В приложении реализованы следующие функции безопасности:

- разграничение доступа к управлению ОО (SF.ACC);
- управление работой ОО (SF.MGT);
- управление параметрами ОО (SF.PAR);
- управление установкой обновлений (актуализации) БД ПКВ ОО (SF.UPD);
- аудит безопасности ОО (SF.AUD);
- выполнение проверок объектов воздействия (SF.SCN);
- обработка объектов воздействия (SF.RCT);
- сигнализация ОО (SF.ALR);
- контроль подключения съемных машинных носителей информации (SF.DC);
- контроль запуска приложений (SF.APP);
- контроль доступа к веб-ресурсам (SF.WAC);

- контроль целостности компонентов ОО (SF.ICT).

О режимах работы приложения

Для оптимизации объема ресурсов, потребляемых приложением, во время установки приложения вы можете выбрать режим работы, который приложение будет использовать сразу после установки. Доступны следующие режимы работы:

- *Защита выключена* (PROTECTION_MODE=Disabled). При запуске приложения после установки все компоненты приложения по умолчанию выключены. Запускаются только служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища.
- *Включена только защита от файловых угроз в информирующем режиме* (PROTECTION_MODE=OAS_Notify). При запуске приложения после установки автоматически запускается только компонент Защита от файловых угроз и служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. Компонент Защита от файловых угроз работает в информирующем режиме. *Информирующий режим* – это такой режим работы приложения, при котором в случае обнаружения угрозы компоненты и задачи приложения не пытаются лечить или удалять вредоносные объекты, запрещать доступ или блокировать активность приложений, а только информируют пользователя об обнаружении угрозы.
- *Включена только защита от файловых угроз* (PROTECTION_MODE=OAS_Block). При запуске приложения после установки автоматически запускается только компонент Защита от файловых угроз и служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. При обнаружении угрозы приложение выполняет действия, заданные в параметрах компонента Защита от файловых угроз.

Вы можете выбрать режим работы приложения следующими способами в зависимости от способа установки приложения:

- При установке с помощью Kaspersky Security Center Web Console или с помощью Консоли администрирования вы можете выбрать режим работы приложения в свойствах инсталляционного пакета (см. раздел "Создание инсталляционного пакета в Web Console" на стр. [35](#)) (этот способ доступен только в Web Console) или в конфигурационном файле autoinstall.ini (см. раздел "Параметры конфигурационного файла autoinstall.ini" на стр. [42](#)), который включен в инсталляционный пакет приложения.
- При установке с помощью командной строки вы можете выбрать режим работы приложения во время первоначальной настройки приложения в автоматическом режиме (см. раздел "Первоначальная настройка приложения в автоматическом режиме" на стр. [59](#)).

Если вы выполняете первоначальную настройку путем запуска скрипта первоначальной настройки (см. раздел "Первоначальная настройка приложения в интерактивном режиме" на стр. [54](#)), выбор режима работы приложения недоступен.

Если вы не выбрали режим работы приложения, по умолчанию приложение устанавливается в режиме *Защита выключена*.

После установки вам нужно включить нужные вам компоненты приложения и настроить нужные задачи. Если приложение используется в режиме *Защита выключена*, ваши устройства находятся под угрозой.

Вы можете включать компоненты, настраивать и запускать задачи с помощью Kaspersky Security Center (см. раздел "Управление приложением через Kaspersky Security Center" на стр. [97](#)) или командной строки (см. раздел "Управление приложением через командную строку" на стр. [118](#)).

Параметры компонентов и задач приложения по умолчанию настроены для работы в информирующем режиме:

- Компонент Защита от файловых угроз: **Первое действие – Пропускать** (FirstAction=Skip).
- Задачи проверки (Поиск вредоносного ПО, Проверка важных областей, выборочная проверка файлов и директорий): **Первое действие – Пропускать** (FirstAction=Skip).
- Компонент Мониторинг контейнеров: **Действие с контейнером при обнаружении угрозы – Пропустить контейнер** (OnAccessContainerScanAction=Skip).
- Задача Проверка контейнеров: **Первое действие – Пропускать** (FirstAction=Skip).
- Проверка съемных дисков: снят флажок **Блокировать доступ к съемному диску во время проверки** (BlockDuringScan=No).
- Компонент Защита от веб-угроз: **Действие при обнаружении угрозы – Информировать** (ActionOnDetect=Notify).
- Компонент Защита от сетевых угроз: **Действие при обнаружении угрозы – Информировать** (ActionOnDetect=Notify).
- Компонент Защита от шифрования: **Действие при обнаружении шифрования – Информировать** (ActionOnDetect=Notify).
- Компонент Контроль приложений: **Режим работы Контроля приложений – Информировать** (AppControlRulesAction=Notify).
- Компонент Контроль устройств: **Режим работы Контроля устройств – Информировать** (OperationMode=Notify).
- Компонент Веб-Контроль: **Правило по умолчанию – Разрешать все, что не указано в списке правил** (WebControlDefaultAction=Allow).
- Компонент Анализ поведения: **Действие при обнаружении вредоносной активности – Информировать** (TaskMode=Notify).
- Режим перехвата файловых операций: снят флажок **Блокировать доступ к файлам во время проверки** (FileBlockDuringScan=No).

Если при установке приложения вы выбрали режим работы *Включена только защита от файловых угроз*, значения некоторых параметров по умолчанию будут отличаться:

- Компонент Защита от файловых угроз: **Первое действие – Пропускать** (FirstAction=Recommended).
- Компонент Мониторинг контейнеров: **Действие с контейнером при обнаружении угрозы – Пропустить контейнер** (OnAccessContainerScanAction=StopContainerIfFailed).
- Режим перехвата файловых операций: установлен флажок **Блокировать доступ к файлам во время проверки** (FileBlockDuringScan=Yes).

После установки вы можете настраивать действия, которые будет выполнять приложение, с помощью Kaspersky Security Center (см. раздел "Управление приложением через Kaspersky Security Center" на стр. [97](#)) или командной строки (см. раздел "Управление приложением через командную строку" на стр. [118](#)).

Параметры настраиваются отдельно для каждого компонента и задачи, общего элемента управления для изменения режима работы приложения не предусмотрено.

Требования

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

В этом разделе

Указания по эксплуатации и требования к среде	21
Аппаратные требования.....	22
Программные требования.....	22
Поддерживаемые версии Kaspersky Security Center	25
Поддерживаемые версии Kaspersky Industrial CyberSecurity for Networks	26

Указания по эксплуатации и требования к среде

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

14. Управление атрибутами безопасности, связанными с доступом к функциям и данным приложения, должно предоставляться только уполномоченным ролям (администраторам приложения и информационной системы).
15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

Аппаратные требования

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes имеет следующие аппаратные требования:

- процессор Core™ 2 Duo 1.86 ГГц;
- раздел подкачки не менее 1 ГБ для всех компонентов;
- 1 ГБ оперативной памяти для 32-битных операционных систем или 2 ГБ оперативной памяти для 64-битных операционных систем;
- 4 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов;
- при использовании графического пользовательского интерфейса монитор должен обеспечивать отображение окон шириной 1000 пикселей и высотой 600 пикселей (если применяется масштабирование экрана, то эти размеры также масштабируются).

Для работы отдельных компонентов на устройствах с низкой производительностью требуется:

- 512 МБ оперативной памяти;
- раздел подкачки не менее 512 МБ для работы компонента Защита от файловых угроз и раздел подкачки не менее 2 ГБ для совместной работы компонентов Защита от файловых угроз и Контроль приложений или только для компонента Контроль приложений.

Программные требования

Для установки Kaspersky Industrial CyberSecurity for Linux Nodes на устройстве должна быть установлена одна из следующих операционных систем (полный перечень поддерживаемых операционных систем можно уточнить в технической поддержке):

- 32-битные операционные системы:
 - CentOS 6.5 и выше.
 - Debian GNU/Linux 10.1 и выше.

- Ubuntu 16.04 LTS.
- 64-битные операционные системы:
 - Astra Linux Common Edition 2.12.
 - Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6).
 - Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7).
 - CentOS 6.5 и выше.

На устройствах с операционной системой CentOS 6.5 не поддерживается установка графического пользовательского интерфейса.

- CentOS Stream 8 и выше.
- Debian GNU/Linux 10.1 и выше.
- Oracle® Linux 7.3 и выше
- Red Hat Enterprise Linux 7.2 и выше

На устройствах с операционной системой Red Hat Enterprise Linux 7.0 не поддерживается работа с файлами размером более 2 ГБ.

- SUSE Linux Enterprise Server 12.5 и выше.

На устройствах с операционной системой Ubuntu 10.04 LTS не поддерживается установка графического пользовательского интерфейса.

- Ubuntu 18.04 LTS.
- Ubuntu 20.04 LTS.
- Ubuntu 22.04 LTS.
- Ubuntu 24.04 LTS.
- РЕД ОС® 7.3.
- РЕД ОС 8.0.

Из-за ограничений технологии fanotify приложение не поддерживает работу со следующими файловыми системами: autofs, binfmt_misc, cgroup, configfs, debugfs, devpts, devtmpfs, fuse, fuse.gvfsd-fuse, gfs2, gvfs, hugetlbfs, mqueue, nfsd, proc, parsecfs, pipefs, pstore, usbfs, rpc_pipefs, securityfs, selinuxfs, sysfs, tracefs.

Поддерживаемые версии Kaspersky Industrial CyberSecurity for Networks

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes совместимо с решением Kaspersky Industrial CyberSecurity for Networks следующих версий:

- Kaspersky Industrial CyberSecurity for Networks 4.2.
- Kaspersky Industrial CyberSecurity for Networks 4.1.
- Kaspersky Industrial CyberSecurity for Networks 4.0.

Подробнее о решении Kaspersky Industrial CyberSecurity for Networks см. в справке Kaspersky Industrial CyberSecurity for Networks.

Поддерживаемые версии Kaspersky Security Center

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes совместимо с приложением Kaspersky Security Center следующих версий:

- Kaspersky Security Center 14.2 Windows. Поддерживается управление приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Консоль администрирования с помощью mmc-плагина управления (см. раздел "Установка mmc-плагина Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [33](#)) и через Kaspersky Security Center Web Console с помощью веб-плагина управления (см. раздел "Установка веб-плагина Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [32](#)).
- Kaspersky Security Center 15 Linux. Поддерживается управление приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Kaspersky Security Center Web Console с помощью веб-плагина управления (см. раздел "Установка веб-плагина Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [32](#)).
- Kaspersky Security Center 15.1 Linux. Поддерживается управление приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Kaspersky Security Center Web Console с помощью веб-плагина управления (см. раздел "Установка веб-плагина Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [32](#)).

Для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Kaspersky Security Center требуется Агент администрирования Kaspersky Security Center.

Агент администрирования Kaspersky Security Center не входит в комплект поставки Kaspersky Industrial CyberSecurity for Linux Nodes. Вы можете скачать его на странице загрузки приложений (https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint?utm_content=downloads) в разделе **Kaspersky Security Center**.

Подготовка к установке приложения

Перед началом установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes вам нужно выполнить следующие действия:

- Проверить соответствие вашего устройства аппаратным и программным требованиям приложения (см. раздел "Требования" на стр. [21](#)).
- Убедиться в том, что на вашем устройстве не установлено стороннее антивирусное программное обеспечение.
- Убедиться в том, что на вашем устройстве не установлено приложение Kaspersky Endpoint Agent для Linux. Если приложение Kaspersky Endpoint Agent для Linux установлено, во время установки отобразится сообщение о необходимости удалить его вручную.
- Убедиться в том, что на вашем устройстве установлен интерпретатор языка Perl версии 5.10 или выше.
- Убедиться в том, что в системе установлена утилита semanage. Если утилита не установлена, установите пакет polycoreutils-python или polycoreutils-python-utils в зависимости от типа менеджера пакетов.
- В зависимости от операционной системы на вашем устройстве установить один из следующих пакетов:
 - На устройстве с операционной системой SUSE Linux Enterprise Server 15 установить пакет insserv-compat.
 - На устройстве с операционной системой Red Hat Enterprise Linux 8 или РЕД ОС установить пакет perl-Getopt-Long.
 - На устройстве с операционной системой Red Hat Enterprise Linux или РЕД ОС установить пакет perl-File-Copy. Этот пакет требуется для работы скрипта первоначальной настройки приложения, но по умолчанию может отсутствовать.
- В операционных системах Astra Linux по умолчанию включен запрет трассировки ptrace (Disable ptrace capability), который может влиять на работу приложения Kaspersky Industrial CyberSecurity for Linux Nodes. Для корректной работы Kaspersky Industrial CyberSecurity for Linux Nodes рекомендуется отключить запрет трассировки ptrace при установке Astra Linux. Если Astra Linux уже установлена, инструкцию по включению и выключению этого режима см. на сайте Справочного центра Astra Linux (**Настройка механизмов защиты и блокировок, раздел Блокировка трассировки ptrace**).
- Для работы компонентов Управление сетевым экраном, Защита от веб-угроз (на стр. [378](#)) и Защита от сетевых угроз (на стр. [398](#)) требуется установить на вашем устройстве пакет утилит iptables.
- Для работы плагина управления Kaspersky Industrial CyberSecurity for Linux Nodes на устройстве, где установлен Сервер администрирования, требуется установить Microsoft® Visual C++® 2015 Redistributable Update 3 RC (см. <https://www.microsoft.com/ru-ru/download/details.aspx?id=52685>).
- Для запуска и корректной работы приложения требуется убедиться, что учетная запись root является владельцем следующих директорий и только владелец имеет право на запись в них: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

Установка и первоначальная настройка приложения

Перед началом установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes требуется выполнить подготовку к установке (см. раздел "Подготовка к установке приложения" на стр. [27](#)).

Сценарий ниже описывает установку и первоначальную настройку приложения Kaspersky Industrial CyberSecurity for Linux Nodes, а также установку и настройку Агента администрирования Kaspersky Security Center и установку плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes.

Процедура установки приложения состоит из следующих этапов:

1. Установка и первоначальная настройка Агента администрирования

Если вы планируете управлять приложением Kaspersky Industrial CyberSecurity for Linux Nodes с помощью Kaspersky Security Center, установите на защищаемом устройстве Агент администрирования Kaspersky Security Center и настройте его параметры (см. раздел "Установка и первоначальная настройка Агента администрирования Kaspersky Security Center" на стр. [29](#)).

a. Установка плагина управления Kaspersky Industrial CyberSecurity for Linux Nodes

Если вы планируете управлять приложением Kaspersky Industrial CyberSecurity for Linux Nodes с помощью Kaspersky Security Center, установите плагин управления Kaspersky Industrial CyberSecurity for Linux Nodes (см. раздел "Установка плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [31](#)). В зависимости от консоли управления Kaspersky Security Center используются следующие плагины управления:

- Веб-плагин управления Kaspersky Industrial CyberSecurity for Linux Nodes позволяет управлять работой приложения через Kaspersky Security Center Web Console. Веб-плагин устанавливается на устройстве с установленным приложением Kaspersky Security Center Web Console.
- Ммс-плагин управления Kaspersky Industrial CyberSecurity for Linux Nodes позволяет управлять работой приложения через Консоль администрирования Kaspersky Security Center. Ммс-плагин устанавливается на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

b. Установка пакетов приложения и графического пользовательского интерфейса

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes распространяется в пакетах форматов DEB и RPM. Предусмотрены отдельные пакеты для приложения и графического пользовательского интерфейса. Установите Kaspersky Industrial CyberSecurity for Linux Nodes и, если требуется, графический пользовательский интерфейс из пакетов нужного формата.

Вы можете выполнить установку одним из следующих способов:

- С помощью Kaspersky Security Center (см. раздел "Установка и первоначальная настройка приложения с помощью Kaspersky Security Center" на стр. [34](#)).
- С помощью командной строки (см. раздел "Установка и первоначальная настройка приложения с помощью командной строки" на стр. [52](#)).

c. Первоначальная настройка Kaspersky Industrial CyberSecurity for Linux Nodes

Выполнение первоначальной настройки требуется для включения защиты клиентского устройства.

Если вы установили приложение Kaspersky Industrial CyberSecurity for Linux Nodes с помощью Kaspersky Security Center, после завершения установки выполните подготовку приложения к работе (см. раздел "Подготовка приложения к работе с помощью Kaspersky Security Center" на стр. [48](#)).

Если вы установили приложение Kaspersky Industrial CyberSecurity for Linux Nodes с помощью командной строки, после завершения установки запустите скрипт первоначальной настройки (см. раздел "Первоначальная настройка приложения в интерактивном режиме" на стр. [54](#)) или выполните первоначальную настройку в автоматическом режиме (см. раздел "Первоначальная настройка приложения в автоматическом режиме" на стр. [59](#)).

В этом разделе

Установка и первоначальная настройка Агента администрирования Kaspersky Security Center	29
Установка плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes.....	31
Установка и первоначальная настройка приложения с помощью Kaspersky Security Center	34
Установка и первоначальная настройка приложения с помощью командной строки.....	52
Настройка разрешающих правил в системе SELinux.....	66
Запуск приложения в ОС Astra Linux в режиме замкнутой программной среды	68
Установка и удаление приложения на устройстве с ОС TeNiX WS.....	70

Установка и первоначальная настройка Агента администрирования Kaspersky Security Center

Установка Агента администрирования требуется для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes с помощью Kaspersky Security Center.

Агент администрирования обеспечивает связь клиентского устройства с Сервером администрирования Kaspersky Security Center. Поэтому его требуется установить на каждое клиентское устройство, которое будет подключено к системе удаленного централизованного управления Kaspersky Security Center.

Вы можете выполнить установку и первоначальную настройку Агента администрирования:

- удаленно с рабочего места администратора с помощью Kaspersky Security Center Web Console или Консоли администрирования (см. раздел "Об установке Агента администрирования с помощью Kaspersky Security Center" на стр. [29](#));
- с помощью командной строки (см. раздел "Об установке Агента администрирования с помощью командной строки" на стр. [30](#)).

В этом разделе

Об установке Агента администрирования с помощью Kaspersky Security Center	29
Об установке Агента администрирования с помощью командной строки	30

Об установке Агента администрирования с помощью Kaspersky Security Center

Перед началом удаленной установки Агента администрирования с помощью Kaspersky Security Center требуется подготовить устройство к удаленной установке (см. в справке Kaspersky Security Center, раздел "Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux").

Для удаленной установки используется инсталляционный пакет Агента администрирования. Файлы, необходимые для создания инсталляционного пакета Агента администрирования, входят в комплект поставки приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

► *Чтобы удаленно установить Агент администрирования:*

1. Создайте инсталляционный пакет Агента администрирования.

Во время создания инсталляционного пакета вам нужно принять условия Лицензионного соглашения для Агента администрирования. Вы можете ознакомиться с текстом Лицензионного соглашения, прочитав документ `license.txt` из комплекта поставки Агента администрирования.

В параметрах инсталляционного пакета укажите адрес Сервера администрирования, к которому должен подключаться Агент администрирования, и порт для подключения.

2. Выполните установку Агента администрирования с помощью задачи удаленной установки приложений.

Подробнее об установке Агента администрирования, см. в справке Kaspersky Security Center.

Об установке Агента администрирования с помощью командной строки

Вы можете установить Агент администрирования с помощью командной строки одним из следующих способов:

- Выполнить установку и первоначальную настройку в тихом режиме с файлом ответов. Файл ответов – это текстовый файл, который содержит пользовательский набор параметров установки и первоначальной настройки Агента администрирования.
- Выполнить установку Агента администрирования из пакета формата RPM или DEB в соответствии с типом менеджера пакетов, затем выполнить первоначальную настройку Агента администрирования с помощью скрипта в интерактивном режиме. Скрипт запускается по команде:

- для 32-битных операционных систем:

```
# /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
```

- для 64-битных операционных систем:

```
# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

Установку Агента администрирования требуется запускать с root-правами.

► *Чтобы выполнить установку Агента администрирования в тихом режиме:*

1. Создайте файл ответов. Добавьте в файл ответов список параметров установки и первоначальной настройки Агента администрирования в формате `<параметр>=<значение>`, каждый параметр в отдельной строке.

Для правильного использования файла ответов вам нужно включить в него следующие обязательные параметры:

- `KLNAGENT_SERVER` – полное доменное имя (FQDN) или IP-адрес Сервера администрирования.
- `KLNAGENT_AUTOINSTALL` – параметр определяет, включен ли тихий режим установки. Укажите значение 1.

- EULA_ACCEPTED – согласие с условиями Лицензионного соглашения для Агента администрирования. Вам нужно принять условия Лицензионного соглашения, чтобы продолжить процедуру установки. Ознакомьтесь с текстом Лицензионного соглашения, прочитав документ license.txt из комплекта поставки Агента администрирования. Если вы понимаете и принимаете условия Лицензионного соглашения, укажите значение 1.

Вы также можете добавить другие параметры установки и первоначальной настройки Агента администрирования. Полный список возможных параметров см. в справке Kaspersky Security Center (раздел "Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)").

2. Задайте значение переменной среды KLAUTOANSWERS, введя полное имя файла ответов (включая путь), например, следующим образом:

```
export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
```

3. Установите Агент администрирования:

- Чтобы установить Агент администрирования из пакета формата RPM на 32-битную операционную систему, выполните следующую команду:

```
# rpm -i klnagent-<номер сборки>.i386.rpm
```

- Чтобы установить Агент администрирования из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:

```
# rpm -i klnagent64-<номер сборки>.x86_64.rpm
```

- Чтобы установить Агент администрирования из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:

```
# apt-get install ./klnagent_<номер сборки>_i386.deb
```

- Чтобы установить Агент администрирования из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:

```
# apt-get install ./klnagent64_<номер сборки>_amd64.deb
```

Установка плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes

Для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Kaspersky Security Center используются следующие плагины управления Kaspersky Industrial CyberSecurity for Linux Nodes:

- веб-плагин управления Kaspersky Industrial CyberSecurity for Linux Nodes (см. раздел "Установка веб-плагины Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [32](#)) позволяет управлять работой приложения через Kaspersky Security Center Web Console;
- mmc-плагин управления Kaspersky Industrial CyberSecurity for Linux Nodes (см. раздел "Установка mmc-плагины Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [33](#)) позволяет управлять работой приложения через Консоль администрирования Kaspersky Security Center.

Вы можете одновременно установить плагины управления для разных версий приложения Kaspersky Industrial CyberSecurity for Linux Nodes. Таким образом вы сможете управлять приложением, используя политики, созданные с помощью разных версий плагина управления.

В этом разделе

Установка веб-плагина Kaspersky Industrial CyberSecurity for Linux Nodes	32
Установка ммс-плагина Kaspersky Industrial CyberSecurity for Linux Nodes	33

Установка веб-плагина Kaspersky Industrial CyberSecurity for Linux Nodes

Веб-плагин управления Kaspersky Industrial CyberSecurity for Linux Nodes требуется установить на клиентское устройство с установленным приложением Kaspersky Security Center Web Console. При этом функции веб-плагины доступны всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console в браузере.

Вы можете установить веб-плагин следующими способами:

- С помощью мастера первоначальной настройки Kaspersky Security Center Web Console.
Kaspersky Security Center Web Console автоматически предлагает запустить мастер первоначальной настройки при первом подключении Web Console к Серверу администрирования. Также вы можете запустить мастер первоначальной настройки в интерфейсе Kaspersky Security Center Web Console (**Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер первоначальной настройки**). Мастер первоначальной настройки также может проверить актуальность установленных веб-плагинов и загрузит необходимые обновления для них. Дополнительная информация о мастере первоначальной настройки Kaspersky Security Center Web Console приведена в справке Kaspersky Security Center.
- Вручную, используя дистрибутив из списка веб-плагинов "Лаборатории Касперского" или из стороннего источника.

► Чтобы установить веб-плагин Kaspersky Industrial CyberSecurity for Linux Nodes вручную:

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры** → **Веб-плагины**.
Откроется список установленных веб-плагинов.
2. Запустите установку веб-плагины Kaspersky Industrial CyberSecurity for Linux Nodes одним из следующих способов:
 - Установка из списка веб-плагинов "Лаборатории Касперского":
 - a. Нажмите на кнопку **Добавить**.
Откроется список всех доступных веб-плагинов "Лаборатории Касперского". Список обновляется автоматически после выпуска новых версий веб-плагинов.
 - b. Найдите в списке веб-плагин **Kaspersky Industrial CyberSecurity for Linux Nodes <номер версии>** и нажмите на его название.
 - c. В открывшемся окне с описанием веб-плагины нажмите на кнопку **Установить плагин**.
 - d. Дождитесь окончания установки и нажмите на кнопку **ОК** в информационном окне.
 - Установка веб-плагины из стороннего источника (архивы, необходимые для установки веб-плагинов, входят в комплект поставки):
 - a. Нажмите на кнопку **Добавить из файла**.

- b. В открывшемся окне укажите путь к ZIP-архиву с дистрибутивом веб-плагина и путь к файлу с подписью в формате TXT. Этот файл находится в архиве с веб-плагином.
- c. Нажмите на кнопку **Добавить**.
- d. Дождитесь окончания установки и нажмите на кнопку **ОК** в информационном окне.

Новый плагин отображается в списке установленных веб-плагинов (**Параметры** → **Веб-плагины**).

Если в свойствах Сервера администрирования Kaspersky Security Center вы выбрали язык, которого нет в дистрибутиве приложения Kaspersky Industrial CyberSecurity for Linux Nodes, то Лицензионное соглашение и весь интерфейс в Kaspersky Security Center Web Console будут отображаться на английском языке.

Установка mmc-плагина Kaspersky Industrial CyberSecurity for Linux Nodes

Mmc-плагин управления Kaspersky Industrial CyberSecurity for Linux Nodes требуется установить на том же клиентском устройстве, на котором установлена Консоль администрирования Kaspersky Security Center.

Перед установкой mmc-плагина управления Kaspersky Industrial CyberSecurity for Linux Nodes требуется убедиться, что установлены Kaspersky Security Center и Redist C++ 2015 (Microsoft Visual C++ 2015 Redistributable).

► Чтобы установить mmc-плагин,

на устройстве, где установлена Консоль администрирования Kaspersky Security Center, запустите исполняемый файл klcfginst.msi.

Файл входит в комплект поставки приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

После установки mmc-плагин управления отображается в списке установленных mmc-плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

► Чтобы посмотреть список установленных mmc-плагинов управления:

1. В дереве Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования <имя сервера>** и откройте окно свойств Сервера администрирования одним из следующих способов:
 - с помощью пункта **Свойства** контекстного меню узла **Сервер администрирования <имя сервера>**;
 - по ссылке **Свойства сервера администрирования**, расположенной в рабочей области узла **Сервер администрирования <имя сервера>** в блоке **Сервер администрирования**.
2. В списке слева в разделе **Дополнительно** выберите раздел **Информация об установленных плагинах управления программами**.

В правой части окна в списке установленных плагинов управления отображается mmc-плагин управления Kaspersky Industrial CyberSecurity for Linux Nodes: **Kaspersky Industrial CyberSecurity for Linux Nodes <номер версии>**.

Установка и первоначальная настройка приложения с помощью Kaspersky Security Center

Вы можете установить приложение Kaspersky Industrial CyberSecurity for Linux Nodes на клиентское устройство удаленно с рабочего места администратора с помощью Kaspersky Security Center Web Console или с помощью Консоли администрирования.

Для удаленной установки используется инсталляционный пакет приложения Kaspersky Industrial CyberSecurity for Linux Nodes. Инсталляционный пакет Kaspersky Industrial CyberSecurity for Linux Nodes является общим для всех поддерживаемых операционных систем и типов архитектуры процессора. Вы можете создать инсталляционный пакет с помощью Kaspersky Security Center Web Console (см. раздел "Создание инсталляционного пакета в Web Console" на стр. [35](#)) или с помощью Консоли администрирования (см. раздел "Создание инсталляционного пакета в Консоли администрирования" на стр. [40](#)).

Вы можете настроить параметры первоначальной настройки приложения (например, выбрать режим работы, который приложение использует сразу после установки (см. раздел "О режимах работы приложения" на стр. [19](#))):

- в свойствах инсталляционного пакета (см. раздел "Создание инсталляционного пакета в Web Console" на стр. [35](#)) (этот способ доступен только в Web Console);
- в конфигурационном файле autoinstall.ini (см. раздел "Параметры конфигурационного файла autoinstall.ini" на стр. [42](#)), который включен в инсталляционный пакет.

Вы можете развернуть приложение Kaspersky Industrial CyberSecurity for Linux Nodes на устройствах в сети организации несколькими способами.

Kaspersky Security Center Web Console поддерживает следующие основные способы развертывания:

- Установка приложения с помощью мастера развертывания защиты.
- Установка приложения с помощью задачи удаленной установки приложений.

Консоль администрирования Kaspersky Security Center поддерживает следующие основные способы развертывания:

- Установка приложения с помощью мастера удаленной установки.
- Установка приложения с помощью задачи удаленной установки приложений.

Описание процедур развертывания см. в справке Kaspersky Security Center.

При необходимости вы можете просмотреть журнал удаленной установки приложения с помощью удаленной диагностики клиентского устройства (см. раздел "Об удаленной диагностике устройства с помощью Kaspersky Security Center" на стр. [669](#)) Kaspersky Security Center.

После завершения установки приложения с помощью Kaspersky Security Center требуется выполнить подготовку приложения к работе (см. раздел "Подготовка приложения к работе с помощью Kaspersky Security Center" на стр. [48](#)).

Чтобы управлять с помощью Kaspersky Security Center работой приложения Kaspersky Industrial CyberSecurity for Linux Nodes, установленного на клиентских устройствах, вам нужно поместить эти устройства в группы администрирования. Перед началом установки приложения Kaspersky Industrial

CyberSecurity for Linux Nodes вы можете создать в Kaspersky Security Center группы администрирования, в которые вы хотите поместить устройства с установленным приложением, и настроить правила автоматического перемещения устройств в группы администрирования. Если правила перемещения устройств в группы администрирования не настроены, Kaspersky Security Center помещает все устройства с установленным Агентом администрирования, подключенным к Серверу администрирования, в список **Нераспределенные устройства**. В этом случае вам нужно вручную переместить устройства в группы администрирования (см. подробнее в справке Kaspersky Security Center).

В этом разделе

Создание инсталляционного пакета в Web Console	35
Создание инсталляционного пакета в Консоли администрирования	40
Подготовка архива с базами приложения для создания инсталляционного пакета с интегрированными базами.....	42
Параметры конфигурационного файла autoinstall.ini	42
Подготовка приложения к работе с помощью Kaspersky Security Center	48
Активация приложения с помощью Kaspersky Security Center	49

Создание инсталляционного пакета в Web Console

В Kaspersky Security Center Web Console вы можете создать инсталляционный пакет одним из следующих способов:

- Из архивного файла, который вы подготовили предварительно.
- Из дистрибутива, размещенного на серверах "Лаборатории Касперского".

► Чтобы подготовить архивный файл для создания инсталляционного пакета:

1. Распакуйте архив kics-1.5.0.<номер сборки>.zip в папку, доступную для Сервера администрирования Kaspersky Security Center. В ту же папку поместите файлы дистрибутива, соответствующие типу операционной системы, на которую вы хотите установить приложение, и типу менеджера пакетов на ней:
 - для установки Kaspersky Industrial CyberSecurity for Linux Nodes:
 - kics-1.5.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
 - kics_1.5.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
 - kics-1.5.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
 - kics_1.5.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
 - для установки графического интерфейса:
 - kics-gui-1.5.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
 - kics-gui_1.5.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
 - kics-gui-1.5.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
 - kics-gui_1.5.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)

Если вы не хотите устанавливать графический пользовательский интерфейс, не используйте эти файлы, тогда размер инсталляционного пакета будет меньше.

Обратите внимание, что если графический пользовательский интерфейс не будет использоваться, то вам нужно установить значение параметра `USE_GUI=No` в свойствах созданного инсталляционного пакета или в конфигурационном файле `autoinstall.ini`. В противном случае установка завершается с ошибкой.

Если вы хотите использовать создаваемый инсталляционный пакет для установки приложения на несколько типов операционных систем или менеджеров пакетов, поместите в папку файлы для всех необходимых типов операционных систем и менеджеров пакетов.

2. Если вы хотите настроить параметры первоначальной настройки приложения с помощью конфигурационного файла, откройте конфигурационный файл `autoinstall.ini` (см. раздел "Параметры конфигурационного файла `autoinstall.ini`" на стр. 42) и внесите необходимые изменения. Файл `autoinstall.ini` находится в папке, в которую вы распаковали архив `kics-1.5.0.<номер сборки>.zip`.

Вы также можете настроить параметры первоначальной настройки приложения в свойствах созданного инсталляционного пакета на закладке **Параметры**.

3. Если вы хотите использовать предварительно скачанные базы, поместите в папку подготовленные архивы с базами (см. раздел "Подготовка архива с базами приложения для создания инсталляционного пакета с интегрированными базами" на стр. 42) для всех необходимых типов операционных систем, откройте конфигурационный файл `autoinstall.ini` (см. раздел "Параметры конфигурационного файла `autoinstall.ini`" на стр. 42) и установите значение параметра `UPDATE_EXECUTE=no`. Файл `autoinstall.ini` находится в папке, в которую вы распаковали архив `kics-1.5.0.<номер сборки>.zip`.
4. Поместите все подготовленные файлы в архив формата ZIP, CAB, TAR или TAR.GZ с произвольным именем.

► *Чтобы создать инсталляционный пакет Kaspersky Industrial CyberSecurity for Linux Nodes в Kaspersky Security Center Web Console:*

1. В главном окне Web Console выберите один из следующих разделов:
 - **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
 - **Операции** → **Хранилища** → **Инсталляционные пакеты**.

Откроется список инсталляционных пакетов, доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

3. На первой странице мастера выберите способ создания инсталляционного пакета:
 - **Создать инсталляционный пакет из файла**. Инсталляционный пакет будет создан из архивного файла, который вы подготовили предварительно.
 - **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**. Инсталляционный пакет будет создан из дистрибутива, размещенного на серверах "Лаборатории Касперского".

4. В зависимости от выбранного способа создания пакета:

- Укажите имя пакета, нажмите на кнопку **Обзор** и укажите путь к архиву, который вы подготовили для создания инсталляционного пакета.
- Выберите дистрибутив приложения Kaspersky Industrial CyberSecurity for Linux Nodes. В окне справа ознакомьтесь с информацией о дистрибутиве и нажмите на кнопку **Загрузить и создать инсталляционный пакет**. Запустится процесс создания инсталляционного пакета.

5. Во время создания инсталляционного пакета требуется принять условия Лицензионного соглашения и Политики конфиденциальности. По запросу мастера ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и с Политикой конфиденциальности, которая описывает обработку и передачу данных. Для продолжения создания инсталляционного пакета требуется подтвердить, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности.

Инсталляционный пакет будет создан и добавлен в список инсталляционных пакетов. С помощью инсталляционного пакета вы можете установить приложение на устройства сети организации или обновить версию приложения.

В свойствах инсталляционного пакета на закладке **Параметры** вы можете настроить параметры установки приложения (см. таблицу ниже).

Настройка инсталляционного пакета Kaspersky Industrial CyberSecurity for Linux Nodes в версии Kaspersky Security Center Web Console ниже 14.2 не поддерживается. Для настройки параметров используйте конфигурационный файл autoinstall.ini (см. раздел "Параметры конфигурационного файла autoinstall.ini" на стр. 42).

Таблица 1. Параметры инсталляционного пакета

Раздел	Описание
Указать языковой стандарт	Установите флажок, чтобы указать языковой стандарт, используемый при работе приложения. Языковой стандарт в формате, определенном в RFC 3066. Если этот параметр не указан, используется языковой стандарт по умолчанию.
Активировать приложение	Установите флажок, чтобы активировать приложение. Вы также можете активировать приложение после установки (см. раздел "Активация приложения с помощью Kaspersky Security Center" на стр. 49).
Выберите источник обновлений	Укажите источник обновлений: - Серверы обновлений "Лаборатории Касперского". - Kaspersky Security Center. - Другие источники в локальной или глобальной сети.
Запустить задачу обновления баз после установки	Установите флажок, чтобы запустить задачу обновления после установки приложения.
Режим защиты	Выберите режим работы приложения (см. раздел "О режимах работы приложения" на стр. 19): Выключить компоненты защиты и задачи проверки при установке – при запуске приложения после установки все компоненты приложения по умолчанию выключены. Запускаются только служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. Это значение установлено по умолчанию. Только Защита от файловых угроз в информирующем режиме – при запуске приложения после установки автоматически запускается только компонент Защита от файловых угроз и служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. Компонент Защита от файловых угроз работает в информирующем режиме. <i>Информирующий режим</i> – это такой режим работы приложения, при котором в случае обнаружения угрозы компоненты и задачи приложения не пытаются лечить или удалять вредоносные объекты, запрещать доступ или блокировать активность приложений, а только информируют пользователя об обнаружении угрозы. Только Защита от файловых угроз – при запуске приложения после установки автоматически запускается только компонент Защита от файловых угроз и служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. При обнаружении угрозы приложение выполняет действия, заданные в параметрах компонента Защита от файловых угроз.
Указать параметры прокси-сервера	Установите флажок, чтобы указать адрес прокси-сервера, используемого для подключения к интернету.
Установить исходный код ядра	Установите флажок, чтобы автоматически начать компиляцию модулей ядра.

Раздел	Описание
Использовать графический пользовательский интерфейс	Установите флажок, чтобы включить использование графического пользовательского интерфейса.
Указать пользователя с ролью Администратор (admin)	Установите флажок, чтобы указать пользователя, которому назначается роль администратора (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. 77) (admin).
Выполнить автоматическую настройку SELinux	Установите флажок, чтобы выполнить автоматическую настройку SELinux для работы с Kaspersky Industrial CyberSecurity for Linux Nodes.
Удалить пользователей из привилегированных групп	Установите флажок, чтобы перед установкой приложения удалить пользователей из привилегированных групп kicsadmin и kicsaudit. Если флажок установлен и группа nogroup отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную.

Создание инсталляционного пакета в Консоли администрирования

Перед тем, как создать инсталляционный пакет приложения Kaspersky Industrial CyberSecurity for Linux Nodes, вам нужно подготовить файлы, которые будут включены в пакет.

► Чтобы подготовить файлы для создания инсталляционного пакета:

1. Распакуйте архив kics-1.5.0.<номер сборки>.zip в папку, доступную для Сервера администрирования Kaspersky Security Center. В ту же папку поместите файлы дистрибутива, соответствующие типу операционной системы, на которую вы хотите установить приложение, и типу менеджера пакетов на ней:
 - для установки Kaspersky Industrial CyberSecurity for Linux Nodes:
 - kics-1.5.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
 - kics_1.5.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
 - kics-1.5.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
 - kics_1.5.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
 - для установки графического интерфейса:
 - kics-gui-1.5.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
 - kics-gui_1.5.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
 - kics-gui-1.5.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
 - kics-gui_1.5.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)

Если вы не хотите устанавливать графический пользовательский интерфейс, не помещайте в папку эти файлы, тогда размер инсталляционного пакета будет меньше.

Обратите внимание, что если графический пользовательский интерфейс не будет использоваться, то вам нужно установить значение параметра `USE_GUI=No` в свойствах созданного инсталляционного пакета или в конфигурационном файле `autoinstall.ini`. В противном случае установка завершается с ошибкой.

Если вы хотите использовать создаваемый инсталляционный пакет для установки приложения на несколько типов операционных систем или менеджеров пакетов, поместите в папку файлы для всех необходимых типов операционных систем и менеджеров пакетов.

2. Если вы хотите настроить параметры первоначальной настройки приложения, откройте конфигурационный файл `autoinstall.ini` (см. раздел "Параметры конфигурационного файла `autoinstall.ini`" на стр. 42) и внесите необходимые изменения. Файл `autoinstall.ini` находится в папке, в которую вы распаковали архив `kics.zip`.
3. Если вы хотите использовать предварительно скачанные базы, поместите в папку подготовленные архивы с базами (см. раздел "Подготовка архива с базами приложения для создания инсталляционного пакета с интегрированными базами" на стр. 42) для всех необходимых типов операционных систем, откройте конфигурационный файл `autoinstall.ini` (см. раздел "Параметры конфигурационного файла `autoinstall.ini`" на стр. 42) и установите значение параметра `UPDATE_EXECUTE=no`. Файл `autoinstall.ini` находится в папке, в которую вы распаковали архив `kics.zip`.

► *Чтобы создать инсталляционный пакет Kaspersky Industrial CyberSecurity for Linux Nodes в Консоли администрирования Kaspersky Security Center:*

1. В дереве консоли выберите **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
2. Нажмите на кнопку **Создать инсталляционный пакет**.
Запустится мастер создания инсталляционного пакета.
3. В открывшемся окне мастера нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
4. Введите имя нового инсталляционного пакета и перейдите к следующему шагу.
5. Выберите дистрибутив приложения Kaspersky Industrial CyberSecurity for Linux Nodes. Для этого откройте стандартное окно Windows® с помощью кнопки **Обзор** и укажите путь к файлу `kics.kud`. Файл находится в папке, в которую вы распаковали архив `kics-1.5.0.<номер сборки>.zip`.

В окне отобразится название приложения.

Перейдите к следующему шагу.

6. Ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и с Политикой конфиденциальности, которая описывает обработку и передачу данных.

Для продолжения создания инсталляционного пакета требуется подтвердить, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности. Для подтверждения установите оба флажка в открывшемся окне.

Перейдите к следующему шагу.

7. Мастер загружает файлы, необходимые для установки приложения, на Сервер администрирования Kaspersky Security Center. Дождитесь окончания загрузки.
8. Завершите работу мастера.

Созданный инсталляционный пакет размещается в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**. Вы можете использовать один и тот же инсталляционный пакет многократно.

Подготовка архива с базами приложения для создания инсталляционного пакета с интегрированными базами

В некоторых случаях может потребоваться создать пакет удаленной установки с предварительно скачанными базами приложения. Например, если вы устанавливаете приложение на устройство с операционной системой Astra Linux Special Edition или хотите установить приложение сразу с готовыми рабочими базами (чтобы дополнительно не обновлять базы позднее).

► *Чтобы создать инсталляционный пакет с интегрированными базами для установки приложения:*

1. Выполните установку и первоначальную настройку приложения Kaspersky Industrial CyberSecurity for Linux Nodes на устройстве с помощью командной строки (см. раздел "Установка и первоначальная настройка приложения с помощью командной строки" на стр. [52](#)) или с помощью Kaspersky Security Center (см. раздел "Установка и первоначальная настройка приложения с помощью Kaspersky Security Center" на стр. [34](#)).
2. Выполните обновление баз приложения. Вы можете обновить базы в ходе первоначальной настройки приложения или после установки, запустив задачу типа Update в командной строке или задачу *Обновление* в Консоли администрирования Kaspersky Security Center или в Kaspersky Security Center Web Console.
3. Скопируйте содержимое директории /var/opt/kaspersky/kics/private/updates/ в одну из следующих поддиректорий в зависимости от архитектуры операционной системы, для которой вы создаете инсталляционный пакет с интегрированными базами: /i386/ или /x86_64/.
4. Поместите директории с базами в архив kics-bases.tgz, сохраняя структуру вложенных директорий. Вы можете поместить в архив только одну поддиректорию с базами для нужной архитектуры операционной системы или все поддиректории с базами (/i386/ или /x86_64/) в один архив под разные архитектуры, если вы планируете создать инсталляционный пакет для установки на несколько операционных систем с разной архитектурой.
5. Созданный архив с базами приложения вы можете использовать при создании инсталляционного пакета в Консоли администрирования Kaspersky Security Center (см. раздел "Создание инсталляционного пакета в Консоли администрирования" на стр. [40](#)) или в Kaspersky Security Center Web Console (см. раздел "Создание инсталляционного пакета в Web Console" на стр. [35](#)).

Параметры конфигурационного файла autoinstall.ini

В конфигурационном файле autoinstall.ini вы можете задавать параметры, приведенные в таблице ниже.

Таблица 2. Параметры конфигурационного файла *autoinstall.ini*

Параметр	Описание	Значения
EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения.	yes (значение по умолчанию) – принять условия Лицензионного соглашения, чтобы продолжить процедуру установки приложения. no – не принимать условия Лицензионного соглашения. Установка приложения будет прервана.
PRIVACY_POLICY_AGREED	Обязательный параметр. Согласие с условиями Политики конфиденциальности.	yes (значение по умолчанию) – принять условия Политики конфиденциальности, чтобы продолжить процедуру установки приложения. no – не принимать условия Политики конфиденциальности. Установка приложения будет прервана.
USE_KSN	Обязательный параметр. Включение использования Kaspersky Security Network. Для включения использования KSN требуется принять условия Положения о Kaspersky Security Network.	yes – принять условия Положения о Kaspersky Security Network и включить использование KSN. no (значение по умолчанию) – не принимать условия Положения о Kaspersky Security Network. Если вы включили использование KSN, автоматически включается облачный режим работы приложения, при котором Kaspersky Industrial CyberSecurity for Linux Nodes использует облегченную версию баз вредоносного ПО.
GROUP_CLEAN	Обязательный параметр. Удаление пользователей из привилегированных групп kicsadmin и kicsaudit.	yes – удалять пользователей из привилегированных групп. Если указано значение yes и группа nogroup отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную. no – не удалять пользователей из привилегированных групп.

Параметр	Описание	Значения
LOCALE	Дополнительный параметр. Языковой стандарт, используемый для локализации событий приложения, отправляемых в Kaspersky Security Center.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр <code>LOCALE</code> не указан, устанавливается язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию <code>en_US.utf8</code> . Локализация графического интерфейса и командной строки приложения зависит от локализации, указанной в переменной окружения <code>LANG</code> . Если в переменной окружения <code>LANG</code> указана локализация, которую приложение Kaspersky Industrial CyberSecurity for Linux Nodes не поддерживает, то графический интерфейс и командная строка отображаются в английской локализации.
INSTALL_LICENSE	Код активации или файл ключа.	
UPDATER_SOURCE	Источник обновлений.	<code>SCServer</code> – использовать в качестве источника обновлений Сервер администрирования Kaspersky Security Center. <code>KLServers</code> – использовать в качестве источника обновлений серверы "Лаборатории Касперского". Это значение используется по умолчанию. Адрес источника обновлений.
PROXY_SERVER	Адрес прокси-сервера, используемого для подключения к интернету.	Адрес прокси-сервера.
UPDATE_EXECUTE	Запуск задачи обновления баз приложения во время процедуры настройки.	<code>yes</code> (значение по умолчанию) – запускать задачу обновления. <code>no</code> – не запускать задачу обновления.
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра.	<code>yes</code> (значение по умолчанию) – компилировать модуль ядра. <code>no</code> – не компилировать модуль ядра.

Параметр	Описание	Значения
USE_GUI	Использование графического пользовательского интерфейса.	yes – включить использование графического пользовательского интерфейса. no (значение по умолчанию) – выключить использование графического пользовательского интерфейса.
ADMIN_USER	Пользователь, которому назначается роль администратора (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. 77) (admin).	Нет
CONFIGURE_SELINUX	Автоматическая настройка SELinux для работы с приложением Kaspersky Industrial CyberSecurity for Linux Nodes.	yes (значение по умолчанию) – выполнить автоматическую настройку SELinux для работы с Kaspersky Industrial CyberSecurity for Linux Nodes. no – не выполнять автоматическую настройку SELinux для работы с Kaspersky Industrial CyberSecurity for Linux Nodes.

Параметр	Описание	Значения
PROTECTION_MODE	Режим работы (см. раздел "О режимах работы приложения" на стр. 19), который приложение использует сразу после установки.	Disabled – при запуске приложения после установки все компоненты приложения по умолчанию выключены. Запускаются только служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. OAS_Notify – при запуске приложения после установки автоматически запускается только компонент Защита от файловых угроз и служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. Компонент Защита от файловых угроз работает в информирующем режиме. Информирующий режим – это такой режим работы приложения, при котором в случае обнаружения угрозы компоненты и задачи приложения не пытаются лечить или удалять вредоносные объекты, запрещать доступ или блокировать активность приложений, а только информируют пользователя об обнаружении угрозы. OAS_Block – при запуске приложения после установки автоматически запускается только компонент Защита от файловых угроз и служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. При обнаружении угрозы приложение выполняет действия, заданные в параметрах компонента Защита от файловых угроз.

Параметр	Описание	Значения
DISABLE_FILEAV_ACTIONS	Выключение функций лечения и удаления файлов для компонентов приложения после его установки. Если функции лечения и удаления файлов выключены, в случае обнаружения угрозы приложение не пытается лечить или удалять файлы, в которых обнаружена угроза, а только информирует пользователя об обнаружении угрозы. После установки приложения вы можете включить функции лечения и удаления файлов с помощью параметра <code>DisableFileAvActions</code> в конфигурационном файле <code>kics.ini</code> (см. раздел "Предустановленные конфигурационные файлы" на стр. 702).	<code>yes</code> – выключить функции лечения и удаления файлов при запуске приложения после установки. <code>no</code> (значение по умолчанию) – не выключать функции лечения и удаления файлов при запуске приложения после установки.

Если вы хотите изменить параметры в конфигурационном файле `autoinstall.ini`, укажите значения параметров в формате `<имя параметра>=<значение параметра>` (приложение не обрабатывает пробелы между именем параметра и его значением).

Подготовка приложения к работе с помощью Kaspersky Security Center

После развертывания приложения Kaspersky Industrial CyberSecurity for Linux Nodes через Kaspersky Security Center вам нужно выполнить следующие действия:

- Активировать приложение. Вы можете создать и выполнить задачу активации через Kaspersky Security Center Web Console или через Консоль администрирования, а также распространить на устройства лицензионный ключ из хранилища ключей Kaspersky Security Center (см. раздел "Активация приложения с помощью Kaspersky Security Center" на стр. [49](#)).
- Обновить базы и модули приложения через Kaspersky Security Center Web Console или через Консоль администрирования. Вы можете использовать задачу *Обновление*, которая создана автоматически мастером первоначальной настройки Kaspersky Security Center после установки mms-плагины управления или веб-плагины управления Kaspersky Industrial CyberSecurity for Linux Nodes.

Kaspersky Industrial CyberSecurity for Linux Nodes обеспечивает защиту устройства только после обновления баз приложения.

- Настроить политику для централизованного управления работой приложения с помощью Kaspersky Security Center Web Console (см. раздел "Управление политиками в Web Console" на стр. [102](#)) или Консоли администрирования (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)). Вы можете использовать политику, которая создана автоматически мастером первоначальной настройки Kaspersky Security Center после установки mms-плагина управления или веб-плагина управления Kaspersky Industrial CyberSecurity for Linux Nodes.

В политике по умолчанию выключены все компоненты, кроме компонента Защита от файловых угроз, параметры настроены на работу в информирующем режиме (см. раздел "О режимах работы приложения" на стр. [19](#)).

Также вы можете настроить задачи управления приложением с помощью Web Console (см. раздел "Управление задачами в Web Console" на стр. [112](#)) или в Консоли администрирования (см. раздел "Управление задачами в Консоли администрирования" на стр. [115](#)).

Активация приложения с помощью Kaspersky Security Center

Активация – это процедура введения в действие лицензии (см. раздел "О лицензии" на стр. [81](#)), дающей право на использование полнофункциональной версии приложения в течение срока действия лицензии. Процедура активации приложения заключается в добавлении лицензионного ключа.

Если вы используете приложение по лицензии, которая не включает функциональность Kaspersky Endpoint Detection and Response Optimum (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response Optimum" на стр. [610](#)), для активации этой функциональности вам нужно добавить дополнительный лицензионный ключ Kaspersky Endpoint Detection and Response Optimum Add-on (далее также "ключ EDR Optimum").

Вы можете добавлять лицензионные ключи в приложение через Kaspersky Security Center следующими способами:

- С помощью задачи добавления ключа в приложение.
Этот способ позволяет добавить лицензионный ключ на конкретное устройство или устройства, входящие в группу администрирования. Вы можете создать и выполнить задачу добавления ключа через Kaspersky Security Center Web Console или через Консоль администрирования.
- Путем распространения на клиентские устройства лицензионного ключа, размещенного на Сервере администрирования Kaspersky Security Center.
Этот способ позволяет автоматически добавлять ключ на клиентские устройства, уже подключенные к Kaspersky Security Center, а также на новые клиентские устройства. Для использования этого способа требуется сначала добавить ключ в хранилище ключей на Сервере администрирования Kaspersky Security Center.
- Путем добавления ключа в инсталляционный пакет Kaspersky Industrial CyberSecurity for Linux Nodes.

Этот способ позволяет добавить ключ в свойствах инсталляционного пакета при разворачивании Kaspersky Industrial CyberSecurity for Linux Nodes. Приложение будет активировано автоматически после установки.

Для создания задачи добавления ключа в приложение, добавления ключа в хранилище ключей и распространения ключа на клиентские устройства вы можете использовать Kaspersky Security Center Web Console или Консоль администрирования Kaspersky Security Center.

Активация в Kaspersky Security Center Web Console

Перед созданием задачи добавления ключа в приложение или распространением ключа требуется добавить ключ в хранилище Сервера администрирования Kaspersky Security Center.

► *Чтобы добавить ключ в хранилище ключей Kaspersky Security Center с помощью Web Console:*

1. В главном окне Web Console выберите **Операции** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне выберите способ добавления ключа в хранилище:
 - **Ввести код активации**, если вы хотите добавить ключ с помощью кода активации.
 - **Добавить файл ключа**, если вы хотите добавить ключ с помощью файла ключа.
4. В зависимости от выбранного вами на предыдущем шаге способа добавления ключа, выполните одно из следующих действий:
 - Введите код активации и нажмите на кнопку **Отправить**.
 - Нажмите на кнопку **Выберите файл ключа** и в открывшемся окне выберите файл с расширением key.
5. Нажмите на кнопку **Заккрыть**.

Добавленный ключ отобразится в списке ключей.

► *Чтобы активировать приложение через Web Console с помощью задачи Добавление ключа:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.
Откроется список задач.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи.
3. Настройте параметры задачи:
 - a. В раскрывающемся списке **Приложение** выберите название приложения Kaspersky Industrial CyberSecurity for Linux Nodes.
 - b. В раскрывающемся списке **Тип задачи** выберите **Добавление ключа**.
 - c. В поле **Название задачи** введите короткое описание, например, **Активация Kaspersky Industrial CyberSecurity for Linux Nodes**.
 - d. В разделе **Выбор устройств, которым будет назначена задача** выберите область действия задачи. Нажмите на кнопку **Далее**.
4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

Откроется окно **Хранилище ключей Kaspersky Security Center**.

5. Если вы добавили ключ в хранилище ключей Kaspersky Security Center предварительно, выберите ключ в списке и нажмите на кнопку **Далее**.
6. Если нужный ключ в хранилище ключей отсутствует, нажмите на кнопку **Добавить ключ**.
 - a. В открывшемся окне выберите способ добавления ключа в хранилище:
 - **Ввести код активации**, если вы хотите добавить ключ с помощью кода активации.
 - **Добавить файл ключа**, если вы хотите добавить ключ с помощью файла ключа.
 - b. В зависимости от выбранного вами на предыдущем шаге способа добавления ключа, выполните одно из следующих действий:
 - Введите код активации и нажмите на кнопку **Отправить**.
 - Нажмите на кнопку **Выберите файл ключа** и в открывшемся окне выберите файл с расширением key.
 - c. Ознакомьтесь с информацией о ключе и нажмите на кнопку **Заккрыть**.
 - d. Добавленный ключ отобразится в списке ключей. Выберите его в списке и нажмите на кнопку **Далее**.
7. Ознакомьтесь с информацией о лицензии и нажмите на кнопку **Далее**.
8. Завершите работу мастера.

В списке задач отобразится новая задача.

9. Установите флажок напротив задачи. Нажмите на кнопку **Запустить**.

В свойствах задачи *Добавление ключа* вы можете добавить на устройство *резервный ключ*. Резервный ключ становится активным либо по истечении срока действия лицензии, связанной с активным ключом, либо при удалении активного ключа. Наличие резервного ключа позволяет избежать ограничения функциональности приложения в момент окончания срока действия лицензии.

Если вы добавляете резервный ключ, но активный ключ еще не добавлен в приложение, задача завершается с ошибкой.

► Чтобы активировать приложение через Web Console путем распространения на устройства ключа, размещенного на Сервере администрирования:

1. В главном окне Web Console выберите **Операции** → **Лицензии "Лаборатории Касперского"**.
2. Откройте свойства ключа по ссылке с названием приложения, для активации которого предназначен ключ.
3. На закладке **Общие** установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.
4. Нажмите на кнопку **Сохранить**.

Лицензионный ключ будет автоматически распространяться на клиентские устройства, для которых он подходит. При автоматическом распространении ключа в качестве активного или резервного учитывается лицензионное ограничение на количество устройств, заданное в свойствах ключа. Если лицензионное ограничение достигнуто, распространение ключа на устройства автоматически прекращается. Вы можете просмотреть количество устройств, на которые добавлен ключ, и другие данные в свойствах ключа на закладке **Устройства**.

Вы можете контролировать использование лицензии с помощью Kaspersky Security Center Web Console следующими способами:

- Просмотреть Отчет об использовании лицензионных ключей (**Мониторинг и отчеты** → **Отчеты**).
- Просмотреть статусы управляемых устройств (**Активы (Устройства)** → **Управляемые устройства**). Если приложение не активировано, то для устройства будет отображаться статус  и описание статуса **Защита выключена**.
- Просмотреть свойства ключа (**Операции** → **Лицензии "Лаборатории Касперского"**).

Установка и первоначальная настройка приложения с помощью командной строки

Вы можете выполнить следующие действия при установке приложения с помощью командной строки:

- Установить приложение с графическим пользовательским интерфейсом.
- Установить приложение без графического пользовательского интерфейса.
- Установить графический пользовательский интерфейс на устройстве, где установлено приложение.

Невозможно установить графический пользовательский интерфейс на устройство, на котором не установлено приложение.

Если версия менеджера пакетов apt ниже 1.1.X, требуется использовать для установки менеджер пакетов dpkg/rpm (в зависимости от операционной системы).

После завершения установки приложения требуется выполнить первоначальную настройку приложения в интерактивном режиме (см. раздел "Первоначальная настройка приложения в интерактивном режиме" на стр. [54](#)) или в автоматическом режиме (см. раздел "Первоначальная настройка приложения в автоматическом режиме" на стр. [59](#)).

При выполнении первоначальной настройки приложения в интерактивном режиме недоступен выбор режима работы, который приложение использует сразу после установки (см. раздел "О режимах работы приложения" на стр. [19](#)). Приложение устанавливается в режиме *Защита выключена*.

В этом разделе

Установка приложения с помощью командной строки	53
Первоначальная настройка приложения в интерактивном режиме	54
Первоначальная настройка приложения в автоматическом режиме	59
Параметры конфигурационного файла первоначальной настройки	60

Установка приложения с помощью командной строки

Установка приложения без графического пользовательского интерфейса

- Чтобы установить Kaspersky Industrial CyberSecurity for Linux Nodes из пакета формата RPM на 32-битную операционную систему, выполните следующую команду:

```
# rpm -i kics-1.5.0-<номер сборки>.i386.rpm
```

- Чтобы установить Kaspersky Industrial CyberSecurity for Linux Nodes из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:

```
# rpm -i kics-1.5.0-<номер сборки>.x86_64.rpm
```

- Чтобы установить Kaspersky Industrial CyberSecurity for Linux Nodes из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:

```
# apt-get install ./kics_1.5.0-<номер сборки>_i386.deb
```

- Чтобы установить Kaspersky Industrial CyberSecurity for Linux Nodes из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:

```
# apt-get install ./kics_1.5.0-<номер сборки>_amd64.deb
```

Установка графического пользовательского интерфейса

- Чтобы установить графический пользовательский интерфейс из пакета формата RPM на 32-битную операционную систему, выполните следующую команду:

```
# rpm -i kics-gui-1.5.0-<номер сборки>.i386.rpm
```

- Чтобы установить графический пользовательский интерфейс из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:

```
# rpm -i kics-gui-1.5.0-<номер сборки>.x86_64.rpm
```

- Чтобы установить графический пользовательский интерфейс из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:

```
# apt-get install ./kics-gui_1.5.0-<номер сборки>_i386.deb
```

- Чтобы установить графический пользовательский интерфейс из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:

```
# apt-get install ./kics-gui_1.5.0-<номер сборки>_amd64.deb
```

Первоначальная настройка приложения в интерактивном режиме

После установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes с помощью командной строки требуется выполнить первоначальную настройку приложения, запустив скрипт первоначальной настройки. Скрипт первоначальной настройки входит в комплект поставки приложения.

Выполнение первоначальной настройки после установки приложения с помощью командной строки требуется для включения защиты клиентского устройства.

- Чтобы запустить скрипт первоначальной настройки Kaspersky Industrial CyberSecurity for Linux Nodes, выполните следующую команду:

```
# /opt/kaspersky/kics/bin/kics-setup.pl
```

Скрипт первоначальной настройки требуется запускать с root-правами после завершения установки пакета Kaspersky Industrial CyberSecurity for Linux Nodes. Скрипт пошагово запрашивает значения параметров Kaspersky Industrial CyberSecurity for Linux Nodes. Завершение работы скрипта и освобождение консоли означает, что процесс первоначальной настройки приложения завершен.

- Чтобы проверить код возврата, выполните следующую команду:

```
echo $?
```

Если команда вернула код 0, первоначальная настройка приложения успешно завершена.

Kaspersky Industrial CyberSecurity for Linux Nodes обеспечивает защиту устройства только после обновления баз приложения.

В этом разделе

Выбор языкового стандарта	55
Просмотр Лицензионного соглашения и Политики конфиденциальности	55
Принятие Лицензионного соглашения	55
Принятие Политики конфиденциальности	55
Использование Kaspersky Security Network.....	56
Удаление пользователей из привилегированных групп	56
Назначение пользователю роли администратора.....	57
Определение типа перехватчика файловых операций.....	57
Включение автоматической настройки SELinux	57
Настройка источника обновлений	57
Настройка параметров прокси-сервера.....	58
Запуск обновления баз приложения	58
Включение автоматического обновления баз приложения	59
Активация приложения.....	59

Выбор языкового стандарта

На этом шаге приложение выводит список обозначений поддерживаемых языковых стандартов в формате, определенном в RFC 3066.

Вам нужно указать языковой стандарт в том формате, в котором он приведен в списке обозначений. Этот стандарт будет использоваться для локализации событий приложения, отправляемых в Kaspersky Security Center, а также для локализации текстов Лицензионного соглашения, Политики конфиденциальности и Положения о Kaspersky Security Network.

Локализация графического интерфейса и командной строки приложения зависит от локализации, указанной в переменной окружения `LANG`. Если в переменной окружения `LANG` указана локализация, которую приложение Kaspersky Industrial CyberSecurity for Linux Nodes не поддерживает, то графический интерфейс и командная строка отображаются в английской локализации.

Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге вам нужно ознакомиться с текстом Лицензионного соглашения, которое заключается между вами и "Лабораторией Касперского" и Политики конфиденциальности, которая описывает обработку и передачу данных.

Принятие Лицензионного соглашения

На этом шаге вам нужно принять или отклонить условия Лицензионного соглашения.

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы принимаете условия Лицензионного соглашения.
- `no` (или `n`), если вы не принимаете условия Лицензионного соглашения.

Если вы не согласны с условиями Лицензионного соглашения, процесс настройки приложения Kaspersky Industrial CyberSecurity for Linux Nodes прерывается.

Принятие Политики конфиденциальности

На этом шаге вам нужно принять или отклонить условия Политики конфиденциальности.

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы принимаете условия Политики конфиденциальности.
- `no` (или `n`), если вы не принимаете условия Политики конфиденциальности.

Если вы не согласны с условиями Политики конфиденциальности, процесс настройки приложения Kaspersky Industrial CyberSecurity for Linux Nodes прерывается.

Использование Kaspersky Security Network

В сертифицированной версии приложения допускается только использование KPSN. Использование KSN не допускается, так как приводит к выходу приложения из сертифицированного состояния. Рекомендуется использовать KPSN или отказаться от использования KSN.

На этом шаге вам нужно принять или отклонить условия использования Kaspersky Security Network. Файл `kns_license.<ID языка>` с текстом Положения о Kaspersky Security Network находится в директории `/opt/kaspersky/kics/doc/`.

Введите одно из следующих значений:

- `yes` (или `y`), если вы принимаете условия Положения о Kaspersky Security Network. Будет включен расширенный режим KSN.
- `no` (или `n`), если вы не принимаете условия Положения о Kaspersky Security Network.

Отказ от использования Kaspersky Security Network не прерывает процесс первоначальной настройки приложения Kaspersky Industrial CyberSecurity for Linux Nodes. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент.

Если вы включили использование Kaspersky Security Network, автоматически включается облачный режим работы приложения, при котором Kaspersky Industrial CyberSecurity for Linux Nodes использует облегченную версию баз вредоносного ПО.

Включение облачного режима приводит к выходу приложения из сертифицированного состояния.

Удаление пользователей из привилегированных групп

Этот шаг отображается, только если обнаружены пользователи в группе `kicsadmin` и/или в группе `kicsaudit`.

На этом шаге укажите, следует ли удалить пользователей из привилегированных групп `kicsadmin` и `kicsaudit`. Пользователи, включенные в группы `kicsadmin` и `kicsaudit`, получают привилегированный доступ к функциям приложения (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. [77](#)).

Введите `yes`, чтобы удалить всех обнаруженных пользователей из группы `kicsadmin` и/или `kicsaudit`. Пользователи, для которых группа `kicsadmin` или `kicsaudit` является первичной, будут перемещены в группу `nogroup`. Если группа `nogroup` отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную.

Введите `no`, если вы не хотите, чтобы приложение удаляло пользователей из привилегированных групп.

Назначение пользователю роли администратора

На этом шаге вы можете назначить пользователю роль (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. [77](#)) администратора (admin).

Введите имя пользователя, которому вы хотите назначить роль администратора.

Вы можете назначить пользователю роль (см. раздел "Назначение роли пользователю" на стр. [79](#)) администратора позже в любой момент.

Определение типа перехватчика файловых операций

На этом шаге определяется тип перехватчика файловых операций для используемой операционной системы. Для операционных систем, не поддерживающих технологию fanotify, будет запущена компиляция модуля ядра.

Если в процессе компиляции модуля ядра не обнаружены необходимые пакеты, Kaspersky Industrial CyberSecurity for Linux Nodes предлагает установить их. Если скачать пакеты не удалось, выводится сообщение об ошибке.

При наличии всех необходимых пакетов модуль ядра будет автоматически скомпилирован при запуске задачи Защита от файловых угроз.

Вы можете выполнить компиляцию модуля ядра позже, после завершения первоначальной настройки приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

Включение автоматической настройки SELinux

Этот шаг отображается, только если в вашей операционной системе установлена система SELinux.

На этом шаге вы можете включить автоматическую настройку системы SELinux для работы с приложением Kaspersky Industrial CyberSecurity for Linux Nodes.

Введите `yes`, чтобы включить автоматическую настройку системы SELinux. Если не удалось настроить систему SELinux автоматически, приложение выводит сообщение об ошибке и предлагает пользователю настроить систему SELinux вручную.

Введите `no`, если вы не хотите, чтобы приложение автоматически настроило систему SELinux.

По умолчанию приложение предлагает значение `yes`.

Если требуется, вы можете вручную настроить систему SELinux (см. раздел "Настройка разрешающих правил в системе SELinux" на стр. [66](#)) для работы с приложением позже, после завершения первоначальной настройки приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

Настройка источника обновлений

На этом шаге вам нужно указать источники обновлений баз и модулей приложения.

Введите одно из следующих значений:

- `KLServers` – приложение получает обновления с одного из серверов обновлений "Лаборатории Касперского".

- `SCServer` – приложение загружает обновления на защищаемое устройство с установленного в вашей организации Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновлений, если вы используете приложение Kaspersky Security Center для централизованного управления защитой устройств в вашей организации.
- `<веб-адрес>` – приложение загружает обновления из пользовательского источника. Вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.
- `<путь>` – приложение получает обновления из указанной директории.

Настройка параметров прокси-сервера

На этом шаге вам нужно указать параметры прокси-сервера, если вы используете прокси-сервер для доступа в интернет. Для загрузки баз приложения (см. раздел "Запуск обновления баз приложения" на стр. [58](#)) с серверов обновлений требуется подключение к интернету.

► Чтобы настроить параметры прокси-сервера, выполните одно из следующих действий:

- Если при подключении к интернету вы используете прокси-сервер, укажите адрес прокси-сервера в одном из следующих форматов:
 - `<IP-адрес прокси-сервера>:<номер порта>`, если для подключения к прокси-серверу не требуется аутентификация;
 - `<имя пользователя>:<пароль>@<IP-адрес прокси-сервера>:<номер порта>`, если для подключения к прокси-серверу требуется аутентификация.

Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.

- Если для подключения к интернету не используется прокси-сервер, введите значение `no`.

По умолчанию приложение предлагает значение `no`.

Вы можете настроить параметры прокси-сервера позже (см. раздел "Настройка прокси-сервера" на стр. [560](#)), без использования скрипта первоначальной настройки.

Запуск обновления баз приложения

На этом шаге вы можете запустить задачу обновления баз приложения на клиентском устройстве. Базы приложения содержат описания сигнатур угроз и методов борьбы с ними. Приложение использует эти записи при поиске и нейтрализации угроз. Вирусные аналитики "Лаборатории Касперского" регулярно добавляют записи о новых угрозах.

Если вы хотите отказаться от запуска обновления баз приложения, введите `no`.

Если вы хотите запустить задачу обновления баз на устройстве, введите `yes`.

По умолчанию приложение предлагает значение `yes`.

Если выбрано значение `yes`, приложение будет автоматически перезапущено после обновления баз.

Kaspersky Industrial CyberSecurity for Linux Nodes обеспечивает защиту устройства только после обновления баз приложения.

Вы можете запустить задачу обновления позже без использования скрипта первоначальной настройки.

Включение автоматического обновления баз приложения

На этом шаге вы можете включить автоматическое обновление баз приложения.

Введите `yes`, чтобы включить автоматическое обновление баз приложения. По умолчанию приложение проверяет наличие обновлений баз каждые 60 минут. При наличии обновлений приложение загружает обновленные базы.

Введите `no`, если вы не хотите, чтобы приложение автоматически обновляло базы.

Вы можете включить автоматическое обновление баз без использования скрипта первоначальной настройки, настроив расписание задачи обновления (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)).

Активация приложения

На этом шаге вы можете активировать приложение с помощью кода активации или файла ключа.

Чтобы активировать приложение с помощью кода активации, требуется ввести код активации.

Чтобы активировать приложение с помощью файла ключа, требуется указать полный путь к файлу ключа.

Если вы не указали код активации или файл ключа, приложение будет активировано с помощью пробного ключа на один месяц.

Вы можете активировать приложение позже (см. раздел "Активация приложения и управление лицензионными ключами" на стр. [154](#)) без использования скрипта первоначальной настройки.

Первоначальная настройка приложения в автоматическом режиме

Вы можете выполнить первоначальную настройку приложения в автоматическом режиме.

- Чтобы запустить первоначальную настройку приложения в автоматическом режиме, выполните следующую команду:

```
# /opt/kaspersky/kics/bin/kics-setup.pl --autoinstall=<конфигурационный файл первоначальной настройки>
```

где `<конфигурационный файл первоначальной настройки>` – путь к конфигурационному файлу, который содержит параметры первоначальной настройки. Вы можете создать этот файл или скопировать структуру для него из конфигурационного файла `autoinstall.ini` (см. раздел "Параметры конфигурационного файла `autoinstall.ini`" на стр. [42](#)), который используется для удаленной установки приложения с помощью Kaspersky Security Center.

Завершение работы скрипта `pe` (см. раздел "Установка и первоначальная настройка приложения с помощью Kaspersky Security Center" на стр. [34](#)) первоначальной настройки и освобождение консоли означает, что процесс первоначальной настройки приложения завершен.

► Чтобы проверить код возврата, выполните следующую команду:

```
echo $?
```

Если команда вернула код 0, первоначальная настройка приложения успешно завершена.

Kaspersky Industrial CyberSecurity for Linux Nodes обеспечивает защиту устройства только после обновления баз приложения.

Для корректного обновления модулей приложения после завершения работы скрипта может потребоваться перезапустить приложение. Проверьте состояние обновлений для приложения с помощью команды `kics-control --app-info`.

Параметры конфигурационного файла первоначальной настройки

В конфигурационном файле первоначальной настройки вы можете задавать параметры, приведенные в таблице ниже.

Таблица 3. Параметры конфигурационного файла первоначальной настройки

Параметр	Описание	Значения
EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения.	yes – принять условия Лицензионного соглашения, чтобы продолжить процедуру установки приложения. no – не принимать условия Лицензионного соглашения. Установка приложения будет прервана.
PRIVACY_POLICY_AGREED	Обязательный параметр. Согласие с условиями Политики конфиденциальности.	yes – принять условия Политики конфиденциальности, чтобы продолжить процедуру установки приложения. no – не принимать условия Политики конфиденциальности. Установка приложения будет прервана.
USE_KSN	Обязательный параметр. Включение использования Kaspersky Security Network. Для включения использования KSN требуется принять условия Положения о Kaspersky Security Network. В сертифицированной версии приложения допускается только использование KPSN. Использование KSN не допускается, так как приводит к выходу приложения из сертифицированного состояния.	yes – принять условия Положения о Kaspersky Security Network и включить использование KSN. no – не принимать условия Положения о Kaspersky Security Network. Если вы включили использование KSN, автоматически включается облачный режим работы приложения, при котором Kaspersky Industrial CyberSecurity for Linux Nodes использует облегченную версию баз вредоносного ПО. Включение облачного режима приводит к выходу приложения из сертифицированного состояния.

Параметр	Описание	Значения
GROUP_CLEAN	Обязательный параметр. Удаление пользователей из привилегированных групп kicsadmin и kicsaudit.	yes – удалять пользователей из привилегированных групп. Если указано значение yes и группа nogroup отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную. no – не удалять пользователей из привилегированных групп.
LOCALE	Дополнительный параметр. Языковой стандарт, используемый для локализации событий приложения, отправляемых в Kaspersky Security Center.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр LOCALE не указан, устанавливается язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию en_US.utf8. Локализация графического интерфейса и командной строки приложения зависит от локализации, указанной в переменной окружения LANG. Если в переменной окружения LANG указана локализация, которую приложение не поддерживает, то графический интерфейс и командная строка отображаются в английской локализации.
INSTALL_LICENSE	Код активации или файл ключа.	
UPDATER_SOURCE	Источник обновлений.	SCServer – использовать в качестве источника обновлений Сервер администрирования. KLServers – использовать в качестве источника обновлений серверы "Лаборатории Касперского". Адрес источника обновлений.
PROXY_SERVER	Адрес прокси-сервера, используемого для подключения к интернету.	Адрес прокси-сервера.

Параметр	Описание	Значения
UPDATE_EXECUTE	Запуск задачи обновления баз приложения во время процедуры настройки.	yes – запускать задачу обновления. no – не запускать задачу обновления.
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра.	yes – компилировать модуль ядра. no – не компилировать модуль ядра.
ADMIN_USER	Пользователь, которому назначена роль администратора (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. 77) (admin).	
CONFIGURE_SELINUX	Автоматическая настройка SELinux для работы с приложением Kaspersky Industrial CyberSecurity for Linux Nodes.	yes – выполнить автоматическую настройку SELinux для работы с приложением. no – не выполнять автоматическую настройку SELinux для работы с приложением.

Параметр	Описание	Значения
PROTECTION_MODE	Режим работы (см. раздел "О режимах работы приложения" на стр. 19), который приложение использует сразу после установки.	<i>Disabled</i> – при запуске приложения после установки все компоненты приложения по умолчанию выключены. Запускаются только служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. <i>OAS_Notify</i> – при запуске приложения после установки автоматически запускается только компонент Защита от файловых угроз и служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. Компонент Защита от файловых угроз работает в информирующем режиме. <i>Информирующий режим</i> – это такой режим работы приложения, при котором в случае обнаружения угрозы компоненты и задачи приложения не пытаются лечить или удалять вредоносные объекты, запрещать доступ или блокировать активность приложений, а только информируют пользователя об обнаружении угрозы. <i>OAS_Block</i> – при запуске приложения после установки автоматически запускается только компонент Защита от файловых угроз и служебные задачи, обеспечивающие активацию приложения и работу резервного хранилища. При обнаружении угрозы приложение выполняет действия, заданные в параметрах компонента Защита от файловых угроз.

Параметр	Описание	Значения
DISABLE_FILEAV_ACTIONS	Выключение функций лечения и удаления файлов для компонентов приложения после его установки. Если функции лечения и удаления файлов выключены, в случае обнаружения угрозы приложение не пытается лечить или удалять файлы, в которых обнаружена угроза, а только информирует пользователя об обнаружении угрозы. После установки приложения вы можете включить функции лечения и удаления файлов с помощью параметра <code>DisableFileAvActions</code> в конфигурационном файле <code>kics.ini</code> (см. раздел "Предустановленные конфигурационные файлы" на стр. 702).	<code>yes</code> – выключить функции лечения и удаления файлов при запуске приложения после установки. <code>no</code> (значение по умолчанию) – не выключать функции лечения и удаления файлов при запуске приложения после установки.

Если вы хотите изменить параметры в конфигурационном файле первоначальной настройки, укажите значения параметров в формате <имя параметра>=<значение параметра> (приложение не обрабатывает пробелы между именем параметра и его значением).

Настройка разрешающих правил в системе SELinux

Настройка SELinux для работы с приложением вручную

Если во время первоначальной настройки приложению Kaspersky Industrial CyberSecurity for Linux Nodes не удалось настроить систему SELinux автоматически (см. раздел "Включение автоматической настройки SELinux" на стр. [57](#)) или вы отказались от автоматической настройки, вы можете вручную настроить систему SELinux для работы с приложением Kaspersky Industrial CyberSecurity for Linux Nodes.

► Чтобы вручную настроить SELinux для работы с приложением:

1. Переведите SELinux в неблокирующий режим:
 - Если SELinux был активирован, выполните следующую команду:

```
# setenforce Permissive
```
 - Если SELinux был выключен, в конфигурационном файле `/etc/selinux/config` задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.
2. Убедитесь, что в системе установлена утилита `semanage`. Если утилита не установлена, установите пакет `polyscoreutils-python` или `polyscoreutils-python-utils` в зависимости от типа менеджера пакетов.

3. Если вы используете пользовательскую политику SELinux, то есть отличную от заданной по умолчанию `targeted policy`, назначьте метку для каждого исходного исполняемого файла приложения Kaspersky Industrial CyberSecurity for Linux Nodes в соответствии с используемой политикой SELinux, выполнив следующие команды:

```
# semanage fcontext -a -t bin_t <исполняемый файл>
# restorecon -v <исполняемый файл>
```

где <исполняемый файл>:

- `/var/opt/kaspersky/kics/1.5.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kics/libexec/kics`
- `/var/opt/kaspersky/kics/1.5.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kics/bin/kics-control`
- `/var/opt/kaspersky/kics/1.5.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kics/libexec/kics-gui`
- `/var/opt/kaspersky/kics/1.5.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kics/shared/kics`

4. Запустите следующие задачи:

- задачу Защита от файловых угроз:
`kics-control --start-task 1`
- задачу Проверка важных областей:
`kics-control --start-task 4 -W`

Рекомендуется запустить все задачи, которые вы планируете запускать при использовании приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

5. Запустите графический пользовательский интерфейс, если вы планируете его использовать.
6. Убедитесь, что в файле `audit.log` нет ошибок:

```
# grep kics /var/log/audit/audit.log
```

7. Если в файле `audit.log` присутствуют ошибки, создайте и загрузите новый модуль правил на основе блокирующих записей, чтобы устранить ошибки, и снова запустите задачи, которые вы планируете запускать при использовании приложения Kaspersky Industrial CyberSecurity for Linux Nodes, выполнив следующие команды:

```
# grep kics /var/log/audit/audit.log | audit2allow -M kics
# semodule -i kics.pp
```

В случае появления новых `audit`-сообщений, связанных с Kaspersky Industrial CyberSecurity for Linux Nodes, требуется обновить файл модуля правил.

8. Переведите SELinux в блокирующий режим:

```
# setenforce Enforcing
```

Если вы используете пользовательскую политику SELinux, то после установки обновлений приложения вам нужно вручную назначить метку для исходных исполняемых файлов приложения Kaspersky Industrial CyberSecurity for Linux Nodes (выполните шаги 1, 3–8).

Дополнительную информацию вы можете найти в документации для используемой операционной системы.

Настройка SELinux для запуска задачи **Запуск процесса**

Если в вашей операционной системе установлена система SELinux в режиме `Enforcing`, то для запуска задачи **Запуск процесса** (см. раздел "Об ответных действиях по командам" на стр. [612](#)) вам нужно дополнительно настроить систему SELinux.

► Чтобы настроить SELinux для запуска задачи **Запуск процесса**:

1. Переведите SELinux в неблокирующий режим:
 - Если SELinux был активирован, выполните следующую команду:

```
# setenforce Permissive
```
 - Если SELinux был выключен, в конфигурационном файле `/etc/selinux/config` задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.
2. Убедитесь, что в системе установлена утилита `semanage`. Если утилита не установлена, установите пакет `polyscoreutils-python` или `polyscoreutils-python-utils` в зависимости от типа менеджера пакетов.
3. Запустите задачу **Запуск процесса**.
4. Убедитесь, что в файле `audit.log` нет ошибок:

```
# grep kics /var/log/audit/audit.log
```
5. Если в файле `audit.log` присутствуют ошибки, создайте и загрузите новый модуль правил на основе блокирующих записей, чтобы устранить ошибки, и снова запустите задачу **Запуск процесса**.

```
# grep kics /var/log/audit/audit.log | audit2allow -M kics
# semodule -i kics.pp
```
6. Переведите SELinux в блокирующий режим:

```
# setenforce Enforcing
```

Запуск приложения в ОС Astra Linux в режиме замкнутой программной среды

В этом разделе описаны действия, которые требуется выполнить, чтобы запустить приложение в операционной системе Astra Linux Special Edition.

Для Astra Linux Special Edition (очередное обновление 1.7) и Astra Linux Special Edition (очередное обновление 1.6)

- Чтобы запустить приложение в операционной системе Astra Linux Special Edition (очередное обновление 1.7) или Astra Linux Special Edition (очередное обновление 1.6):

1. Укажите следующие параметры в файле `/etc/digisig/digisig_initramfs.conf`:

```
DIGSIG_ELF_MODE=1
```

2. Установите пакет совместимости:

```
apt install astra-digisig-oldkeys
```

3. Создайте директорию для ключа приложения:

```
mkdir -p /etc/digisig/keys/legacy/kaspersky/
```

4. Разместите ключ приложения (`/opt/kaspersky/kics/shared/kaspersky_astra_pub_key.gpg`) в директории, созданной на предыдущем шаге:

```
cp kaspersky_astra_pub_key.gpg /etc/digisig/keys/legacy/kaspersky/
```

5. Обновите образ `initramfs`:

```
update-initramfs -u -k all
```

Для Astra Linux Special Edition (очередное обновление 1.5)

- Чтобы запустить приложение в операционной системе Astra Linux Special Edition (очередное обновление 1.5):

1. Укажите следующие параметры в файле `/etc/digisig/digisig_initramfs.conf`:

```
DIGSIG_LOAD_KEYS=1
```

```
DIGSIG_ENFORCE=1
```

2. Создайте директорию для ключа приложения:

```
mkdir -p /etc/digisig/keys/legacy/kaspersky/
```

3. Разместите ключ приложения (`/opt/kaspersky/kics/shared/kaspersky_astra_pub_key.gpg`) в директории, созданной на предыдущем шаге:

```
cp kaspersky_astra_pub_key.gpg /etc/digisig/keys/legacy/kaspersky/
```

4. Обновите образ `initramfs`:

```
sudo update-initramfs -u -k all
```

Работа с графическим пользовательским интерфейсом приложения поддерживается для сессий с мандатным разграничением доступа.

Установка и удаление приложения на устройстве с ОС TeNIX WS

► Чтобы установить приложение на устройство с операционной системой TeNIX WS:

1. Распакуйте архив с пакетами в нужную директорию.
2. Установите нужные пакеты с помощью менеджера пакетов `tpkg`, выполнив одну из следующих команд:
 - `PKGDIR=<директория с пакетами> tpkg kics` – для установки приложения без графического пользовательского интерфейса;
 - `PKGDIR=<директория с пакетами> tpkg kics-gui` – для установки приложения и графического пользовательского интерфейса;
 - `PKGDIR=<директория с пакетами> tpkg klnagent` – для установки пакета Агента администрирования.
3. Выполните первоначальную настройку приложения (см. раздел "Первоначальная настройка приложения в интерактивном режиме" на стр. [54](#)) и Агента администрирования (см. раздел "Установка и первоначальная настройка Агента администрирования Kaspersky Security Center" на стр. [29](#)).

► Чтобы удалить приложение с устройства с операционной системой TeNIX WS, выполните команду:

```
PKGDIR=<директория с пакетами> tpkg -d <пакет>
```

где `<пакет>` – один из следующих установочных пакетов:

- `kics` – пакет приложения без графического пользовательского интерфейса;
- `kics-gui` – пакет приложения с графическим пользовательским интерфейсом;
- `klnagent` – пакет Агента администрирования.

Удаление приложения

Процедура удаления приложения Kaspersky Industrial CyberSecurity for Linux Nodes состоит из следующих этапов:

1. Удаление приложения и графического пользовательского интерфейса приложения

Вам нужно удалить с защищаемых устройств пакеты приложения и графического пользовательского интерфейса приложения, если вы использовали графический пользовательский интерфейс.

Вы можете одновременно удалить пакет приложения и пакет графического пользовательского интерфейса или удалить только пакет графического пользовательского интерфейса. Невозможно удалить только пакет приложения, если установлен пакет графического пользовательского интерфейса.

Вы можете удалять приложение и графический пользовательский интерфейс приложения следующими способами:

- Удаленно с помощью Kaspersky Security Center (см. раздел "Об удалении приложения и Агента администрирования с помощью Kaspersky Security Center" на стр. [72](#)).
- Локально из командной строки (см. раздел "Удаление приложения с помощью командной строки" на стр. [72](#)).

В процессе удаления приложения на устройстве будут остановлены все задачи Kaspersky Industrial CyberSecurity for Linux Nodes.

d. Удаление Агента администрирования

Если вы использовали Kaspersky Security Center для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes, вам нужно удалить Агент администрирования с защищаемых устройств.

Вы можете удалять Агент администрирования следующими способами:

- Удаленно с помощью Kaspersky Security Center (см. раздел "Об удалении приложения и Агента администрирования с помощью Kaspersky Security Center" на стр. [72](#)).
- Локально из командной строки (см. раздел "Удаление Агента администрирования с помощью командной строки" на стр. [73](#)).

e. Удаление плагина управления Kaspersky Industrial CyberSecurity for Linux Nodes

Если вы использовали Kaspersky Security Center для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes, вам нужно удалить веб-плагин или mms-плагин управления (см. раздел "Об удалении плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [74](#)) Kaspersky Industrial CyberSecurity for Linux Nodes, в зависимости от консоли управления Kaspersky Security Center, которую вы использовали.

После удаления приложения удаляется вся информация, сохраненная во время его работы, кроме базы данных лицензий. Удаляются в том числе установленные сертификаты приложения. База данных лицензий сохраняется, вы можете использовать ее для повторной установки приложения.

Если приложение было установлено в systemd-системе, то после удаления приложения параметры systemd возвращаются в исходное состояние.

В этом разделе

Об удалении приложения и Агента администрирования с помощью Kaspersky Security Center	72
Удаление приложения с помощью командной строки.....	72
Удаление Агента администрирования с помощью командной строки.....	73
Об удалении плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes	74

Об удалении приложения и Агента администрирования с помощью Kaspersky Security Center

Вы можете удаленно удалять с клиентских устройств приложение Kaspersky Industrial CyberSecurity for Linux Nodes и Агент администрирования.

Удаление выполняется с помощью задачи удаленной деинсталляции приложений в Kaspersky Security Center Web Console или в Консоли администрирования. См подробнее в справке Kaspersky Security Center.

Если вы хотите удалить только графический пользовательский интерфейс, не удаляя при этом приложение, вам нужно установить значение параметра `USE_GUI=No` в конфигурационном файле `autoinstall.ini` (см. раздел "Параметры конфигурационного файла `autoinstall.ini`" на стр. [42](#)) и запустить задачу удаленной установки приложений.

Удаление выполняется в фоновом режиме. После завершения удаления приложения отобразится запрос на перезагрузку клиентского устройства.

Удаление приложения с помощью командной строки

Удаление пакета приложения и пакета графического интерфейса

- Чтобы удалить приложение и графический пользовательский интерфейс, установленные из пакетов формата *RPM*, выполните следующую команду:

```
# rpm -e kics kics-gui
```

- Чтобы удалить приложение и графический пользовательский интерфейс, установленные из пакетов формата *DEB*, выполните следующую команду:

```
# apt-get purge kics kics-gui
```

Удаление пакета приложения без удаления пакета графического интерфейса

- Чтобы удалить приложение, установленное из пакета формата *RPM*, без удаления графического пользовательского интерфейса, выполните следующую команду:

```
# rpm -e kics
```


- Чтобы удалить приложение, установленное из пакета формата DEB, без удаления графического пользовательского интерфейса, выполните следующую команду:

```
# apt-get purge kics
```

Удаление пакета графического интерфейса

- Чтобы удалить графический пользовательский интерфейс, установленный из пакета формата RPM, выполните следующую команду:

```
# rpm -e kics-gui
```

- Чтобы удалить графический пользовательский интерфейс, установленный из пакета формата DEB, выполните следующую команду:

```
# apt-get purge kics-gui
```

После завершения процедуры удаления выводится сообщение о результатах удаления.

Удаление Агента администрирования с помощью командной строки

- Чтобы удалить Агент администрирования, установленный на 32-битную операционную систему из пакета формата RPM, выполните следующую команду:

```
# rpm -e klnagent
```

- Чтобы удалить Агент администрирования, установленный на 64-битную операционную систему из пакета формата RPM, выполните следующую команду:

```
# rpm -e klnagent64
```

- Чтобы удалить Агент администрирования, установленный на 32-битную операционную систему из пакета формата DEB, выполните следующую команду:

```
# apt-get purge klnagent
```

- Чтобы удалить Агент администрирования, установленный на 64-битную операционную систему из пакета формата DEB, выполните следующую команду:

```
# apt-get purge klnagent64
```

После завершения процедуры удаления выводится сообщение о результатах удаления.

Об удалении плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes

Удаление веб-плагина управления Kaspersky Industrial CyberSecurity for Linux Nodes выполняется в Kaspersky Security Center Web Console в списке установленных плагинов (**Параметры** → **Веб-плагины**).

Для удаления mms-плагина используйте стандартные средства удаления приложений в операционной системе. В списке приложений вам нужно выбрать для удаления **Kaspersky Industrial CyberSecurity for Linux Nodes <номер версии>**.

Процедура приемки

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

В этом разделе

Безопасное состояние приложения	75
Проверка работоспособности. Тестовый файл EICAR	75

Безопасное состояние приложения

Приложение находится в безопасном состоянии (сертифицированной конфигурации), если выполняются следующие условия:

- Приложение активировано: добавлен лицензионный ключ.
- Обновлено базы приложения.
- KSN выключен или используется KPSN.
- Настроена и запущена задача Защита от файловых угроз (см. стр. [172](#)).
- Параметры приложения находятся в рамках допустимых значений, приведенных в Приложении 6 (см. раздел "Приложение 6. Значения параметров приложения в сертифицированной конфигурации" на стр. [737](#)) к этому документу.

Проверка работоспособности. Тестовый файл EICAR

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

Тестовый файл EICAR предназначен для проверки работы антивирусных приложений. 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 устройству, но антивирусные приложения большинства производителей идентифицируют в нем угрозу.

Вы можете загрузить тестовый файл EICAR со страницы веб-сайта организации EICAR <https://www.eicar.org/download-anti-malware-testfile/>.

Перед сохранением файла в папке на диске устройства убедитесь, что Защита от файловых угроз и Защиты от веб-угроз остановлены.

► *Чтобы проверить работоспособность приложения:*

1. Убедитесь, что параметры приложения находятся в рамках допустимых значений, приведенных в Приложении 6 (см. раздел "Приложение 6. Значения параметров приложения в сертифицированной конфигурации" на стр. [737](#)) к этому документу.
2. Убедитесь, что приложение активировано и базы приложения обновлены, выполнив следующую команду:

```
kics-control --app-info
```

Ожидаемый результат: приложение выводит на экран следующую информацию:

Информация о лицензии: Ключ действителен

Базы приложения загружены: Да

Защита от файловых угроз: Задача доступна и выполняется

3. Убедитесь, что запущены задача Защита от файловых угроз и Задача от веб-угроз, выполнив следующую команду:

```
kics-control --get-task-list
```

Ожидаемый результат: задачи Защита от файловых угроз и Задача от веб-угроз присутствуют в списке задач, статус обеих задач *Started*.

4. Остановите задачу Защита от файловых угроз, выполнив следующую команду:

```
kics-control --stop-task 1
```

5. Остановите задачу Защита от веб-угроз, выполнив следующую команду:

```
kics-control --stop-task 14
```

6. Скачайте EICAR-файл на сайте <https://www.eicar.org/download-anti-malware-testfile/>.

Если вы скачали архив, предварительно распакуйте его в защищаемую область. По умолчанию защищается вся файловая система.

7. Запустите задачу Защита от файловых угроз, выполнив следующую команду:

```
kics-control --start-task 1
```

8. Запустите задачу Защита от веб-угроз, выполнив следующую команду:

```
kics-control --start-task 14
```

9. Попытайтесь открыть файл `eicar.com`, выполнив следующую команду:

```
cat <абсолютный путь к файлу>/eicar.com
```

Ожидаемый результат: приложение выдает ошибку о том, что указанный файл отсутствует или доступ к нему запрещен.

10. Убедитесь, что зараженный файл был удален из директории устройства.

11. Проверьте наличие событий об удалении зараженного файла, выполнив следующую команду:

```
kics-control -E --query "EventType=='ObjectDeleted'"
```

Разделение доступа к функциям приложения по пользовательским ролям

Доступ к функциям приложения Kaspersky Industrial CyberSecurity for Linux Nodes через командную строку предоставляется пользователю в соответствии с его ролью. *Роль* – это набор прав и разрешений на управление приложением.

В операционной системе создаются четыре группы пользователей системы: *kicsadmin*, *kicsuser*, *kicsaudit* и *pokics*. Когда роль в приложении назначается пользователю (см. раздел "Назначение роли пользователю" на стр. [79](#)) системы, этот пользователь добавляется в соответствующую группу ролей (см. таблицу *Роли* ниже). При отзыве роли у пользователя (см. раздел "Отзыв роли у пользователя" на стр. [79](#)) пользователь удаляется из соответствующей группы ролей.

Если пользователю системы не назначено ни одной роли в приложении, этот пользователь относится к отдельной группе *пользователи без прав*.

Таким образом, роли соответствуют четырем группам пользователей операционной системы:

- *kicsadmin* соответствует роли Администратор;
- *kicsuser* соответствует роли Пользователь;
- *kicsaudit* соответствует роли Аудитор;
- *pokics* назначается пользователю, если не назначена ни одна из ролей. В этом случае пользователь относится к отдельной группе *пользователи без прав*.

Таблица 4. Роли пользователей

Название роли	Роль в приложении	Пользователь ОС	Права
Администратор	admin	kicsadmin	Управление параметрами приложения и параметрами задач. Управление лицензированием приложения. Назначение ролей пользователям. Отзыв ролей у пользователей (администратор не имеет права отозвать роль admin у себя самого). Просмотр и управление хранилищами пользователей.
Пользователь	user	kicsuser	Управление только задачами выборочной проверки файлов. Запуск и остановка задач обновления. Просмотр отчетов для созданных пользователем задач. Просмотр особых событий, общих для всех пользователей приложения.
Аудитор	audit	kicsaudit	Просмотр параметров приложения. Просмотр статуса приложения. Просмотр всех задач, их параметров и расписания запуска. Просмотр всех событий. Просмотр всех объектов в резервном хранилище.
—	—	nokics	Роль в приложении не назначена, права отсутствуют.

В этом разделе

Просмотр списка пользователей и ролей	78
Назначение роли пользователю	79
Отзыв роли у пользователя	79

Просмотр списка пользователей и ролей

- Чтобы просмотреть список пользователей и их ролей, выполните следующую команду:

```
kics-control [-U] --get-user-list
```

Назначение роли пользователю

- Чтобы назначить роль определенному пользователю, выполните следующую команду:

```
kics-control [-U] --grant-role <роль> <пользователь>
```

Пример:

Назначить роль *audit* пользователю *test15*:

```
kics-control --grant-role audit test15
```

Отзыв роли у пользователя

- Чтобы отозвать роль у определенного пользователя, выполните следующую команду:

```
kics-control [-U] --revoke-role <роль> <пользователь>
```

Пример:

Отозвать роль *audit* у пользователя *test15*:

```
kics-control --revoke-role audit test15
```

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

В этом разделе

О Лицензионном соглашении	80
О лицензии	81
О лицензионном сертификате	81
О лицензионном ключе	82

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать приложение.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом использования приложения.

Вы можете ознакомиться с условиями Лицензионного соглашения для решения Kaspersky Industrial CyberSecurity for Linux Nodes и с Политикой конфиденциальности, которая описывает обработку и передачу данных, следующими способами:

- Прочитав текст файла `license.<идентификатор языка>`. Этот файл включен в комплект поставки приложения.
- Во время установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes (см. раздел "Установка и первоначальная настройка приложения" на стр. [28](#)).

Вы принимаете условия Лицензионного соглашения и Политики конфиденциальности, подтверждая свое согласие с текстом Лицензионного соглашения и Политики конфиденциальности во время создания инсталляционного пакета приложения (в случае установки с помощью Kaspersky Security Center (см. раздел "Установка и первоначальная настройка приложения с помощью Kaspersky Security Center" на стр. [34](#))) или во время первоначальной настройки приложения (см. раздел "Первоначальная настройка приложения в интерактивном режиме" на стр. [54](#)) (в случае установки с помощью командной строки). Если вы не согласны с условиями Лицензионного соглашения и Политики конфиденциальности, вы должны прервать установку приложения и не должны использовать приложение.

- После установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes.
После установки приложения файлы с текстом Лицензионного соглашения приложения Kaspersky Industrial CyberSecurity for Linux Nodes и Политики конфиденциальности расположены на защищаемом устройстве в директории `/opt/kaspersky/kics/doc/license.<идентификатор языка>`.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Industrial CyberSecurity for Linux Nodes, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения). Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с приложением.

Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Industrial CyberSecurity for Linux Nodes прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая* – платная лицензия.

По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Industrial CyberSecurity for Linux Nodes вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о приложении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*. Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Код активации – это уникальная последовательность из двадцати латинских букв и цифр.

Использование кода активации не допускается в сертифицированной конфигурации. Для активации приложения требуется использовать файл ключа.

Файл ключа предназначен для добавления лицензионного ключа, активирующего приложение. Если файл ключа был случайно удален, вы можете его восстановить. Для восстановления файла ключа вам нужно обратиться к продавцу лицензии.

Для активации приложения с помощью файла ключа подключение к серверам активации "Лаборатории Касперского" не требуется.

Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

Для приложения Kaspersky Industrial CyberSecurity for Linux Nodes предусмотрены лицензионные ключи следующих *типов*:

- *Ключ приложения* – лицензионный ключ для активации функциональности приложения Kaspersky Industrial CyberSecurity for Linux Nodes. Набор доступных функций приложения зависит от лицензии, связанной с ключом приложения.
- *Ключ EDR Optimum* – дополнительный лицензионный ключ Kaspersky Endpoint Detection and Response Optimum Add-on для активации функциональности Kaspersky Endpoint Detection and Response Optimum (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response Optimum" на стр. [610](#)). Этот ключ требуется, если вы используете приложение по лицензии, которая не включает функциональность Kaspersky Endpoint Detection and Response Optimum.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы приложения требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и резервным.

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен лицензионный ключ для пробной лицензии или ключ для коммерческой лицензии (коммерческий ключ). В приложении можно добавить только один активный ключ каждого типа.

Резервный лицензионный ключ – лицензионный ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Резервный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным

лицензионным ключом. Резервный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа того же типа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа.

Предоставление данных

Этот раздел содержит информацию о данных, которые приложение Kaspersky Industrial CyberSecurity for Linux Nodes может сохранять на устройстве и передавать в автоматическом режиме в "Лабораторию Касперского" в ходе своей работы.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Более подробная информация об обработке, хранении и уничтожении информации, полученной во время использования приложения и переданной в "Лабораторию Касперского", приведена в Лицензионном соглашении (см. раздел "О Лицензионном соглашении" на стр. 80), Положении о Kaspersky Security Network и Политике конфиденциальности на веб-сайте "Лаборатории Касперского" <https://www.kaspersky.ru/products-and-services-privacy-policy>. Файлы license.<идентификатор языка> и ksn_license.<идентификатор языка> с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки приложения.

В этом разделе

Данные, предоставляемые при загрузке обновлений с серверов обновлений "Лаборатории Касперского"	84
Данные, передаваемые приложению Kaspersky Security Center	85
Данные, предоставляемые при переходе по ссылкам из интерфейса приложения	88
Данные, предоставляемые при использовании Kaspersky Security Network	88
Данные, передаваемые приложению Kaspersky Industrial CyberSecurity for Networks	89
Данные, предоставляемые при использовании Kaspersky Endpoint Detection and Response Optimum	92

Данные, предоставляемые при загрузке обновлений с серверов обновлений "Лаборатории Касперского"

Если вы используете серверы обновлений «Лаборатории Касперского» для загрузки обновлений, с целью повышения эффективности процедуры обновления и для получения статистической информации о распространении и использовании приложения, вы соглашаетесь предоставлять в автоматическом режиме следующую информацию:

- идентификатор приложения, полученный из лицензии;
- полную версию приложения;
- идентификатор лицензии приложения;
- тип используемой лицензии;
- идентификатор установки приложения (PCID);
- идентификатор запуска обновления приложения;
- обрабатываемый веб-адрес.

Данные, передаваемые приложению Kaspersky Security Center

Во время работы приложение Kaspersky Industrial CyberSecurity for Linux Nodes сохраняет и передает приложению Kaspersky Security Center следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Информацию о базах, используемых в приложении:
 - список категорий баз, необходимых приложению;
 - дату и время выпуска и загрузки используемых баз в приложение;
 - дату выпуска загруженных обновлений баз приложения;
 - время последнего обновления баз приложения;
 - количество записей в текущих используемых базах приложения.
- Информацию о лицензии на использование приложения:
 - серийный номер и тип лицензии;
 - срок действия лицензии в днях;
 - количество устройств, на которые распространяется лицензия;
 - даты начала и окончания срока действия лицензии;
 - статус лицензионного ключа;
 - дату и время последней удачной синхронизации с серверами активации в случае, если приложение активировано с помощью кода активации;
 - идентификатор приложения, для активации которого предоставлена лицензия;
 - доступную по лицензии функциональность;
 - название организации, которой предоставлена лицензия;
 - дату и время окончания срока действия лицензии на устройстве.
- Информацию об обновлениях приложения:
 - список обновлений, которые требуется установить или удалить;
 - дату выпуска обновления и наличие статуса *Критическое*;
 - название, версию и краткое описание обновления;
 - ссылку на статью с полным описанием обновления;
 - идентификатор и текст Лицензионного соглашения и Политики конфиденциальности для обновления приложения;
 - идентификатор и текст Положения о Kaspersky Security Network для обновления приложения;
 - признак возможности удаления обновления;
 - версии политики и плагина управления приложением;
 - веб-адрес для загрузки плагина управления приложением;
 - названия установленных обновлений приложения, версии и даты их установки;
 - код и описание ошибки, если установка или удаление обновления завершились с ошибкой;

- признак и причину необходимости перезагрузки устройства или приложения по причине обновления приложения.
- Согласие или несогласие пользователя с условиями Положения о Kaspersky Security Network, Лицензионного соглашения и Политики конфиденциальности.
- Список тегов, назначенных устройству.
- Список статусов устройства и причины их назначения.
- Общий статус приложения и статус всех его компонентов; информацию о соответствии политике, статус постоянной защиты устройства, статус стабильности работы приложения, информация об остановке приложения.
- Дату и время последней проверки устройства; количество проверенных объектов; количество обнаруженных вредоносных объектов; количество заблокированных, удаленных и вылеченных объектов; количество объектов, которые не удалось вылечить; количество ошибок проверки; количество обнаруженных сетевых атак.
- Данные о текущих примененных значениях параметров приложения.
- Текущий статус и результат выполнения групповых и локальных задач и значения их параметров.
- Информацию о внешних устройствах, подключенных к клиентскому устройству (идентификатор, имя, тип, производитель, описание, серийный номер и VID/PID).
- Информацию о резервных копиях файлов, помещенных в резервное хранилище (имя, путь, размер и тип объекта, описание объекта, имя обнаруженной угрозы, версию баз приложения, с помощью которых была обнаружена угроза, дату и время помещения объекта в резервное хранилище, действия над объектом в резервном хранилище (удален, восстановлен)), а также сами файлы по запросу администратора.
- Информацию о работе каждого компонента приложения и о выполнении каждой задачи в виде событий:
 - дату и время возникновения события;
 - название и тип события;
 - уровень важности события;
 - название задачи или компонента приложения, во время работы которых произошло событие;
 - информацию о приложении, которое вызвало событие: название приложения, путь к файлу на диске, идентификатор процесса, значения параметров в случае публикации события о запуске или изменении параметров работы приложения;
 - идентификатор пользователя;
 - имя инициатора (планировщика задач, или приложения, или Kaspersky Security Center, или имя пользователя), действия которого привели к возникновению события;
 - имя и идентификатор пользователя, инициировавшего доступ к файлу;
 - результат обработки объекта или действия (описание, тип, название, уровень угрозы и точность, имя файла и тип операции над устройством, решение приложения по этой операции);
 - информацию об объекте (имя и тип объекта, путь к объекту на диске, версия объекта, размер, информация о выполненном действии, описание причины возникновения события, описание причины необработки и пропуска объекта);

- информацию об устройстве (имя производителя, имя устройства, путь, тип устройства, тип шины, идентификатор, VID/PID, признак системного устройства, название расписания правила доступа к устройству);
- информацию о блокировке и разблокировке устройства; информацию о заблокированных подключениях (название, описание, имя устройства, протокол, удаленный адрес и порт, локальный адрес и порт, пакетные правила, действия);
- информацию о запрошенном веб-адресе;
- информацию об обнаруженных объектах;
- тип, метод и идентификатор обнаружения;
- информацию о выполненном действии;
- информацию о базах приложения (дату выпуска загруженных обновлений баз, информацию о применении баз, ошибки применения баз, информацию об отмене установленных обновлений баз);
- информацию об обнаружении шифрования (имя шифровальщика; имя устройства, на котором обнаружено шифрование; информацию о блокировке и разблокировке устройства);
- параметры приложения и сетевые параметры;
- информацию о сработавшем правиле Контроля приложений (имя и тип) и результат его применения;
- информацию о контейнерах и образах контейнеров (имена контейнеров или образов контейнеров, пути к контейнерам или образам контейнеров, веб-адрес репозитория);
- информацию об активных и заблокированных подключениях (название, описание и тип);
- информацию о блокировке и разблокировке доступа к недоверенным устройствам;
- информацию об использовании KSN (статус подключения к KSN, инфраструктура KSN, идентификатор Положения о KSN в расширенном режиме, принятие Положения о KSN в расширенном режиме, идентификатор Положения о KSN, принятие Положения о KSN);
- информацию о сертификатах (доменное имя, название субъекта, название издателя, дату окончания срока действия, статус сертификата, тип сертификата, время добавления сертификата, дату выпуска, серийный номер, отпечаток SHA256);
- информацию о внешних системах, входящих в состав корпоративных программных решений (адрес сервера интеграции);
- информацию о включении и выключении сетевой изоляции для устройства;
- имя устройства, для которого включена или выключена сетевая изоляция;
- статистику выполнения задачи проверки: количество проверенных объектов; количество найденных угроз; количество зараженных объектов; количество возможно зараженных объектов; количество вылеченных объектов; количество объектов, добавленных в резервное хранилище; количество удаленных объектов; количество невылеченных объектов; количество ошибок проверки; количество объектов, защищенных паролем; количество пропущенных объектов; количество проверенных контейнеров и образов;
- информацию о версии компонента EDR Optimum, используемого в приложении;
- информацию о цепочках развития угрозы: имя сетевого списка цепочек развития угрозы, идентификатор цепочки развития угрозы.

- Информацию о работе задачи проверки целостности системы (имя, тип, путь) и информацию о снимке состояния системы.
- Информацию о сетевой активности, о пакетных правилах и о сетевых атаках.
- Информацию о роли пользователя:
 - имя и идентификатор пользователя, инициировавшего изменение роли пользователя;
 - роль пользователя;
 - имя пользователя, которому назначена или у которого отозвана роль.
- Информацию об исполняемых файлах приложений, обнаруженных на клиентском устройстве (имя, путь, тип и хеш файла; список категорий, к которым отнесено приложение; KL-категория, к которой отнесено приложение; группу доверия, к которой отнесено приложение; первое время запуска файла; название и версию приложения; название производителя приложения; информацию о сертификате, которым подписано приложение: серийный номер, отпечаток, издатель, субъект, дату выпуска, дату окончания действия и открытый ключ).
- Информацию о сетевом списке цепочек развития угрозы: идентификатор цепочки развития угрозы, время создания цепочки развития угрозы в виде метки времени, формат цепочки развития угрозы (текст или архив), размер тела цепочки развития угрозы в байтах.

Данные, предоставляемые при переходе по ссылкам из интерфейса приложения

При переходе по ссылкам из интерфейса приложения Kaspersky Industrial CyberSecurity for Linux Nodes вы соглашаетесь предоставлять в «Лабораторию Касперского» в автоматическом режиме следующую информацию:

- полную версию приложения;
- локализацию приложения;
- идентификатор приложения (PID);
- имя ссылки.

Данные, предоставляемые при использовании Kaspersky Security Network

Если вы используете Kaspersky Security Network в расширенном режиме, вы соглашаетесь передавать в "Лабораторию Касперского" в автоматическом режиме все данные, перечисленные в Положении о Kaspersky Security Network. Кроме того, в "Лабораторию Касперского" для проверки могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда устройству и хранящимся в его операционной системе данным.

Файл ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Данные, передаваемые приложению Kaspersky Industrial CyberSecurity for Networks

При интеграции приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Industrial CyberSecurity for Networks приложение передает на сервер интеграции Kaspersky Industrial CyberSecurity for Networks следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Адреса серверов интеграции.
- Открытый ключ сертификата сервера интеграции.
- Криптоконтейнер с сертификатом клиента.
- Учетные данные для авторизации на прокси-сервере.
- Параметры частоты синхронизации с сервером интеграции и параметры передачи данных на сервер интеграции.
- Статус соединения с сервером интеграции и сведения об ошибках сертификата клиента и сертификата сервера.
- Параметры задач, поступающих от серверов интеграции:
 - Тип источника OVAL®-скриптов: базы приложения или файл.
 - Полный путь и имя файла, описанного на языке OVAL/XCCDF/CPE, или его архив, если источником выбран файл.
 - Режим проверки OVAL-определений: все OVAL-определения, список указанных OVAL-определений или список всех OVAL-определений за исключением указанных.
 - Список имен OVAL-определений (идентификаторы вида "oval:org.mitre.oval.test:def:998"), разделенных точкой с запятой, которые необходимо проверить или исключить из проверки.
 - Признак необходимости логирования проверки и его уровень.
 - Параметры расписания запуска задач.
 - Имена и пароли учетных записей, под которыми требуется запускать задачи.
 - Версии параметров.
 - Тип запуска служб.
 - Названия служб.

При интеграции приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Industrial CyberSecurity for Networks приложение Kaspersky Industrial CyberSecurity for Linux Nodes сохраняет и может передавать серверу интеграции следующие данные:

- Данные из запросов на синхронизацию к серверу интеграции:
 - Уникальный идентификатор.
 - Базовую часть веб-адреса сервера.
 - Имя устройства.
 - IP-адрес устройства.
 - MAC-адрес устройства.
 - Локальное время на устройстве.

- Название, семейство и версию операционной системы, установленной на устройстве.
- Версию Kaspersky Industrial CyberSecurity for Linux Nodes.
- Дату выпуска используемых баз приложения.
- Состояние лицензии.
- Данные из запросов к серверу интеграции в отчетах о результатах выполнения задач:
 - Ошибки выполнения задач и коды возврата.
 - Статусы, с которыми завершались задачи.
 - Время завершения выполнения задач.
 - Версии параметров, с которыми выполнялись задачи.
 - Информацию из отчета по проверке на уязвимости:
 - Идентификаторы OVAL-определений.
 - Класс OVAL-определений.
 - Наименования OVAL-определений.
 - Типы результатов проверки OVAL-определений: True, False, Unknown, Error, Not Evaluated, Not Applicable.
 - Полные пути и имена файловых объектов, а также ветвей и ключей реестра, для которых сработало OVAL-определение типа vulnerability с результатом проверки True.
- Параметры устройства:
 - Производителя устройства.
 - Модель устройства.
 - Версию устройства.
 - Список процессоров; для каждого процессора: имя, количество ядер, количество логических процессоров.
 - Производителя BIOS устройства, версию, дату выпуска.
 - Общий объем оперативной памяти.
 - Список локальных дисков; для каждого диска: имя локального диска, общий размер и свободное место на диске.
 - Список USB-устройств; для каждого USB-устройства: имя, класс, идентификатор.
 - Список оптических устройств; для каждого устройства: модель, наличие вставленного диска.
 - Список сетевых интерфейсов; для каждого сетевого интерфейса: имя сетевого интерфейса, адресная информация, виртуальный или нет, активирован или нет.
- Параметры конфигурации устройства:
 - Доменное имя пользователя в формате domain\name.
 - Полное имя пользователя.
 - Уникальный идентификатор пользователя.
 - Название группы, в которую входит пользователь.
 - Уникальный идентификатор группы.

- Уникальный идентификатор пользователя как члена группы.
- Имя пользователя как члена группы.
- Информацию об активности аккаунта.
- Информацию о блокировке аккаунта.
- Информацию об ограниченности срока действия пароля.
- Информацию об актуальности пароля.
- Информацию о возможности изменения пароля пользователем.
- Название приложения, установленного на устройстве.
- Производителя приложения, установленного на устройстве.
- Размер установленного на устройстве приложения в байтах.
- Версию приложения, установленного на устройстве.
- Время установки приложения на устройство.
- Данные в пакетах телеметрии:
 - Информацию об устройстве и пользователях:
 - Имя и время устройства.
 - Семейство, имя и версию операционной системы.
 - Информацию о сетевых интерфейсах (описание, список IP-адресов с маской подсети, MAC-адрес, номер метрики, имя DNS-домена, данные о маршрутизации, номера прослушиваемых портов).
 - Внутренний уникальный идентификатор устройства.
 - Имена и идентификаторы пользователей.
 - Имена и идентификаторы групп пользователей.
 - Информацию о приложении Kaspersky Industrial CyberSecurity for Linux Nodes:
 - Имя и версию приложения.
 - Дату последнего обновления приложения.
 - Информацию о лицензионных ключах (серийный номер, тип, срок действия лицензии, статус ключа).
 - Версию баз приложения.
 - Список поддерживаемых версий API.
 - Информацию об установленных соединениях:
 - Локальный IP-адрес, порт и MAC-адрес.
 - Удаленный IP-адрес, порт и MAC-адрес.
 - IP-адрес шлюза.
 - Тип протокола (по IANA), номер протокола и EtherType.
 - Количество принятых и переданных пакетов.
 - Информацию об обрабатываемых файлах:

- Имя и уникальный идентификатор файла.
- Тип и размер файла.
- Полный путь к образу файла.
- Маску атрибутов файловой системы.
- Время создания и изменения файла.
- Контрольные суммы (MD5 и SHA256).
- Привилегии файла, в том числе унаследованные и эффективные.
- Информацию о запущенных процессах:
 - UID и PID процесса.
 - Тип процесса.
 - Идентификатор сеанса.
 - Выполняемую команду.
 - Переменные окружения.
- Информацию об обнаруженных и обработанных угрозах:
 - Название обнаруженной угрозы и технологии, обнаружившей угрозу, согласно классификации "Лаборатории Касперского".
 - Версию баз приложения.
 - Веб-адрес, с которого был загружен зараженный объект.
 - Статус обработки угрозы.
 - Причину невозможности устранения угрозы.

Также указанная информация может сохраняться в файлах трассировки (см. раздел "О файлах трассировки приложения" на стр. [663](#)) и файлах дампа (см. раздел "О файлах дампа" на стр. [667](#)).

Данные, предоставляемые при использовании Kaspersky Endpoint Detection and Response Optimum

Данные, передаваемые вместе с результатами выполнения задач *Поиск IOC*

Kaspersky Industrial CyberSecurity for Linux Nodes автоматически передает данные о результатах выполнения задач *Поиск IOC* в Kaspersky Security Center.

Данные о результатах выполнения задач *Поиск IOC* могут содержать следующую информацию:

- Сетевую информацию:
 - IP-адрес из таблицы протокола разрешения адресов (Address Resolution Protocol, ARP);
 - MAC-адрес из таблицы протокола разрешения адресов;
 - тип и имя записи DNS;

- IP-адрес защищаемого устройства;
- MAC-адрес защищаемого устройства;
- IP-адрес удаленного соединения и порт;
- IP-адрес локального сетевого адаптера;
- номер порта, открытого на локальном адаптере;
- номер протокола согласно стандарту Internet Assigned Numbers Authority (IANA).
- Информацию о процессах:
 - имя процесса;
 - аргументы процесса;
 - путь к исполняемому файлу процесса;
 - идентификатор процесса (PID);
 - идентификатор родительского процесса (PPID);
 - имя пользователя, запустившего процесс;
 - дату и время запуска процесса.
- Информацию о службах:
 - имя службы;
 - описание службы;
 - путь и имя исполняемого файла службы;
 - идентификатор службы;
 - тип службы (драйвер ядра, адаптер и т.д.);
 - статус службы;
 - режим запуска службы;
 - имя пользователя, под которым запущена служба.
- Информацию о файловой системе:
 - имя тома;
 - букву тома;
 - тип тома.
- Информацию об операционной системе:
 - имя и версию операционной системы;
 - сетевое имя защищаемого устройства;
 - домен или группу, к которым принадлежит устройство.
- Информацию о веб-активности:
 - имя браузера;
 - версию браузера;
 - время последнего обращения к веб-ресурсу;

- веб-адрес HTTP-запроса;
- имя пользователя, выполнившего HTTP-запрос;
- имя процесса, выполнившего HTTP-запрос;
- путь к исполняемому файлу процесса, выполнившего HTTP-запрос;
- идентификатор процесса, выполнившего HTTP-запрос;
- веб-адрес источника HTTP-запроса;
- веб-адрес запрошенного ресурса;
- агент пользователя обрабатываемого веб-запроса (HTTP User-Agent);
- время выполнения HTTP-запроса;
- уникальный идентификатор процесса, выполнившего HTTP-запрос.

Данные для построения цепочки развития угрозы

Данные для построения цепочки развития угрозы могут содержать следующую информацию:

- Общую информацию об алерте:
 - дату и время алерта;
 - имя объекта;
 - режим проверки;
 - статус последнего действия, связанного с алертом;
 - причину неудачной обработки алерта.
- Информацию об обрабатываемом объекте:
 - идентификатор процесса;
 - идентификатор родительского процесса;
 - идентификатор файла процесса;
 - командную строку процесса;
 - имя пользователя, запустившего процесс;
 - идентификатор сеанса, в котором запущен процесс;
 - тип сеанса, в котором запущен процесс;
 - уровень целостности обрабатываемого процесса;
 - принадлежность пользователя к привилегированным группам;
 - идентификатор обрабатываемого объекта;
 - полное имя обрабатываемого объекта;
 - идентификатор защищаемого устройства;
 - полное имя объекта (локальный файл или веб-адрес);
 - хеш-суммы MD5 и SHA256 обрабатываемого объекта;
 - тип обрабатываемого объекта;
 - дату создания и последнего изменения объекта;

- размер обрабатываемого объекта;
- атрибуты обрабатываемого объекта;
- информацию об организации, подписавшей объект;
- результат проверки цифрового сертификата объекта;
- идентификатор безопасности (SID) объекта;
- идентификатор часового пояса объекта;
- веб-адрес загрузки объекта (только для файлов);
- название приложения, загрузившего файл;
- хеш-суммы MD5 и SHA256 приложения, загрузившего файл;
- название приложения, последний раз изменившего файл;
- хеш-суммы MD5 и SHA256 приложения, последний раз изменившего файл;
- количество запусков обрабатываемого объекта;
- дату и время первого запуска объекта;
- уникальный идентификатор файла;
- полное имя файла (локальный файл или веб-адрес);
- веб-адрес обрабатываемого веб-запроса;
- источник ссылок обрабатываемого веб-запроса (HTTP referer);
- агент пользователя обрабатываемого веб-запроса;
- тип обрабатываемого веб-запроса (GET или POST);
- локальный IP-порт для обрабатываемого веб-запроса;
- удаленный IP-порт для обрабатываемого веб-запроса;
- направление соединения (входящее или исходящее) обрабатываемого веб-запроса;
- идентификатор процесса, в который произошло внедрение вредоносного кода.

Интерфейсы управления приложением

Вы можете управлять приложением Kaspersky Industrial CyberSecurity for Linux Nodes следующими способами:

- С помощью команд управления из командной строки (см. раздел "Управление приложением через командную строку" на стр. [118](#)).
- С помощью Консоли администрирования Kaspersky Security Center (см. раздел "Управление приложением через Kaspersky Security Center" на стр. [97](#)).
- С помощью Kaspersky Security Center Web Console (см. раздел "Управление приложением через Kaspersky Security Center" на стр. [97](#)).
- С помощью графического пользовательского интерфейса (см. раздел "Управление приложением через графический пользовательский интерфейс" на стр. [645](#)).

Концепция управления приложением

Для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes вы можете использовать:

- Kaspersky Security Center (см. раздел "Управление приложением через Kaspersky Security Center" на стр. [97](#));
- командную строку (см. раздел "Управление приложением через командную строку" на стр. [118](#));
- графический пользовательский интерфейс (см. раздел "Управление приложением через графический пользовательский интерфейс" на стр. [645](#)).

Набор действий, которые вы можете выполнять с помощью графического пользовательского интерфейса приложения Kaspersky Industrial CyberSecurity for Linux Nodes, ограничен (см. раздел "Управление приложением через графический пользовательский интерфейс" на стр. [645](#)).

В этом разделе описаны особенности управления приложением через Kaspersky Security Center и командную строку, и основные приемы работы в консолях управления Kaspersky Security Center и в командной строке.

В этом разделе

Управление приложением через Kaspersky Security Center	97
Управление приложением через командную строку	118

Управление приложением через Kaspersky Security Center

Kaspersky Security Center позволяет вам удаленно и централизованно управлять работой приложения Kaspersky Industrial CyberSecurity for Linux Nodes на клиентских устройствах. Вы можете удаленно устанавливать и удалять, запускать и останавливать приложение Kaspersky Industrial CyberSecurity for Linux Nodes; настраивать параметры работы приложения, отдельных компонентов и задач приложения; запускать и останавливать задачи на управляемых устройствах.

Для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Kaspersky Security Center вы можете использовать следующие консоли управления Kaspersky Security Center:

- Консоль администрирования Kaspersky Security Center (далее также "Консоль администрирования"). Представляет собой оснастку к Microsoft Management Console (MMC), которая устанавливается на рабочее место администратора и предоставляет пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

Интерфейс для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Консоль администрирования Kaspersky Security Center обеспечивает mmc-плагин управления (см. раздел "О плагинах управления Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [99](#)) для Консоли администрирования на основе MMC (далее также "mmc-плагин").

В этой справке описание работы с Консолью администрирования приведено для версии Kaspersky Security Center 14.2 Windows.

- Kaspersky Security Center Web Console (далее также "Web Console"). Представляет собой веб-интерфейс для управления системой защиты, построенной на основе приложений "Лаборатории Касперского". Вы можете работать в Kaspersky Security Center Web Console через браузер на любом устройстве, которое имеет доступ к Серверу администрирования.

Интерфейс для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Kaspersky Security Center Web Console обеспечивает веб-плагин управления (см. раздел "О плагинах управления Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [99](#)) (далее также "веб-плагин").

В этой справке описание работы с Web Console приведено для версии Kaspersky Security Center 15.1 Linux.

Ммс-плагин и веб-плагин позволяют создавать в Kaspersky Security Center политики и задачи для управления работой приложения Kaspersky Industrial CyberSecurity for Linux Nodes:

- *Политика* – это набор параметров, который применяется на всех устройствах группы администрирования. С помощью политик вы можете устанавливать одинаковые значения параметров приложения для всех клиентских устройств, входящих в состав группы администрирования.

Политика Kaspersky Industrial CyberSecurity for Linux Nodes определяет общие параметры работы приложения Kaspersky Industrial CyberSecurity for Linux Nodes и параметры работы отдельных функциональных компонентов приложения на устройствах, где применяется политика.

- *Задачи* для Kaspersky Industrial CyberSecurity for Linux Nodes, созданные в Kaspersky Security Center, выполняются на защищаемых устройствах и реализуют такие функции Kaspersky Industrial CyberSecurity for Linux Nodes, как проверка по требованию, активация приложения, обновление баз и модулей приложения.

В Kaspersky Security Center вы можете создавать как задачи, которые должны выполняться на отдельном устройстве (локальные задачи), так и задачи для всех устройств группы администрирования (групповые задачи) или задачи для произвольной выборки устройств (задачи для наборов устройств).

Независимо от консоли управления Kaspersky Security Center, которую вы используете, чтобы управлять через Kaspersky Security Center работой приложения Kaspersky Industrial CyberSecurity for Linux Nodes, установленного на устройствах, вам нужно поместить эти устройства в группы администрирования. Вы можете создать группы администрирования в Kaspersky Security Center перед началом установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes и настроить правила автоматического перемещения устройств в группы администрирования. Или вы можете вручную переместить устройства в группы администрирования после установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes (см. подробнее в документации Kaspersky Security Center).

В этом разделе

О плагинах управления Kaspersky Industrial CyberSecurity for Linux Nodes	99
О политиках Kaspersky Security Center	99
О задачах для Kaspersky Industrial CyberSecurity for Linux Nodes, созданных в Kaspersky Security Center	100
Вход и выход из Web Console	101
Управление политиками в Web Console	102
Управление политиками в Консоли администрирования	107
Управление задачами в Web Console	112
Управление задачами в Консоли администрирования	115

О плагинах управления Kaspersky Industrial CyberSecurity for Linux Nodes

Для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Kaspersky Security Center требуются следующие плагины управления:

- Веб-плагин управления Kaspersky Industrial CyberSecurity for Linux Nodes (далее также *веб-плагин*) обеспечивает взаимодействие приложения Kaspersky Industrial CyberSecurity for Linux Nodes с приложением Kaspersky Security Center через Kaspersky Security Center Web Console.
Веб-плагин требуется установить (см. раздел "Установка веб-плагина Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [32](#)) на устройство с установленным приложением Kaspersky Security Center Web Console. Управление приложением Kaspersky Industrial CyberSecurity for Linux Nodes с помощью веб-плагина доступно всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console в браузере.
- Ммс-плагин управления Kaspersky Industrial CyberSecurity for Linux Nodes (далее также *ммс-плагин*) обеспечивает взаимодействие приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Security Center через Консоль администрирования.

Ммс-плагин требуется установить (см. раздел "Установка ммс-плагина Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [33](#)) на устройство с установленной Консолью администрирования Kaspersky Security Center.

Плагины управления Kaspersky Industrial CyberSecurity for Linux Nodes позволяют управлять приложением Kaspersky Industrial CyberSecurity for Linux Nodes с помощью политик (см. раздел "О политиках Kaspersky Security Center" на стр. [99](#)) и задач (см. раздел "О задачах для Kaspersky Industrial CyberSecurity for Linux Nodes, созданных в Kaspersky Security Center" на стр. [100](#)).

Дополнительная информация о плагинах управления приведена в документации Kaspersky Security Center.

О политиках Kaspersky Security Center

Политика – это набор параметров приложения Kaspersky Industrial CyberSecurity for Linux Nodes, которые применяются для всех клиентских устройств, входящих в состав группы администрирования.

Для одного приложения вы можете настроить несколько политик с различными значениями параметров. Однако одновременно для приложения может быть активна только одна политика в пределах группы

администрирования. При создании новой политики все остальные политики в группе администрирования становятся неактивными. Вы можете изменить статус политики позже.

Политики, как и группы администрирования, имеют иерархию. По умолчанию дочерняя политика наследует параметры родительской политики. *Дочерняя политика* – это политика вложенного уровня иерархии, то есть политика для вложенных групп администрирования и подчиненных Серверов администрирования. Вы можете выключить наследование параметров из родительской политики.

Вы можете локально изменять значения параметров, заданные политикой, для отдельных устройств в группе администрирования, если изменение этих параметров не запрещено политикой.

Использование профилей политик позволяет более гибко настроить параметры работы приложения. *Профиль политики* может содержать параметры, которые отличаются от параметров "базовой" политики и применяются на клиентских устройствах при выполнении настроенных вами условий (правил активации). Использование профилей политики позволяет более гибко настроить параметры работы на разных устройствах. Вы можете создавать и настраивать профили в свойствах политики в разделе **Профили политики**.

Каждый параметр политики имеет атрибут "замок", который показывает, наложен ли запрет на изменение параметров в дочерних политиках и локально в параметрах приложения. Возможность изменять параметр приложения на клиентском устройстве определяется статусом "замка" у параметра в свойствах политики:

- Если параметр закрыт "замком" (🔒), это означает, что вы не можете изменить значение параметра локально или в политиках вложенного уровня иерархии. Для всех клиентских устройств группы администрирования и вложенных групп используется значение параметра, заданное этой политикой.
- Если параметр не закрыт "замком" (🔓), это означает, что вы можете изменить значение параметра локально или в политиках вложенного уровня иерархии. Если для клиентских устройств группы администрирования значения параметра заданы локально или в политиках вложенного уровня иерархии, то значение параметра, заданное в свойствах политики, не применяется.

В веб-плагине и mms-плагине количество параметров с "замками" отличается. В веб-плагине присутствуют "замки", которых нет в mms-плагине.

Параметры работы приложения изменяются в соответствии с параметрами политики после первого применения политики.

Подробнее о политиках и профилях политик см. в справке Kaspersky Security Center.

О задачах для Kaspersky Industrial CyberSecurity for Linux Nodes, созданных в Kaspersky Security Center

Вы можете создавать в Kaspersky Security Center задачи следующих типов для приложения Kaspersky Industrial CyberSecurity for Linux Nodes:

- локальные задачи для выполнения на отдельных устройствах;
- групповые задачи для выполнения на устройствах, входящих в группу администрирования;
- задачи для наборов устройств для выполнения на нескольких устройствах, независимо от их вхождения в группы администрирования.

Задачи для наборов устройств выполняются только на устройствах, указанных в параметрах задачи. Если в выборку устройств, для которой сформирована задача, добавлены новые устройства, то для них эта задача не выполняется. В этом случае вам нужно создать новую задачу или изменить параметры уже существующей задачи.

Вы можете создавать любое количество групповых задач, задач для наборов устройств и локальных задач.

Задачи выполняются, только если на устройствах запущено приложение Kaspersky Industrial CyberSecurity for Linux Nodes.

Общая информация о задачах, созданных в Kaspersky Security Center, приведена в документации Kaspersky Security Center.

Для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes в Kaspersky Security Center предусмотрены следующие задачи:

- **Поиск вредоносного ПО** (на стр. [225](#)). Во время выполнения задачи приложение проверяет области устройства, указанные в параметрах задачи, на вирусы и другие вредоносные программы.
- **Проверка важных областей** (на стр. [274](#)). Во время выполнения задачи приложение проверяет загрузочные секторы, объекты автозапуска, память процессов и память ядра.
- **Проверка контейнеров** (см. раздел "**Проверка контейнеров и образов по требованию**" на стр. [328](#)). Во время выполнения задачи приложение проверяет контейнеры и образы на вирусы и другие вредоносные программы.
- **Инвентаризация** (на стр. [450](#)). Во время выполнения задачи приложение получает информацию обо всех исполняемых файлах приложений, хранящихся на устройствах.
- **Проверка целостности системы** (на стр. [528](#)). Во время выполнения задачи приложение определяет изменение каждого объекта путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.
- **Добавление ключа** (см. раздел "**Активация приложения с помощью Kaspersky Security Center**" на стр. [49](#)). Во время выполнения задачи приложение добавляет ключ, в том числе резервный, для активации приложения.
- **Обновление**. Во время выполнения задачи приложение обновляет базы в соответствии с настроенными параметрами обновления.
- **Откат обновления баз** (см. раздел "**Откат обновления баз и модулей приложения**" на стр. [170](#)). Во время выполнения задачи приложение откатывает последнее обновление баз.

Вход и выход из Web Console

Для входа в Web Console вам нужно знать веб-адрес Сервера администрирования и номер порта, указанные во время установки Web Console (по умолчанию используется порт 8080). Также требуется включить JavaScript в браузере.

► *Чтобы войти в Web Console:*

1. В браузере перейдите по адресу `<веб-адрес Сервера администрирования>:<номер порта>`.

Откроется страница входа.

2. Введите имя пользователя и пароль вашей учетной записи.

Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев.

3. Нажмите на кнопку **Войти**.

Если Сервер администрирования не отвечает или вы указали неверные учетные данные, отобразится сообщение об ошибке.

После входа отобразится панель мониторинга (dashboard) с последними использованными языком и темой.

Подробнее об интерфейсе Web Console см. в документации Kaspersky Security Center.

► Чтобы выйти из Web Console:

в левом нижнем углу экрана выберите **<Имя учетной записи> → Выход**.

Web Console закроется и отобразится страница входа.

Управление политиками в Web Console

Вы можете выполнять следующие действия с политиками в Web Console:

- Создавать (см. раздел "Создание политики в Web Console" на стр. [103](#)) политику.
- Изменять (см. раздел "Изменение параметров политики в Web Console" на стр. [104](#)) параметры политики (см. раздел "Параметры политики в Web Console" на стр. [104](#)).

Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Экспортировать и импортировать параметры политики.
- Копировать и перемещать политику.
- Удалять политику.
- Изменять статус политики.
- Создавать профили политики.

Общую информацию о работе с политиками см. в справке Kaspersky Security Center.

В этом разделе

Создание политики в Web Console	103
Изменение параметров политики в Web Console	104
Параметры политики в Web Console	104

Создание политики в Web Console

► Чтобы создать политику в Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.
Откроется список политик и профилей политик.
2. Выберите группу администрирования, содержащую устройства, на которых должна применяться политика. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите группу администрирования в открывшемся окне.
3. Нажмите на кнопку **Добавить**.
Запустится мастер создания политики.
4. В открывшемся окне в списке выберите **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5**.
Перейдите к следующему шагу мастера.
5. Примите решение об использовании Kaspersky Security Network. Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:
 - Если вы согласны со всеми пунктами Положения и хотите использовать Kaspersky Security Network в работе приложения, выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.
 - Если вы не хотите принимать использовать Kaspersky Security Network, выберите вариант **Я не принимаю условия Положения о Kaspersky Security Network** и подтвердите свое решение в открывшемся окне.

Отказ от использования Kaspersky Security Network не прерывает процесс создания политики. Вы можете в любой момент включить, выключить использование Kaspersky Security Network или изменить режим Kaspersky Security Network для управляемых устройств в параметрах политики.

Перейдите к следующему шагу мастера.

6. Откроется окно параметров созданной политики на закладке **Общие**. Укажите название новой политики.

Вы также можете настроить следующие параметры политики:

- **Состояние политики:**
 - **Активна.** Политика, которая применяется к устройству в настоящий момент. Если выбран этот вариант, при следующей синхронизации устройства с Сервером администрирования эта политика станет активной на устройстве. Этот вариант выбран по умолчанию.
 - **Неактивна.** Политика, которая в настоящее время не применяется к устройству. Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. Позже вы можете активировать неактивную политику.
- **Наследование параметров политики:**
 - **Наследовать параметры родительской политики.** Если переключатель включен, значения параметров политики наследуются из групповой политики верхнего уровня и, следовательно, недоступны для изменения. По умолчанию переключатель включен.
 - **Обеспечить принудительное наследование параметров для дочерних политик.** Если переключатель включен, значения параметров дочерних политик недоступны для изменения. По умолчанию переключатель выключен.

Общая информация о параметрах политик приведена в справке Kaspersky Security Center.

7. Если вы хотите настроить другие параметры политики (см. раздел "Параметры политики в Web Console" на стр. [104](#)), перейдите на закладку **Параметры приложения** и внесите необходимые изменения.

Вы также можете изменить параметры политики (см. раздел "Изменение параметров политики в Web Console" на стр. [104](#)) позже.

8. Нажмите на кнопку **Сохранить**.

Созданная политика появится в списке политик.

Общую информацию об управлении политиками см. в справке Kaspersky Security Center.

Изменение параметров политики в Web Console

► *Чтобы изменить параметры политики в Web Console:*

1. В главном окне Web Console выберите **Активы (Устройства) → Политики и профили политик**.
Откроется список политик.
2. Выберите группу администрирования, содержащую устройства, на которых применяется политика. Для этого нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите группу администрирования в открывшемся окне.
В списке отобразятся политики, настроенные для выбранной группы администрирования.
3. Нажмите на название нужной политики в списке.
Откроется окно свойств политики.
4. Измените параметры политики (см. раздел "Параметры политики в Web Console" на стр. [104](#)) на закладке **Параметры приложения**.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Политика будет сохранена с обновленными параметрами.

Параметры политики в Web Console

Вы можете настраивать параметры политики на закладке **Параметры приложения** окна свойств политики.

Таблица 5. Параметры политики

Раздел	Подразделы
Базовая защита	Защита от файловых угроз (см. раздел "Настройка защиты от файловых угроз в Web Console" на стр. 173) Исключения Защиты от файловых угроз (на стр. 182) Управление сетевым экраном (см. раздел "Управление сетевым экраном в Web Console" на стр. 359) Защита от веб-угроз (см. раздел "Настройка защиты от веб-угроз в Web Console" на стр. 379) Защита от сетевых угроз (см. раздел "Настройка защиты от сетевых угроз в Web Console" на стр. 399)
Продвинутая защита	Kaspersky Security Network Защита от шифрования (см. раздел "Настройка защиты от шифрования в Web Console" на стр. 405) Анализ поведения (см. раздел "Настройка анализа поведения в Web Console" на стр. 544)
Detection and Response	Managed Detection and Response Endpoint Detection and Response Optimum (см. раздел "Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console" на стр. 614) Интеграция с KICS for Networks (см. раздел "Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в Web Console" на стр. 594)
Контроль безопасности	Контроль приложений (см. раздел "Настройка контроля приложений в Web Console" на стр. 433) Контроль устройств (см. раздел "Настройка контроля устройств в Web Console" на стр. 466) Контроль целостности системы (см. раздел "Настройка контроля целостности системы в Web Console" на стр. 517) Веб-Контроль (см. раздел "Настройка Веб-Контроля в Web Console" на стр. 491)
Локальные задачи	Управление задачами (см. раздел "Настройка разрешений на управление задачами" на стр. 584) Проверка съемных дисков (см. раздел "Настройка проверки съемных дисков в Web Console" на стр. 314)

Раздел	Подразделы
Общие параметры	Параметры прокси-сервера (см. раздел "Настройка параметров прокси-сервера в Web Console" на стр. 560) Параметры приложения (см. раздел "Дополнительные параметры работы приложения" на стр. 559) Параметры проверки контейнеров (см. раздел "Настройка мониторинга контейнеров в Web Console" на стр. 323) Параметры сети (см. раздел "Настройка проверки защищенных соединений в Web Console" на стр. 388) Глобальные исключения (см. раздел "Настройка глобальных исключений в Web Console" на стр. 567) Параметры Хранилища (см. раздел "Настройка параметров резервного хранилища в Web Console" на стр. 587)

Управление политиками в Консоли администрирования

Вы можете выполнять следующие действия с политиками в Консоли администрирования Kaspersky Security Center:

- Создавать (см. раздел "Создание политики с помощью Консоли администрирования" на стр. [108](#)) политику.
- Изменять (см. раздел "Изменение параметров политики в Консоли администрирования Kaspersky Security Center" на стр. [109](#)) параметры политики (см. раздел "Параметры политики в Консоли администрирования" на стр. [109](#)).

Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Экспортировать и импортировать параметры политики.
- Удалять политику.
- Изменять статус политики.
- Создавать профили политики.

Общую информацию о работе с политиками см. в справке Kaspersky Security Center.

В этом разделе

Создание политики с помощью Консоли администрирования	108
Изменение параметров политики в Консоли администрирования Kaspersky Security Center.....	109
Параметры политики в Консоли администрирования	109

Создание политики с помощью Консоли администрирования

► Чтобы создать политику в Консоли администрирования:

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, содержащую устройства, на которых должна применяться политика.
На закладке **Устройства** папки с названием группы администрирования вы можете просмотреть список устройств, которые входят в состав этой группы администрирования.
2. В рабочей области выберите закладку **Политики**.
3. Нажмите на кнопку **Новая политика**, чтобы запустить мастер создания политики.
Вы также можете запустить мастер с помощью пункта **Создать** → **Политику** контекстного меню в списке политик.
4. На первом шаге мастера в списке выберите **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5**.
Перейдите к следующему шагу мастера.
5. Введите название новой политики.
6. Если вы хотите перенести в создаваемую политику параметры из политики предыдущей версии приложения Kaspersky Industrial CyberSecurity for Linux Nodes, установите флажок **Использовать параметры политики для предыдущей версии программы**.
Перейдите к следующему шагу мастера.
7. Примите решение об использовании Kaspersky Security Network. Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:
 - Если вы согласны со всеми пунктами Положения и хотите использовать Kaspersky Security Network в работе приложения, выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.
 - Если вы не хотите использовать Kaspersky Security Network, выберите вариант **Я не принимаю условия Положения о Kaspersky Security Network** и подтвердите свое решение в открывшемся окне.

Отказ от использования Kaspersky Security Network не прерывает процесс создания политики. Вы можете в любой момент включить, выключить использование Kaspersky Security Network или изменить режим Kaspersky Security Network для управляемых устройств в параметрах политики.

Перейдите к следующему шагу мастера.
8. Если требуется, настройте основные параметры Защиты от файловых угроз (см. раздел "Настройка защиты от файловых угроз в Консоли администрирования" на стр. [190](#)).
Перейдите к следующему шагу мастера.
9. Если требуется, измените настроенные по умолчанию параметры защиты от файловых угроз (см. раздел "Окно Параметры проверки" на стр. [196](#)).
Перейдите к следующему шагу мастера.
10. Если требуется, настройте исключения из защиты от файловых угроз (см. раздел "Исключения Защиты от файловых угроз" на стр. [201](#)).
Перейдите к следующему шагу мастера.
11. Если требуется, измените настроенные по умолчанию действия при обнаружении угрозы (см. раздел "Окно Действие при обнаружении угрозы" на стр. [200](#)).
Перейдите к следующему шагу мастера.

12. Если требуется, настройте параметры интеграции с Kaspersky Industrial CyberSecurity for Networks.

Перейдите к следующему шагу мастера.

13. Завершите работу мастера создания политики.

Созданная политика отобразится в списке политик группы администрирования на закладке **Политики** и в папке **Политики** дерева консоли.

Вы можете изменить параметры политики (см. раздел "Изменение параметров политики в Консоли администрирования Kaspersky Security Center" на стр. [109](#)) позже. Общую информацию об управлении политиками см. в справке Kaspersky Security Center.

Изменение параметров политики в Консоли администрирования Kaspersky Security Center

► *Чтобы изменить параметры политики в Консоли администрирования:*

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.
2. В рабочей области выберите закладку **Политики**.
3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

Вы также можете открыть окно свойств политики с помощью пункта **Свойства** контекстного меню политики или по ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

4. Измените параметры политики (см. раздел "Параметры политики в Консоли администрирования" на стр. [109](#)).
5. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**, чтобы сохранить изменения.

Параметры политики в Консоли администрирования

Вы можете настраивать параметры политики в разделах и подразделах окна свойств политики. О настройке общих параметров политики и параметрах событий см. в справке Kaspersky Security Center.

Таблица 6. Параметры политики

Раздел	Подразделы
Базовая защита	Защита от файловых угроз (см. раздел "Настройка защиты от файловых угроз в Консоли администрирования" на стр. 190) Исключения Защиты от файловых угроз (на стр. 201) Управление сетевым экраном (см. раздел "Управление сетевым экраном в Консоли администрирования" на стр. 364) Защита от веб-угроз (см. раздел "Настройка защиты от веб-угроз в Консоли администрирования" на стр. 381) Защита от сетевых угроз (см. раздел "Настройка защиты от сетевых угроз в Консоли администрирования" на стр. 400)
Продвинутая защита	Kaspersky Security Network Защита от шифрования (см. раздел "Настройка защиты от шифрования в Консоли администрирования" на стр. 414) Анализ поведения (см. раздел "Настройка анализа поведения в Консоли администрирования" на стр. 546)
Detection and Response	Managed Detection and Response Интеграция с KICS for Networks (см. раздел "Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в Консоли администрирования" на стр. 598)
Контроль безопасности	Контроль приложений (см. раздел "Настройка контроля приложений в Консоли администрирования" на стр. 436) Контроль целостности системы (см. раздел "Настройка контроля целостности системы в Консоли администрирования" на стр. 522) Контроль устройств (см. раздел "Настройка контроля устройств в Консоли администрирования" на стр. 471) Веб-Контроль (см. раздел "Настройка Веб-Контроля в Консоли администрирования" на стр. 498)
Локальные задачи	Управление задачами (см. раздел "Настройка разрешений на управление задачами" на стр. 584) Проверка съемных дисков (см. раздел "Настройка проверки съемных дисков в Консоли администрирования" на стр. 316)

Раздел	Подразделы
Общие параметры	Параметры прокси-сервера (см. раздел "Настройка параметров прокси-сервера в Консоли администрирования" на стр. 563) Параметры приложения (см. раздел "Дополнительные параметры работы приложения" на стр. 559) Параметры проверки контейнеров (см. раздел "Настройка мониторинга контейнеров в Консоли администрирования" на стр. 325) Параметры сети (см. раздел "Настройка проверки защищенных соединений в Консоли администрирования" на стр. 391) Глобальные исключения (см. раздел "Настройка глобальных исключений в Консоли администрирования" на стр. 570) Исключение памяти процессов (см. раздел "Исключение памяти процессов из проверки" на стр. 572) Параметры Хранилища (см. раздел "Настройка параметров резервного хранилища в Консоли администрирования" на стр. 587)

Управление задачами в Web Console

Вы можете выполнять следующие действия над задачами для Kaspersky Industrial CyberSecurity for Linux Nodes в Web Console:

- Создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) новые задачи.
- Изменять (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) параметры задач.

Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Запускать, останавливать, приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)) выполнение задач.

Задачу **Обновление** невозможно приостановить и возобновить, ее можно только запустить или остановить.

- Экспортировать и импортировать задачи.
- Удалять задачи.

В списке задач вы можете следить за выполнением задачи: статус задачи и статистику выполнения задачи на устройствах. Также вы можете создать выборку событий для контроля за выполнением задач (**Мониторинг и отчеты** → **Выборки событий**). Дополнительная информация о выборке событий приведена в документации Kaspersky Security Center. Результаты выполнения задач также сохраняются локально на устройстве и в отчетах Kaspersky Security Center.

Общую информацию о работе с задачами см. в справке Kaspersky Security Center.

Если устройство находится под управлением политики, просмотр и управление задачами, созданными в Kaspersky Security Center, могут быть недоступны (см. раздел "Настройка разрешений на управление задачами" на стр. 584) через командную строку или локальный пользовательский интерфейс на устройстве.

В этом разделе

Создание задач в Web Console	113
Изменение параметров задач в Web Console	114
Запуск, остановка, приостановка и возобновление задач в Web Console	115

Создание задач в Web Console

► Чтобы создать задачу в Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.
Откроется список задач.
2. Нажмите на кнопку **Добавить**.
Запустится мастер создания задачи.
3. На первом шаге мастера выполните следующие действия:
 - a. В раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5**.
 - b. В раскрывающемся списке **Тип задачи** выберите тип задачи, которую вы хотите создать.
 - c. В поле **Название задачи** введите название новой задачи.
 - d. В блоке **Устройства, которым будет назначена задача** выберите способ определения области действия задачи. Область действия задачи – это устройства, на которых будет выполняться задача:
 - Выберите вариант **Назначить задачу группе администрирования**, если задача должна выполняться на всех устройствах, входящих в определенную группу администрирования.
 - Выберите вариант **Задать адреса устройств вручную или импортировать из списка**, если задача должна выполняться на указанных устройствах.
 - Выберите вариант **Назначить задачу выборке устройств**, если задача должна выполняться на устройствах, входящих в выборку устройств по предопределенному критерию. О создании выборки устройств см. в справке Kaspersky Security Center.

Перейдите к следующему шагу мастера.
4. В зависимости от выбранного способа определения области действия задачи выполните одно из следующих действий:
 - В дереве групп администрирования установите флажки рядом с нужными группами администрирования.
 - В списке устройств установите флажки рядом с нужными устройствами. Если нужные устройства отсутствуют в списке, вы можете добавить их следующими способами:

- С помощью кнопки **Добавить устройства**. Вы можете добавить устройства по имени или IP-адресу, добавить устройства из указанного IP-диапазона или выбрать устройства из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.
- С помощью кнопки **Импортировать устройства из файла**. Для импорта используется файл формата TXT с перечнем адресов устройств, где каждый адрес должен располагаться в отдельной строке.
- В списке выберите название выборки, содержащей нужные устройства.

Перейдите к следующему шагу мастера.

5. Чтобы настроить параметры задачи (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) сразу после создания, на последнем шаге мастера установите флажок **Открыть окно свойств задачи после ее создания**. Задача создается с параметрами по умолчанию.
6. Завершите работу мастера.

В списке задач отобразится новая задача.

Изменение параметров задач в Web Console

► *Чтобы изменить параметры задачи в Web Console:*

1. В главном окне Web Console выберите **Активы (Устройства) → Задачи**.
Откроется список задач.
2. Выполните одно из следующих действий:
 - Если вы хотите изменить параметры задачи, которая выполняется на всех устройствах, входящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и в открывшемся окне выберите группу администрирования.
В списке отобразятся только задачи, настроенные для выбранной группы администрирования.
 - Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), нажмите на ссылку в поле **Текущий путь** в верхней части окна и в открывшемся окне выберите верхний узел с именем Сервера администрирования.
В списке отобразятся все задачи, созданные на Сервере администрирования.
3. В списке задач выберите нужную задачу и откройте окно свойств задачи по ссылке в названии задачи.
4. Настройте параметры задачи:
 - На закладке **Общие** вы можете изменить название задачи.
 - На закладке **Параметры приложения** вы можете настроить специфические параметры задачи. Наличие настраиваемых параметров зависит от типа задачи.
 - На закладке **Расписание** вы можете настроить расписание запуска задачи и дополнительные параметры запуска и остановки задачи.

Закладки **Общие**, **Результаты**, **Параметры**, **Расписание** и **История ревизий** окна свойств задачи стандартны для Kaspersky Security Center, см. подробнее в справке Kaspersky Security Center.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск, остановка, приостановка и возобновление задач в Web Console

► Чтобы запустить, остановить, приостановить или возобновить задачу в Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Задачи**.
Откроется список задач.
2. Выполните одно из следующих действий:
 - Если вы хотите запустить или остановить задачу, которая выполняется на всех устройствах, входящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и в открывшемся окне выберите группу администрирования.
В списке отобразятся только задачи, созданные для выбранной группы администрирования.
 - Если вы хотите запустить или остановить задачу, которая выполняется на одном или нескольких устройствах (задачу для набора устройств), нажмите на ссылку в поле **Текущий путь** в верхней части окна и в открывшемся окне выберите верхний узел с именем Сервера администрирования.
В списке отобразятся все задачи, созданные на Сервере администрирования.
3. В списке задач установите флажок рядом с названием нужной задачи и нажмите на кнопку нужного действия над списком задач.

Управление задачами в Консоли администрирования

Вы можете выполнять следующие действия над задачами для Kaspersky Industrial CyberSecurity for Linux Nodes в Консоли администрирования:

- Создавать (см. раздел "Создание задач в Консоли администрирования" на стр. [116](#)) новые задачи.
- Изменять (см. раздел "Изменение параметров задач в Консоли администрирования" на стр. [117](#)) параметры задач.

Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Запускать, останавливать, приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление задач в Консоли администрирования" на стр. [117](#)) выполнение задач.

Задачу **Обновление** невозможно приостановить и возобновить, ее можно только запустить или остановить.

- Экспортировать и импортировать задачи.
- Удалять задачи.

В списке задач вы можете следить за выполнением задачи: статус задачи и статистику выполнения задачи на устройствах.

Информацию о ходе и результатах выполнения задач вы можете посмотреть в списке событий, которые приложение Kaspersky Industrial CyberSecurity for Linux Nodes отправляет на Сервер администрирования Kaspersky Security Center (на закладке **События** в рабочей области узла **Сервер администрирования**

<имя сервера>). Также вы можете создать выборку событий для контроля за выполнением задач. Дополнительная информация о выборке событий приведена в документации Kaspersky Security Center.

Результаты выполнения задач также сохраняются локально на устройстве и в отчетах Kaspersky Security Center.

Общую информацию о работе с задачами см. в справке Kaspersky Security Center.

Если устройство находится под управлением политики, просмотр и управление задачами, созданными в Kaspersky Security Center, могут быть недоступны (см. раздел "Настройка разрешений на управление задачами" на стр. 584) через командную строку или локальный пользовательский интерфейс на устройстве.

В этом разделе

Создание задач в Консоли администрирования	116
Изменение параметров задач в Консоли администрирования	117
Запуск, остановка, приостановка и возобновление задач в Консоли администрирования	117

Создание задач в Консоли администрирования

► Чтобы создать задачу в Консоли администрирования:

- В Консоли администрирования выполните одно из следующих действий:
 - Если вы хотите создать задачу, которая будет выполняться на устройствах, входящих в выбранную группу администрирования, в дереве консоли в папке **Управляемые устройства** выберите эту группу администрирования, затем в рабочей области выберите закладку **Задачи** и нажмите на кнопку **Новая задача**.
Запустится мастер создания задачи для устройств выбранной группы администрирования.
 - Если вы хотите создать задачу, которая будет выполняться на одном или нескольких устройствах (задачу для набора устройств), в дереве консоли выберите папку **Задачи** и нажмите на кнопку **Новая задача** в рабочей области.
Запустится мастер создания задачи для набора устройств.
- На первом шаге мастера выберите **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5** и тип задачи.
Перейдите к следующему шагу мастера.
- Если вы создаете задачу для набора устройств, мастер предложит определить область действия задачи. Область действия задачи – это устройства, на которых будет выполняться задача.
 - Укажите способ определения области действия задачи: выбрать устройства из списка устройств, обнаруженных Сервером администрирования; задать адреса устройств вручную; импортировать список устройств из файла или указать ранее настроенную выборку устройств (см. подробнее в справке Kaspersky Security Center).
 - В зависимости от указанного вами способа определения области действия в открывшемся окне выполните одно из следующих действий:

- В списке обнаруженных устройств укажите устройства, на которых будет выполняться задача. Для этого установите флажок в списке слева от названия устройства.
- Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса устройств вручную.
- Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов устройств.
- Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей устройства, на которых будет выполняться задача.

Перейдите к следующему шагу мастера.

4. Настройте доступные параметры задачи, следуя указаниям мастера.
5. Введите название новой задачи и перейдите к следующему шагу мастера.
6. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера, на последнем шаге установите флажок **Запустить задачу после завершения работы мастера**.
7. Завершите работу мастера.

В списке задач отобразится новая задача.

Изменение параметров задач в Консоли администрирования

► *Чтобы изменить параметры задачи в Консоли администрирования:*

1. В Консоли администрирования выполните одно из следующих действий:
 - Если вы хотите изменить параметры задачи, которая выполняется на устройствах, входящих в определенную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите закладку **Задачи**.
 - Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), в дереве консоли выберите папку **Задачи**.
2. В списке задач выберите нужную задачу и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.

Вы также можете открыть окно свойств задачи с помощью пункта **Свойства** контекстного меню задачи.
3. Измените параметры задачи. Наличие настраиваемых параметров зависит от типа задачи.

Закладки **Общие**, **Уведомление**, **Расписание** и **История ревизий** окна свойств задачи стандартны для Kaspersky Security Center, см. подробнее в справке Kaspersky Security Center.
4. Нажмите на кнопку **Применить** или на кнопку **ОК** в окне **Свойства: <Название задачи>**, чтобы сохранить внесенные изменения.

Запуск, остановка, приостановка и возобновление задач в Консоли администрирования

► *Чтобы запустить, остановить, приостановить или возобновить задачу в Консоли администрирования:*

1. В Консоли администрирования выполните одно из следующих действий:

- Если вы хотите запустить или остановить задачу, которая выполняется на устройствах, входящих в определенную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите закладку **Задачи**.
Откроется список задач, созданных для выбранной группы администрирования.
 - Если вы хотите запустить или остановить задачу, которая выполняется на одном или нескольких устройствах (задачу для набора устройств), в дереве консоли выберите папку **Задачи**.
Откроется список всех задачи, созданных на Сервере администрирования.
2. В списке задач выберите нужную задачу, откройте контекстное меню задачи и выберите действие, которое вы хотите выполнить.

Управление приложением через командную строку

С помощью командной строки вы можете устанавливать и удалять, запускать и останавливать приложение Kaspersky Industrial CyberSecurity for Linux Nodes на устройстве, а также локально управлять работой приложения.

Работу функциональных компонентов приложения обеспечивают *локальные задачи* Kaspersky Industrial CyberSecurity for Linux Nodes (см. раздел "Управление задачами в командной строке" на стр. [119](#)), которые выполняются в операционной системе. Вы можете включать и выключать функциональные компоненты приложения на устройстве путем запуска и остановки задач Kaspersky Industrial CyberSecurity for Linux Nodes в командной строке. Однократные проверки устройства также выполняются путем запуска задач Kaspersky Industrial CyberSecurity for Linux Nodes. Вы можете задавать параметры работы функциональных компонентов на устройстве и параметры проверки устройства, настраивая *параметры задач* Kaspersky Industrial CyberSecurity for Linux Nodes.

Помимо параметров задач для настройки работы приложения предусмотрены следующие параметры:

- Общие параметры проверки контейнеров (на стр. [728](#)).
- Параметры проверки защищенных соединений (на стр. [731](#)).
- Общие параметры приложения, которые определяют работу приложения в целом и работу отдельных функций.

Управление приложением Kaspersky Industrial CyberSecurity for Linux Nodes в командной строке выполняется с помощью *команд управления* Kaspersky Industrial CyberSecurity for Linux Nodes (см. раздел "Приложение 2. Команды управления Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [676](#)).

В этом разделе

Включение автоматического дополнения команды kics-control (bash completion).....	119
Управление задачами в командной строке	119
Вывод параметров задачи в командной строке.....	129
Изменение параметров задачи в командной строке	129
Настройка расписания задачи в командной строке.....	135
Управление общими параметрами приложения в командной строке	137
Использование фильтра для ограничения результатов запросов.....	140
Экспорт и импорт параметров приложения	142

Включение автоматического дополнения команды kics-control (bash completion)

Для оболочки bash есть возможность включить автоматическое дополнение команды kics-control.

- Чтобы включить автоматическое дополнение команды kics-control в текущей сессии оболочки bash, выполните следующую команду:

```
source /opt/kaspersky/kics/shared/bash_completion.sh
```

- Чтобы включить автоматическое дополнение для всех новых сессий оболочки bash, выполните следующую команду:

```
echo "source /opt/kaspersky/kics/shared/bash_completion.sh" >> ~/.bashrc
```

Управление задачами в командной строке

Для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes с помощью командной строки предусмотрены следующие задачи приложения:

- **Защита от файловых угроз.** Эта задача позволяет включать и выключать защиту от файловых угроз (см. раздел "Защита от файловых угроз" на стр. [172](#)) в реальном времени и определяет параметры компонента Защита от файловых угроз. Задача запускается автоматически при запуске приложения, если при установке приложения вы выбрали режим работы *Включена только защита от файловых угроз в информирующем режиме* (PROTECTION_MODE=OAS_Notify) или *Включена только защита от файловых угроз* (PROTECTION_MODE=OAS_Block).
- **Поиск вредоносного ПО.** Эта задача позволяет выполнять проверку объектов файловой системы на наличие вредоносного ПО по требованию и определяет параметры проверки. Вы можете использовать эту задачу для полной или выборочной проверки устройств (см. раздел "Поиск вредоносного ПО" на стр. [225](#)).
- **Проверка важных областей.** Эта задача позволяет выполнять проверку важных областей (см. раздел "Проверка важных областей" на стр. [274](#)) операционной системы по требованию и определяет параметры проверки.
- **Выборочная проверка файлов.** Эта задача предназначена для настройки и хранения параметров, которые используются во время проверки файлов и директорий по команде `kics-control --scan-file` (см. раздел "Выборочная проверка файлов и директорий" на стр. [265](#)). В результате выполнения команды приложение создает и запускает временную задачу проверки файлов.
- **Проверка контейнеров.** Эта задача позволяет выполнять проверку контейнеров и образов (см. раздел "Проверка контейнеров и образов по требованию" на стр. [328](#)) по требованию и определяет параметры проверки.
- **Выборочная проверка контейнеров.** Эта задача предназначена для настройки и хранения параметров, которые используются во время проверки указанных контейнеров и образов по команде `kics-control [-T] --scan-container` (см. раздел "Выборочная проверка контейнеров и образов" на стр. [352](#)). В результате выполнения команды приложение создает и запускает временную задачу проверки контейнеров.
- **Проверка съемных дисков.** Эта задача позволяет в реальном времени контролировать подключение съемных дисков (см. раздел "Проверка съемных дисков" на стр. [314](#)) к устройству и определяет параметры проверки съемных дисков и их загрузочных секторов на наличие вредоносного ПО.

- *Защита от веб-угроз.* Эта задача позволяет включать и выключать защиту от веб-угроз и определяет параметры работы компонента Защита от веб-угроз (см. раздел "Защита от веб-угроз" на стр. [378](#)).
- *Защита от сетевых угроз.* Эта задача позволяет включать и выключать защиту от сетевых угроз и определяет параметры работы компонента Защита от сетевых угроз (см. раздел "Защита от сетевых угроз" на стр. [398](#)).
- *Защита от шифрования.* Эта задача позволяет включать и выключать защиту файлов от удаленного вредоносного шифрования (см. раздел "Защита от удаленного вредоносного шифрования" на стр. [404](#)) и определяет параметры компонента Защита от шифрования.
- *Управление сетевым экраном.* Эта задача позволяет включать и выключать управление сетевым экраном и определяет параметры контроля сетевых соединений на устройстве.
- *Контроль приложений.* Эта задача позволяет включать и выключать контроль приложений (на стр. [431](#)) и определяет параметры компонента Контроль приложений.
- *Инвентаризация.* Эта задача позволяет получать информацию обо всех исполняемых файлах (см. раздел "Инвентаризация" на стр. [450](#)) приложений, хранящихся на устройстве.
- *Контроль устройств.* Эта задача позволяет включать и выключать Контроль устройств (на стр. [464](#)) и определяет параметры компонента Контроль устройств.
- *Веб-Контроль.* Эта задача позволяет включать и выключать Веб-Контроль (на стр. [489](#)) и определяет параметры компонента Веб-Контроль.
- *Анализ поведения.* Эта задача позволяет контролировать вредоносную активность приложений (см. раздел "Анализ поведения" на стр. [544](#)) в операционной системе.
- *Контроль целостности системы.* Эта задача позволяет в реальном времени отслеживать действия, выполняемые с объектами из области мониторинга, указанной в параметрах компонента Контроль целостности системы (см. раздел "Контроль целостности системы" на стр. [516](#)).
- *Проверка целостности системы.* Эта задача позволяет проверять (см. раздел "Проверка целостности системы" на стр. [528](#)) наличие изменений в файлах и директориях, которые вы включили в область мониторинга, путем сравнения текущего состояния контролируемого объекта с ранее зафиксированным состоянием.
- *Управление резервным хранилищем.* Эта задача обеспечивает возможность сохранять резервные копии файлов в резервном хранилище (см. раздел "Резервное хранилище" на стр. [586](#)) на устройстве. Задача запускается автоматически при запуске приложения и постоянно находится в оперативной памяти устройства. Задача недоступна для запуска, остановки и удаления.
- *Лицензирование.* Эта задача обеспечивает возможность активировать приложение (см. раздел "Активация приложения и управление лицензионными ключами" на стр. [154](#)), установленное на устройстве. Задача запускается автоматически при запуске приложения и постоянно находится в оперативной памяти устройства. Задача не имеет параметров, управление ключами реализовано с помощью специальных команд управления. Задача недоступна для запуска, остановки и удаления.
- *Обновление.* С помощью этой задачи вы можете выполнять обновление баз и модулей приложения по расписанию и по требованию и настраивать параметры обновления.
- *Откат обновления баз.* С помощью этой задачи вы можете выполнять откат последнего обновления баз и модулей приложения (см. раздел "Откат обновления баз и модулей приложения" на стр. [170](#)).
- *Интеграция с Kaspersky Industrial CyberSecurity for Networks.* Эта задача позволяет включать и выключать интеграцию с приложением Kaspersky Industrial CyberSecurity for Networks (см. раздел "Интеграция с Kaspersky Industrial CyberSecurity for Networks" на стр. [592](#)) и определяет параметры интеграции.

Каждая задача приложения имеет имя, используемое в командной строке, идентификатор и тип (см. таблицу ниже).

Идентификаторы уникальны для всех задач, включая удаленные. Приложение не использует повторно идентификаторы удаленных задач. Идентификатор новой задачи представляет собой номер, следующий по порядку за идентификатором последней созданной задачи.

Имена задач не чувствительны к регистру.

Во время установки приложения создаются *предустановленные задачи*. Эти задачи недоступны для удаления. Для каждой предустановленной задачи зарезервированы имя и идентификатор.

Задачи, которые вы создаете во время работы с приложением, называются *пользовательские задачи*. Имена этих задач вы задаете при создании задачи. Идентификаторы пользовательских задач приложение задает и присваивает задаче при ее создании. Идентификаторы пользовательских задач начинаются со 100.

Во время работы приложение создает *временные задачи проверки*. Имена и идентификаторы временных задач задаются приложением. Временные задачи автоматически удаляются после завершения.

Таблица 7. Задачи приложения

Задача	Имя задачи в командной строке	ID задачи	Тип задачи
Защита от файловых угроз (см. раздел "Параметры задачи Защита от файловых угроз" на стр. 210)	File_Threat_Protection	1	OAS
Поиск вредоносного ПО (см. раздел "Параметры предустановленной задачи Поиск вредоносного ПО" на стр. 255)	Scan_My_Computer	2	ODS
Поиск вредоносного ПО (см. раздел "Параметры предустановленной задачи Поиск вредоносного ПО" на стр. 255) (пользовательская)	задается пользователем	от 100	ODS
Выборочная проверка файлов (см. раздел "Выборочная проверка файлов и директорий" на стр. 265)	Scan_File	3	ODS
Проверка важных областей (см. раздел "Проверка важных областей в командной строке" на стр. 304)	Critical_Areas_Scan	4	ODS
Обновление	Update	6	Update
Обновление (пользовательская)	задается пользователем	от 100	Update
Откат обновления баз (см. раздел "Откат обновления баз и модулей приложения" на стр. 170)	Rollback	7	Rollback
Откат обновления баз (см. раздел "Откат обновления баз и модулей приложения" на стр. 170) (пользовательская)	задается пользователем	от 100	Rollback
Лицензирование	License	9	License
Управление резервным хранилищем (см. раздел "Настройка параметров резервного хранилища в командной строке" на стр. 588)	Backup	10	Backup
Контроль целостности системы (см. раздел "Проверка целостности системы в командной строке" на стр. 539)	System_Integrity_Monitoring	11	OAFIM

Задача	Имя задачи в командной строке	ID задачи	Тип задачи
Контроль целостности системы (см. раздел "Проверка целостности системы в командной строке" на стр. 539) (пользовательская)	задается пользователем	от 100	ODFIM
Управление сетевым экраном (см. раздел "Управление сетевым экраном в командной строке" на стр. 370)	Firewall_Management	12	Firewall
Защита от шифрования (см. раздел "Настройка защиты от шифрования в командной строке" на стр. 423)	Anti_Cryptor	13	AntiCryptor
Защита от веб-угроз (см. раздел "Настройка защиты от веб-угроз в командной строке" на стр. 383)	Web_Threat_Protection	14	WTP
Контроль устройств (см. раздел "Параметры задачи Контроль устройств" на стр. 477)	Device_Control	15	DeviceControl
Проверка съемных дисков (см. раздел "Настройка проверки съемных дисков в командной строке" на стр. 318)	Removable_Drives_Scan	16	RDS
Защита от сетевых угроз (см. раздел "Настройка защиты от сетевых угроз в командной строке" на стр. 401)	Network_Threat_Protection	17	NTP
Проверка контейнеров (см. раздел "Параметры задачи Проверка контейнеров" на стр. 342)	Container_Scan	18	ContainerScan
Проверка контейнеров (см. раздел "Параметры задачи Проверка контейнеров" на стр. 342) (пользовательская)	задается пользователем	от 100	ContainerScan
Выборочная проверка контейнеров (см. раздел "Выборочная проверка контейнеров и образов" на стр. 352)	Custom_Container_Scan	19	ContainerScan

Задача	Имя задачи в командной строке	ID задачи	Тип задачи
Анализ поведения (см. раздел "Настройка анализа поведения в командной строке" на стр. 548)	Behavior_Detection	20	BehaviorDetection
Контроль приложений (см. раздел "Параметры задачи Контроль приложений" на стр. 441)	Application_Control	21	AppControl
Инвентаризация (см. раздел "Параметры задачи Инвентаризация" на стр. 459)	Inventory_Scan	22	InventoryScan
Инвентаризация (см. раздел "Параметры задачи Инвентаризация" на стр. 459) (пользовательская)	задается пользователем	от 100	InventoryScan
Интеграция с Kaspersky Industrial CyberSecurity for Networks (см. раздел "Параметры задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks" на стр. 604)	KICS4Networks_Integration	23	KICS4NetworksIntegration
Веб-Контроль (см. раздел "Параметры задачи Веб-Контроль" на стр. 508)	Web_Control	26	WebControl

Вы можете выполнять следующие действия над задачами:

- Запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) все предустановленные и пользовательские задачи, кроме задач типов *Backup* и *License*.
- Приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачи типов *ODS*, *ODFIM* и *InventoryScan*.
- Создавать (см. раздел "Создание задачи в командной строке" на стр. [127](#)) и удалять (см. раздел "Удаление задачи в командной строке" на стр. [128](#)) пользовательские задачи типов *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*.
- Изменять параметры (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) всех пользовательских задач и всех предустановленных задач, кроме задач типов *Rollback* и *License*.
- Настраивать расписание запуска задач (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)).

В этом разделе

Просмотр списка задач в командной строке	126
Просмотр состояния задачи в командной строке	126
Создание задачи в командной строке	127
Запуск, остановка, приостановка и возобновление задачи в командной строке	128
Удаление задачи в командной строке	128

Просмотр списка задач в командной строке

- Чтобы просмотреть список задач приложения, выполните следующую команду:

```
kics-control --get-task-list [--json]
```

где:

`--json` – формат вывода списка задач приложения. Если вы не укажете формат, вывод будет выполнен в формате INI.

Отобразится список задач приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

Для каждой задачи отображается следующая информация (см. раздел "Управление задачами в командной строке" на стр. [119](#)):

- `Name` – имя задачи.
- `ID` – идентификатор задачи.
- `Type` – тип задачи.
- `State` – текущее состояние (см. раздел "Просмотр состояния задачи в командной строке" на стр. [126](#)) задачи.

Если политика Kaspersky Security Center запрещает пользователям просматривать и изменять задачи локально, отображается информация только о задачах *Scan_File*, *Backup*, *License*, *File_Threat_Protection*, *System_Integrity_Monitoring* и *Anti_Cryptor*. Информация о других задачах недоступна.

Просмотр состояния задачи в командной строке

- Чтобы посмотреть состояние задачи, выполните следующую команду:

```
kics-control --get-task-state <идентификатор/имя задачи> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--json` – выводить параметры в формате JSON.

Для задач приложения предусмотрены следующие основные состояния:

- `Started` – задача запущена.
- `Starting` – задача запускается.
- `Stopped` – задача остановлена.
- `Stopping` – задача останавливается.

Задачи типов *ODS*, *ODFIM* и *InventoryScan* могут также находиться в одном из следующих состояний:

- `Pausing` – приостанавливается;
- `Suspended` – приостановлена;
- `Resuming` – возобновляется.

Создание задачи в командной строке

Вы можете создавать задачи следующих типов (см. раздел "Управление задачами в командной строке" на стр. [119](#)): *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*.

Вы можете создавать задачи с параметрами по умолчанию или с параметрами, указанными в конфигурационном файле.

- Чтобы создать задачу с параметрами по умолчанию, выполните следующую команду:

```
kics-control -create-task <имя задачи> --type <тип задачи>
```

где:

- `<имя задачи>` – имя, которое вы задаете для новой задачи;
- `<тип задачи>` – обозначение типа создаваемой задачи (см. раздел "Управление задачами в командной строке" на стр. [119](#)).

- Чтобы создать задачу с параметрами, указанными в конфигурационном файле, выполните следующую команду:

```
kics-control --create-task <имя задачи> --type <тип задачи> --file <путь к конфигурационному файлу> [--json]
```

где:

- `<имя задачи>` – имя, которое вы задаете для новой задачи;
- `<тип задачи>` – обозначение типа создаваемой задачи (см. раздел "Управление задачами в командной строке" на стр. [119](#));
- `<путь к файлу>` – полный путь к конфигурационному файлу (см. раздел "Параметры задач командной строки по умолчанию" на стр. [711](#)), параметры из которого будут использоваться при создании задачи;
- `--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Запуск, остановка, приостановка и возобновление задачи в командной строке

Вы можете запускать и останавливать предустановленные и пользовательские задачи, кроме задач типов (см. раздел "Управление задачами в командной строке" на стр. [119](#)) *Backup* и *License*.

Вы можете приостанавливать и возобновлять задачи типов *ODS*, *ODFIM* и *InventoryScan*.

► Чтобы запустить задачу, выполните следующую команду:

```
kics-control --start-task <идентификатор/имя задачи> [-W] [--progress]
```

где:

- **<идентификатор/имя задачи>** – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- **[-W]** – используйте эту команду совместно с командой запуска задачи, если вы хотите включить вывод текущих событий, связанных с этой задачей.
- **[--progress]** – укажите этот ключ, если вы хотите отображать ход выполнения задачи.

Пример:

Запустить задачу с идентификатором 1 и включить вывод текущих событий, связанных с задачей:

```
kics-control --start-task 1 -W
```

► Чтобы остановить задачу, выполните следующую команду:

```
kics-control --stop-task <идентификатор/имя задачи> [-W]
```

где:

- **<идентификатор/имя задачи>** – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- **[-W]** – используйте эту команду совместно с командой остановки задачи, если вы хотите включить вывод текущих событий, связанных с этой задачей.

► Чтобы приостановить задачу, выполните следующую команду:

```
kics-control --suspend-task <идентификатор/имя задачи>
```

► Чтобы возобновить задачу, выполните следующую команду:

```
kics-control --resume-task <идентификатор/имя задачи>
```

Удаление задачи в командной строке

Вы можете удалять только пользовательские задачи. Предустановленные задачи (см. раздел "Управление задачами в командной строке" на стр. [119](#)) недоступны для удаления.

- Чтобы удалить задачу, выполните следующую команду:

```
kics-control --delete-task <идентификатор/имя задачи>
```

где <идентификатор/имя задачи> – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

Вывод параметров задачи в командной строке

Вы можете выводить текущие значения параметров всех пользовательских задач и всех предустановленных задач, кроме задач *Rollback* и *License* (эти задачи не имеют параметров).

Вы можете выводить текущие значения параметров задачи в консоль или в конфигурационный файл, который вы можете использовать (см. раздел "Изменение параметров задачи с помощью конфигурационного файла" на стр. [130](#)) для изменения параметров задачи.

- Чтобы вывести в консоль текущие значения параметров задачи, выполните следующую команду:

```
kics-control --get-settings <идентификатор/имя задачи> [--json]
```

где:

- <идентификатор/имя задачи> – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

- Чтобы вывести в конфигурационный файл текущие значения параметров задачи, выполните следующую команду:

```
kics-control --get-settings <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

где:

- <идентификатор/имя задачи> – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены параметры задачи. Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанной директории не существует, конфигурационный файл не будет создан.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Изменение параметров задачи в командной строке

Вы можете изменять параметры всех пользовательских задач и всех предустановленных задач, кроме задач *Rollback* и *License*.

В командной строке вы можете изменять параметры задач с помощью команды `kics-control --set-settings`:

- Вы можете изменять все параметры задачи (см. раздел "Изменение параметров задачи с помощью конфигурационного файла" на стр. [130](#)), используя конфигурационный файл, который содержит параметры задачи. Конфигурационный файл вы можете получить с помощью команды вывода параметров задачи (см. раздел "Вывод параметров задачи в командной строке" на стр. [129](#)).
- Вы можете изменять отдельные параметры задачи (см. раздел "Изменение параметров задачи с помощью ключей командной строки" на стр. [132](#)), используя ключи командной строки в формате `<имя параметра>=<значение параметра>`. Текущие значения параметров задачи вы можете получить с помощью команды вывода параметров задачи (см. раздел "Вывод параметров задачи в командной строке" на стр. [129](#)).
- Вы можете восстанавливать заданные по умолчанию параметры (см. раздел "Восстановление параметров задачи по умолчанию в командной строке" на стр. [134](#)) задачи.

Вы можете добавлять и удалять области проверки и области исключения используя конфигурационный файл, который содержит параметры задачи, или ключи командной строки. Настройка областей проверки и областей исключения доступна для задач с типами *OAS*, *ODS*, *OAFIM*, *ODFIM* и *AntiCryptor*.

В системах с файловой системой *btfs* и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе *SUSE/OpenSUSE* в качестве пути для исключения вы можете указать `/.snapshots/*/snapshot/`.

Для некоторых задач также предусмотрены отдельные команды управления (см. раздел "Приложение 2. Команды управления Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [676](#)), которые позволяют изменять параметры задач.

В этом разделе

Изменение параметров задачи с помощью конфигурационного файла	130
Изменение параметров задачи с помощью ключей командной строки.....	132
Восстановление параметров задачи по умолчанию в командной строке	134

Изменение параметров задачи с помощью конфигурационного файла

► Чтобы изменить значения параметров задачи с помощью конфигурационного файла:

1. Выведите параметры задачи в конфигурационный файл (см. раздел "Вывод параметров задачи в командной строке" на стр. [129](#)) с помощью команды `kics-control --get-settings`.
2. Откройте конфигурационный файл и измените значения нужных параметров.

Для задач типа (см. раздел "Управление задачами в командной строке" на стр. [119](#)) *OAS*, *ODS*, *OAFIM*, *ODFIM* и *AntiCryptor* вы можете добавлять или удалять области проверки и области исключения.

Если вы хотите добавить область проверки, добавьте в файл секцию `[ScanScope.item_#]` со следующими параметрами:

- `AreaDesc` – описание области проверки, содержащее дополнительную информацию об этой области.
- `UseScanArea` – включить проверку указанной области.
- `Path` – путь к директории с проверяемыми объектами. Вы можете указывать путь к локальной директории или включать проверку удаленных директорий, смонтированных на клиентском устройстве.
- `AreaMask.item_#` – ограничение области проверки. Вы можете указать маску имени файлов, которые нужно проверять. По умолчанию проверка включена для всех объектов области проверки. Вы можете указать несколько элементов `AreaMask.item_#`.

Если вы хотите добавить область исключения, добавьте в файл секцию `[ExcludedFromScanScope.item_#]` со следующими параметрами:

- `AreaDesc` – описание области исключения, содержащее дополнительную информацию об области исключения.
- `UseScanArea` – включить исключение указанной области.
- `Path` – путь к директории с исключаемыми объектами. Вы можете указывать путь к локальной директории или исключать удаленные директории, смонтированные на клиентском устройстве. Возможные значения параметра зависят от типа задачи.
- `AreaMask.item_#` – ограничение области исключения. Вы можете указать маску имени файлов, которые вы хотите исключить из области проверки. По умолчанию исключаются все объекты области.

Пример:

```
[ExcludedFromScanScope.item_0000]

AreaDesc=

UseScanArea=Yes

Path=/tmp/notchecked

AreaMask.item_0000=*
```

Вы можете указать несколько секций `[ScanScope.item_#]` и `[ExcludedFromScanScope.item_#]`. Приложение будет обрабатывать области по индексу в порядке возрастания.

3. Сохраните конфигурационный файл.
4. Выполните команду:

```
kics-control --set-settings <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры задачи.

- `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения параметров задачи, заданные в файле, будут импортированы в приложение.

Если в параметрах задачи Контроль приложений (на стр. 431) вы меняете разрешающий список или запрещаете запуск всех приложений и/или приложений, влияющих на работу приложения Kaspersky Industrial CyberSecurity for Linux Nodes, требуется запускать команду `--set-settings` с ключом `--accept`.

Изменение параметров задачи с помощью ключей командной строки

С помощью ключей команды `kics-control --set-settings` вы можете изменять отдельные значения параметров задачи, а также добавлять или удалять области проверки и области исключения для задач типа (см. раздел "Управление задачами в командной строке" на стр. 119) OAS, ODS, OAFIM, ODFIM и AntiCryptor.

Настройка отдельных параметров задач

- Чтобы изменить отдельные значения параметров задачи с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-settings <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где:

- `<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. 119), присвоенный задаче в момент создания, или имя задачи в командной строке.
- `<имя параметра>=<значение параметра>` – имя и значение одного из параметров задачи. Текущие значения параметров задачи вы можете получить с помощью команды вывода параметров задачи (см. раздел "Вывод параметров задачи в командной строке" на стр. 129).

Значения указанных параметров задачи будут изменены.

Если в параметрах задачи Контроль приложений (на стр. 431) вы меняете разрешающий список или запрещаете запуск всех приложений и/или приложений, влияющих на работу приложения Kaspersky Industrial CyberSecurity for Linux Nodes, требуется запускать команду `--set-settings` с ключом `--accept`.

Добавление и удаление области проверки

- Чтобы добавить область проверки с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-settings <идентификатор/имя задачи> --add-path <путь>
```

где:

- `<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. 119), присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--add-path <путь>` – добавить путь к директории с проверяемыми объектами.

В параметры задачи будет добавлена новая секция `[ScanScope.item_#]`. Приложение будет проверять объекты в директории, указанной параметром `Path`. Остальные параметры области проверки принимают значения по умолчанию (см. раздел "Параметры задач командной строки по умолчанию" на стр. 711).

Если в параметрах задачи уже есть секция `[ScanScope.item_#]` с указанным значением параметра `Path`, дублирующая секция не добавляется.

Если для параметра `UseScanArea` установлено значение `No`, после выполнения этой команды значение изменится на `Yes` и будет выполняться проверка объектов, расположенных в этой директории.

Пример:

Добавление области проверки для задачи с ID=100:

```
kics-control --set-settings 100 ScanScope.item_0001.UseScanArea=Yes  
ScanScope.item_0001.Path=/home
```

В задачу будут добавлены следующие параметры области проверки:

```
[ScanScope.item_0001]  
AreaDesc=  
UseScanArea=Yes  
Path=/home  
AreaMask.item_0000=*
```

- Чтобы удалить область проверки с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-settings <идентификатор/имя задачи> --del-path <путь>
```

где:

- `<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. 119), присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--del-path <путь>` – удалить путь к директории с проверяемыми объектами.

Секция `[ScanScope.item_#]`, содержащая указанный путь, будет удалена из параметров задачи. Приложение не будет проверять объекты в указанной директории.

Добавление и удаление области исключения

- Чтобы добавить область исключения с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-settings <идентификатор/имя задачи> --add-exclusion <путь>
```

где:

- <идентификатор/имя задачи> – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- --add-exclusion <путь> – добавить путь к директории с объектами, которые вы хотите исключить из проверки.

В параметры задачи будет добавлена новая секция [ExcludedFromScanScope.item_#]. Приложение будет исключать из проверки объекты в директории, указанной параметром Path. Остальные параметры области исключения принимают значения по умолчанию (см. раздел "Параметры задач командной строки по умолчанию" на стр. [711](#)).

Если в параметрах задачи уже есть секция [ExcludedFromScanScope.item_#] с указанным значением параметра Path, дублирующая секция не добавляется.

Если для параметра UseScanArea установлено значение No, после выполнения этой команды значение изменится на Yes и объекты, расположенные в этой директории, будут исключаться из проверки.

- Чтобы удалить область исключения с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-settings <идентификатор/имя задачи> --del-exclusion <путь>
```

где:

- <идентификатор/имя задачи> – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- --del-exclusion <путь> – удалить путь к директории с исключаемыми объектами.

Секция [ExcludedFromScanScope.item_#], содержащая указанный путь, будет удалена из параметров задачи. Приложение не будет исключать из проверки объекты в указанной директории.

Восстановление параметров задачи по умолчанию в командной строке

Вы можете восстанавливать заданные по умолчанию параметры для всех пользовательских задач и всех предустановленных задач, кроме задач типов (см. раздел "Управление задачами в командной строке" на стр. [119](#)) Rollback и License (эти задачи не имеют параметров).

- Чтобы восстановить заданные по умолчанию параметры задачи, выполните следующую команду:

```
kics-control --set-settings <идентификатор/имя задачи> --set-to-default
```

где `<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

Приложение изменит значения параметров на заданные по умолчанию (см. раздел "Параметры задач командной строки по умолчанию" на стр. [711](#)).

Настройка расписания задачи в командной строке

Вы можете настраивать расписание запуска для задач следующих типов (см. раздел "Управление задачами в командной строке" на стр. [119](#)): *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*. Вы можете выводить текущие значения параметров расписания запуска задачи в консоль или в конфигурационный файл.

- *Чтобы вывести в консоль текущие параметры расписания запуска задачи, выполните следующую команду:*

```
kics-control --get-schedule <идентификатор/имя задачи> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

- *Чтобы вывести в конфигурационный файл текущие параметры расписания запуска задачи, выполните следующую команду:*

```
kics-control --get-schedule <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены параметры расписания задачи. Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанной директории не существует, конфигурационный файл не будет создан.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Примеры:

Сохранить параметры задачи обновления в файле с именем `update_schedule.ini` и сохранить созданный файл в текущей директории:

```
kics-control --get-schedule 6 --file update_schedule.ini
```

Вы можете изменять параметры расписания запуска задачи следующими способами:

- Импортировать параметры из конфигурационного файла, который содержит все параметры расписания.
- Задавать с помощью командной строки отдельные параметры расписания запуска задачи в формате `<имя параметра>=<значение параметра>`.

► Чтобы изменить значения параметров расписания запуска задачи с помощью конфигурационного файла, выполните следующие действия:

1. Выведите параметры задачи в конфигурационный файл с помощью команды `kics-control --get-schedule`.
2. Измените в файле значения нужных параметров и сохраните изменения.
3. Выполните команду:

```
kics-control --set-schedule <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

где:

`<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры расписания задачи.

`--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения параметров расписания запуска задачи, заданные в файле, будут импортированы в приложение.

Пример:

Импортировать в задачу с ID=2 параметры расписания из конфигурационного файла с именем `/home/test/on_demand_schedule.ini`:

```
kics-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

► Чтобы изменить отдельные значения параметров расписания запуска задачи с помощью командной строки, выполните следующую команду:

```
kics-control --set-schedule <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где:

- `<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.
- `<имя параметра>=<значение параметра>` – имя и значение одного из параметров расписания задач (см. раздел "Параметры расписания задач" на стр. [734](#)).

Значения указанных параметров расписания запуска задачи будут изменены.

Примеры:

Чтобы настроить запуск задачи каждые 10 часов, укажите следующие параметры:

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2021/May/30 23:05:00;10
RandomInterval=0
```

Чтобы настроить запуск задачи каждые 10 минут, укажите следующие параметры:

```
RuleType=Minutely
RunMissedStartRules=No
StartTime=23:10:00;10
RandomInterval=0
```

Чтобы настроить запуск задачи 15-го числа каждого месяца, укажите следующие параметры:

```
RuleType=Monthly
RunMissedStartRules=No
StartTime=23:25:00;15
RandomInterval=0
```

Чтобы настроить запуск задачи каждый вторник, укажите следующие параметры:

```
RuleType=Weekly
StartTime=18:01:30;Tue
RandomInterval=99
RunMissedStartRules=No
```

Чтобы настроить запуск задачи через каждые 11 дней, укажите следующие параметры:

```
RuleType=Daily
RunMissedStartRules=No
StartTime=23:15:00;11
RandomInterval=0
```

Управление общими параметрами приложения в командной строке

Общие параметры приложения определяют работу приложения в целом и работу отдельных функций. Вы можете управлять общими параметрами приложения с помощью специальных команд управления (см. раздел «Команды управления общими параметрами приложения» на стр. [679](#)):

- Выводить (см. раздел "Вывод общих параметров приложения" на стр. [138](#)) текущие значения общих параметров приложения в консоль или в конфигурационный файл.
- Изменять (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) общие параметры приложения, используя конфигурационный файл, содержащий все общие параметры, или ключи командной строки в формате `<имя параметра>=<значение параметра>`.

С помощью общих параметров вы можете:

- Настраивать использование Kaspersky Security Network и облегченной версии баз вредоносного ПО в работе приложения.
- Настраивать использование прокси-сервера в работе приложения.
- Выбирать режим перехвата файловых операций (см. раздел "Выбор режима перехвата файловых операций" на стр. [574](#)) (блокировать / не блокировать файлы во время проверки).
- Настраивать исключения из проверки точек монтирования (см. раздел "Настройка глобальных исключений в командной строке" на стр. [571](#)) (глобальные исключения).
- Настраивать исключения из проверки памяти процессов (см. раздел "Исключение памяти процессов из проверки" на стр. [572](#)).
- Включать и выключать проверку контейнеров в реальном времени (см. раздел "Настройка мониторинга контейнеров в командной строке" на стр. [326](#)).
- Включать и выключать обнаружение легальных приложений (см. раздел "Настройка обнаружения приложений, которые злоумышленники могут использовать для нанесения вреда" на стр. [575](#)), которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
- Включать и выключать интеграцию с Kaspersky Managed Detection and Response.
- Настраивать использование журналов событий (см. раздел "Просмотр событий и отчетов" на стр. [638](#)).
- Настраивать ограничение на использование ресурсов процессора (см. раздел "Ограничение на использование памяти и ресурсов процессора" на стр. [578](#)) для задач проверки (типа ODS).
- Ограничивать количество задач выборочной проверки, которые может одновременно запустить непривилегированный пользователь (см. раздел "Ограничение на количество задач выборочной проверки" на стр. [583](#)).

В этом разделе

Вывод общих параметров приложения	138
Изменение общих параметров приложения.....	139

Вывод общих параметров приложения

Вы можете выводить текущие значения общих параметров приложения в консоль или в конфигурационный файл, который вы можете использовать (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) для изменения параметров задачи.

- Чтобы вывести в консоль текущие значения общих параметров приложения, выполните следующую команду:

```
kics-control --get-app-settings [--json]
```

где `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

- *Чтобы вывести в конфигурационный файл текущие значения общих параметров приложения, выполните следующую команду:*

```
kics-control --get-app-settings --file <путь к конфигурационному файлу> [--json]
```

где:

- `--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены общие параметры приложения. Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанной директории не существует, конфигурационный файл не будет создан.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Пример:

Вывести общие параметры приложения в файл с именем `kics_config.ini`. Сохранить созданный файл в текущей директории:

```
kics-control --get-app-settings --file kics_config.ini
```

Изменение общих параметров приложения

В командной строке вы можете изменять общие параметры приложения с помощью команды `kics-control --set-app-settings`:

- Вы можете изменять все общие параметры, используя конфигурационный файл, который содержит общие параметры приложения. Конфигурационный файл вы можете получить с помощью команды вывода общих параметров (см. раздел "Вывод общих параметров приложения" на стр. [138](#)).
- Вы можете изменять отдельные параметры, используя ключи командной строки в формате `<имя параметра>=<значение параметра>`. Текущие значения общих параметров приложения вы можете получить с помощью команды вывода общих параметров (см. раздел "Вывод общих параметров приложения" на стр. [138](#)).

- *Чтобы изменить значения общих параметров приложения с помощью конфигурационного файла:*

1. Выведите общие параметры приложения в конфигурационный файл (см. раздел "Вывод общих параметров приложения" на стр. [138](#)).
2. Измените значения нужных параметров в файле и сохраните изменения.
3. Выполните команду:

```
kics-control --set-app-settings --file <путь к конфигурационному файлу> [--json]
```

где:

- `--file` <путь к конфигурационному файлу> – полный путь к конфигурационному файлу с общими параметрами приложения.
- `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения общих параметров, заданные в файле, будут импортированы в приложение.

- Чтобы изменить значения общих параметров приложения с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-app-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где <имя параметра>=<значение параметра> – имя и значение одного из общих параметров приложения.

Значения указанных общих параметров будут изменены.

Примеры:

Импортировать в приложение общие параметры из конфигурационного файла /home/test/kics_config.ini:

```
kics-control --set-app-settings --file /home/test/kics_config.ini
```

Установить низкий уровень детализации файла трассировки:

```
kics-control --set-app-settings TraceLevel=NotDetailed
```

Добавить точку монтирования, которую требуется исключить из перехвата файловых операций:

```
kics-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

Использование фильтра для ограничения результатов запросов

Фильтр позволяет ограничивать результаты запроса при выполнении команд управления приложением.

Условия фильтра задаются с помощью одного или нескольких *логических выражений*, скомбинированных с помощью логического оператора `and`. Условия фильтра требуется заключать в кавычки:

```
"<поле> <операция сравнения> '<значение>'"
```

```
"<поле> <операция сравнения> '<значение>' and <поле> <операция сравнения> '<значение>'"
```

где:

- <поле> – название поля базы данных.
- <операция сравнения> – одна из следующих операций сравнения:
 - > – больше.
 - < – меньше.

- `like` – соответствует указанному значению. При указании значения можно использовать маски %, например: логическое выражение "FileName like "%etc%" задаёт ограничение "содержит текст "etc" в поле FileName".
 - `==` – равно.
 - `!=` – не равно.
 - `>=` – больше или равно.
 - `<=` – меньше или равно.
 - `<значение>` – значение поля. Значение требуется указывать в одинарных кавычках (').
- Значение даты вы можете указывать в системе отметок времени UNIX™ (количество секунд, прошедших с 00:00:00 (UTC), 1 января 1970 года) или в формате YYYY-MM-DD hh:mm:ss. Значение даты и времени указывается пользователем и отображается приложением по локальному времени пользователя.

Вы можете использовать фильтр в следующих командах управления приложением:

- Вывод информации об определенных текущих событиях приложения (см. раздел "Просмотр событий в командной строке" на стр. [642](#)):

```
kics-control -W --query "<условия фильтра>"
```
- Вывод информации об определенных событиях приложения (см. раздел "Просмотр событий в командной строке" на стр. [642](#)) в журнале событий:

```
kics-control -E --query "<условия фильтра>"
```
- Вывод информации об определенных объектах в резервном хранилище (см. раздел "Работа с объектами резервного хранилища в командной строке" на стр. [589](#)):

```
kics-control -B --query "<условия фильтра>"
```
- Удаление определенных объектов из резервного хранилища (см. раздел "Работа с объектами резервного хранилища в командной строке" на стр. [589](#)):

```
kics-control -B --mass-remove --query "<условия фильтра>"
```

Примеры:

Вывести информацию о событиях, которые содержат текст "etc" в поле FileName:

```
kics-control -E --query "FileName like '%etc%'"
```

Вывести информацию о событиях с типом ThreatDetected (обнаружена угроза):

```
kics-control -E --query "EventType == 'ThreatDetected'"
```

Вывести информацию о событиях с типом ThreatDetected, сформированных задачами типа ODS:

```
kics-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

Вывести информацию о событиях, сформированных после даты, указанной в системе отметок времени UNIX (количество секунд, прошедших с 00:00:00 (UTC), 1 января 1970 года):

```
kics-control -E --query "Date > '1583425000'"
```

Вывести информацию о событиях, сформированных после даты, указанной в формате YYYY-MM-DD hh:mm:ss:

```
kics-control -E --query "Date > '2022-12-22 18:52:45'"
```

Вывести информацию о файлах в резервном хранилище, имеющих высокий (High) уровень важности:

```
kics-control -B --query "DangerLevel == 'High'"
```

Экспорт и импорт параметров приложения

Kaspersky Industrial CyberSecurity for Linux Nodes позволяет импортировать и экспортировать все параметры приложения для диагностики сбоев, проверки параметров или для упрощения настройки приложения на устройствах пользователей.

При экспорте параметров все параметры приложения и задач сохраняются в конфигурационном файле. Этот конфигурационный файл используется, чтобы импортировать параметры для настройки приложения.

Во время импорта или экспорта параметров приложение должно быть запущено. После импорта параметров требуется перезапустить приложение.

При импорте или экспорте параметров из более старой версии приложения для новых параметров устанавливаются значения по умолчанию. Импорт параметров в более старую версию приложения недоступен.

Экспорт параметров

Для экспорта параметров предназначена команда `kics-control --export-settings`.

Синтаксис команды

```
kics-control --export-settings --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут сохранены параметры приложения;

`--json` – формат конфигурационного файла, в который будут сохранены параметры приложения. Если вы не укажете формат файла, экспорт будет выполнен в файл формата INI.

Импорт параметров

Для импорта параметров предназначена команда `kics-control --import-settings`.

Если вы управляете приложением через Kaspersky Security Center, импорт параметров недоступен.

Синтаксис команды

```
kics-control --import-settings --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры приложения;

`--json` – формат конфигурационного файла, из которого будут импортированы параметры приложения. Если вы не укажете формат файла, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

При импорте параметров для параметра `UseKSN` устанавливается значение `No`. Чтобы начать или возобновить использование Kaspersky Security Network, требуется указать `UseKSN=Basic` или `UseKSN=Extended`.

После импорта параметров приложения внутренние идентификаторы задач могут измениться. Для управления ими рекомендуется использовать названия задач.

Запуск и остановка приложения

После установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes на устройство запуск приложения выполняется автоматически. Далее по умолчанию приложение запускается автоматически при запуске операционной системы (на уровнях выполнения по умолчанию, принятых для каждой операционной системы).

Запуск функциональных компонентов приложения сразу после установки зависит от режима работы приложения (см. раздел "О режимах работы приложения" на стр. [19](#)). Если во время установки вы не выбрали режим работы приложения или выбрали режим *Защита выключена*, все функциональные компоненты приложения выключены.

После того как вы включите нужные вам компоненты приложения, они будут запускаться автоматически при запуске приложения.

При запуске приложения на устройстве автоматически запускаются служебные задачи, обеспечивающие работу дополнительных функций приложения: функции активации приложения и функции резервного хранилища.

По умолчанию приложение также запускает настроенные в командной строке пользовательские задачи, для которых задан режим запуска (см. раздел "Параметры расписания задач" на стр. [734](#)) "после запуска приложения" (режим запуска `PS`).

Если вы остановите приложение, все выполняющиеся на устройстве задачи будут прерваны. Прерванные пользовательские задачи после повторного запуска приложения автоматически не возобновляются.

В этом разделе

Запуск и остановка приложения с помощью Web Console	144
Запуск и остановка приложения с помощью Консоли администрирования	145
Запуск и остановка приложения с помощью командной строки.....	145

Запуск и остановка приложения с помощью Web Console

► Чтобы запустить или остановить приложение дистанционно:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
Откроется список управляемых устройств.
2. В списке выберите устройство, на котором вы хотите запустить или остановить приложение, и по ссылке с названием устройства откройте окно свойств устройства.
3. Выберите закладку **Приложения**.
4. Установите флажок напротив приложения **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5**.
5. Выполните одно из следующих действий:
 - Если вы хотите запустить приложение, нажмите на кнопку **Запустить**.
 - Если вы хотите остановить работу приложения, нажмите на кнопку **Остановить**.

Вы можете контролировать статус работы приложения с помощью веб-виджета **Состояние защиты** в окне **Мониторинг и отчеты / Панель мониторинга**.

Запуск и остановка приложения с помощью Консоли администрирования

► Чтобы запустить или остановить приложение на клиентском устройстве:

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите закладку **Устройства**.
3. В списке управляемых устройств выберите устройство, на котором вы хотите запустить или остановить приложение, и в контекстном меню устройства выберите пункт **Свойства**.
4. В окне **Свойства: <Имя устройства>** выберите раздел **Программы**.
В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.
5. Выберите приложение **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5**.
6. Выполните одно из следующих действий:

- Если вы хотите запустить приложение, нажмите на кнопку  справа от списка приложений "Лаборатории Касперского" или в контекстном меню приложения выберите пункт **Запустить**.
- Если вы хотите остановить работу приложения, нажмите на кнопку  справа от списка приложений "Лаборатории Касперского" или в контекстном меню приложения выберите пункт **Остановить**.

Запуск и остановка приложения с помощью командной строки

Для запуска приложения требуется, чтобы учетная запись root была владельцем следующих директорий и только владелец имел право на запись в них: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

Запуск, перезапуск и остановка приложения Kaspersky Industrial CyberSecurity for Linux Nodes

► Чтобы запустить приложение в systemd-системе, выполните следующую команду:

```
systemctl start kics
```

► Чтобы остановить приложение в systemd-системе, выполните следующую команду:

```
systemctl stop kics
```

- Чтобы перезапустить приложение в *systemd*-системе, выполните следующую команду:

```
systemctl restart kics
```

- Чтобы запустить приложение в системе без *systemd*, выполните следующую команду:

```
/etc/init.d/kics start
```

- Чтобы остановить приложение в системе без *systemd*, выполните следующую команду:

```
/etc/init.d/kics stop
```

- Чтобы перезапустить приложение в системе без *systemd*, выполните следующую команду:

```
/etc/init.d/kics restart
```

Мониторинг статуса приложения Kaspersky Industrial CyberSecurity for Linux Nodes

Мониторинг статуса приложения Kaspersky Industrial CyberSecurity for Linux Nodes выполняется с помощью контрольной службы. Контрольная служба автоматически запускается при запуске приложения.

В случае сбоя приложения создается файл дампа (см. раздел "О файлах дампа" на стр. [667](#)), и приложение автоматически перезапускается.

- Чтобы вывести статус приложения в *systemd*-системе, выполните следующую команду:

```
systemctl status kics
```

- Чтобы вывести статус приложения в системе без *systemd*, выполните следующую команду:

```
/etc/init.d/kics status
```

Просмотр состояния защиты устройства и параметров приложения

Вы можете просматривать информацию о состоянии защиты устройства и о статусе работы приложения Kaspersky Industrial CyberSecurity for Linux Nodes и его компонентов на устройстве.

Вы можете получать информацию о состоянии защиты устройства следующими способами:

- В Web Console (см. раздел "Просмотр состояния защиты устройства в Web Console" на стр. [148](#)) или в Консоли администрирования (см. раздел "Просмотр состояния защиты устройства в Консоли администрирования" на стр. [149](#)) с помощью статусов клиентских устройств (*ОК*, *Критический*, *Предупреждение*). Устройство, на котором установлен Агент администрирования Kaspersky Security Center, является клиентским устройством для Kaspersky Security Center. Статус клиентского устройства может изменяться на *Критический* или *Предупреждение* по следующим причинам:
 - В соответствии с правилами, определенными в Kaspersky Security Center. Например, статус изменяется, если на устройстве не установлено приложение защиты, давно не выполнялся поиск вирусов, устарели базы приложения, истек срок действия лицензии или приложение работает нестабильно. Подробнее о причинах изменения статусов и настройке условий присвоения статусов см. в справке Kaspersky Security Center.
 - Kaspersky Security Center получает статус устройства от управляемого приложения, то есть от Kaspersky Industrial CyberSecurity for Linux Nodes.

Получение статуса устройства от управляемого приложения должно быть включено в Kaspersky Security Center в списках условий назначения статусов *Критический* и *Предупреждение*. Условия назначения статусов устройства настраиваются в окне свойств группы администрирования.

Подробнее о статусах клиентского устройства см. в справке Kaspersky Security Center.

- В Web Console (см. раздел "Просмотр информации о работе приложения в Web Console" на стр. [149](#)) или в Консоли администрирования (см. раздел "Просмотр информации о работе приложения в Консоли администрирования" на стр. [150](#)) с помощью статусов функциональных компонентов приложения Kaspersky Industrial CyberSecurity for Linux Nodes на устройстве. В свойствах приложения, установленного на устройстве, отображается список функциональных компонентов приложения. Для каждого компонента отображается его статус.
- В командной строке с помощью команды `kics-control --app-info`. Команда выводит информацию о работе приложения и состоянии функциональных компонентов и задач приложения.

В этом разделе

Просмотр состояния защиты устройства в Web Console	148
Просмотр состояния защиты устройства в Консоли администрирования	149
Просмотр информации о работе приложения в Web Console	149
Просмотр информации о работе приложения в Консоли администрирования	150
Просмотр информации о работе приложения в командной строке	152

Просмотр состояния защиты устройства в Web Console

► Чтобы просмотреть состояние защиты устройства в Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
Откроется список управляемых устройств.
2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и в открывшемся окне выберите группу администрирования.
В списке отобразятся только управляемые устройства выбранной группы администрирования.
3. В списке найдите устройство, информацию о котором вы хотите просмотреть, и нажмите на имя устройства.
4. В открывшемся окне свойств управляемого устройства на закладке **Общие** выберите раздел **Защита**.

В разделе **Защита** отображается следующая информация об устройстве:

- **Видимо в сети** – видимость выбранного устройства в сети: *Да* или *Нет*.
- **Статус устройства** – статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на выбранном устройстве и активности устройства в сети: *ОК*, *Критический* или *Предупреждение*.
- **Описание статуса** – причины смены статуса устройства на *Критический* или *Предупреждение*.
- **Состояние защиты** – текущий статус защиты от файловых угроз на выбранном устройстве, например: *Выполняется*, *Остановлена*, *Приостановлена*.
- **Последняя полная проверка** – дата и время выполнения последней полной проверки на выбранном устройстве.
- **Обнаружено вирусов** – общее количество вредоносных объектов, обнаруженных на выбранном устройстве (счетчик обнаруженных угроз) с момента установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes.
- **Объекты, которые не удалось вылечить** – количество зараженных объектов, которые приложению Kaspersky Industrial CyberSecurity for Linux Nodes не удалось вылечить.

Просмотр состояния защиты устройства в Консоли администрирования

► Чтобы просмотреть состояние защиты устройства в Консоли администрирования:

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите закладку **Устройства**.
3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.
4. В открывшемся окне свойств управляемого устройства выберите раздел **Защита**.

В разделе **Защита** отображается следующая информация об устройстве:

- **Статус устройства** – статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на выбранном устройстве и активности устройства в сети.
- **Все проблемы** – полный список проблем, обнаруженных управляемыми приложениями, установленными на выбранном устройстве. Каждая проблема имеет статус, который приложение предлагает вам назначить устройству.
- **Статус постоянной защиты** – текущий статус защиты от файловых угроз на выбранном устройстве, например, *Выполняется* или *Остановлена*. При изменении статуса защиты новый статус отобразится в окне свойств устройства только после синхронизации устройства с Сервером администрирования.
- **Последняя проверка по требованию** – дата и время выполнения последнего поиска вредоносного ПО на выбранном устройстве.
- **Всего обнаружено угроз** – общее количество угроз, обнаруженных на выбранном устройстве с момента установки приложения (первой проверки устройства) или с момента последнего обнуления счетчика угроз.
Чтобы обнулить счетчик, нажмите на кнопку **Обнулить**.
- **Активные угрозы** – количество необработанных файлов на выбранном устройстве.

Просмотр информации о работе приложения в Web Console

► Чтобы просмотреть в Web Console информацию о работе приложения:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
Откроется список управляемых устройств.
2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и выберите в открывшемся окне группу администрирования.
В списке отобразятся только управляемые устройства выбранной группы администрирования.
3. В списке найдите устройство, информацию о котором вы хотите просмотреть, и нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.
5. В списке приложений "Лаборатории Касперского", установленных на устройстве, нажмите на название приложения **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5**.

Откроется окно свойств приложения.

В окне **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5** отображается следующая информация о Kaspersky Industrial CyberSecurity for Linux Nodes:

- На закладке **Общие** в разделе **Информация** содержится общая информация об установленном приложении:
 - **Имя** – название приложения.
 - **Версия** – номер версии приложения.
 - **Установлено** – дата и время установки приложения на устройстве.
 - **Последнее обновление ПО** – дата и время последнего обновления модулей приложения Kaspersky Industrial CyberSecurity for Linux Nodes.
 - **Последняя синхронизация** – дата и время последнего соединения устройства с Сервером администрирования Kaspersky Security Center.
 - **Текущий статус** – состояние защиты от файловых угроз на устройстве, например: *Выполняется* или *Приостановлена*.
 - Блок **Устанавливаемые обновления** содержит информацию об обновлении модулей приложения.
 - Блок **Базы приложения** содержит информацию о дате и времени выпуска обновления баз приложения и дате и времени последнего обновления.
- На закладке **Общие** в разделе **Лицензии** приведена информация о лицензионных ключах, добавленных в приложение, и связанных с этими ключами лицензиях.
- На закладке **Общие** в разделе **Компоненты** содержится список функциональных компонентов приложения. Для каждого компонента отображается его статус (например, *Остановлен*, *Приостановлен*, *Не установлен*) и версия.
- На закладке **События** отображается список событий приложения на устройстве.
- На закладке **Настройка событий** отображаются типы событий, которые приложение сохраняет в хранилище событий, и время их хранения.
- На закладке **Параметры приложения** в разделе **Detection and Response** вы можете управлять сетевой изоляцией устройства.

Просмотр информации о работе приложения в Консоли администрирования

► Чтобы просмотреть в Консоли администрирования Kaspersky Security Center информацию о работе приложения:

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите закладку **Устройства**.

3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.
4. В открывшемся окне свойств управляемого устройства выберите раздел **Программы**.
В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.
5. Выберите приложение **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5** и откройте окно свойств приложения двойным щелчком мыши или с помощью кнопки **Свойства** в нижней части окна.

Откроется окно **Параметры Kaspersky Industrial CyberSecurity for Linux Nodes 1.5**.

В окне **Параметры Kaspersky Industrial CyberSecurity for Linux Nodes 1.5** отображается следующая информация о Kaspersky Industrial CyberSecurity for Linux Nodes:

- В разделе **Общие** содержится общая информация об установленном приложении:
 - **Номер версии** – номер версии приложения.
 - **Установлено** – дата и время установки приложения на устройстве.
 - **Текущее состояние** – состояние защиты от файловых угроз на устройстве, например: *Выполняется* или *Приостановлена*.
 - **Последнее обновление ПО** – дата и время последнего обновления модулей приложения Kaspersky Industrial CyberSecurity for Linux Nodes.
 - **Установленные обновления** – список модулей, для которых установлены обновления.
 - **Базы программы** – дата и время выпуска обновления баз приложения.
- В разделе **Компоненты** содержится список стандартных компонентов приложения. Для каждого компонента отображается его статус (например, *Остановлен*, *Приостановлен*, *Не установлен*) и версия.
- В разделе **Лицензионные ключи** приведена информация об активном и резервном лицензионных ключах:
 - **Серийный номер** – уникальная буквенно-цифровая последовательность.
 - **Статус** – статус лицензионного ключа, например, активный или резервный.
 - **Тип** – тип лицензии: коммерческая или пробная.
 - **Срок действия лицензии** – количество дней, в течение которых возможно использование приложения, активированного путем добавления этого ключа.
 - **Ограничения лицензии** – количество устройств, на которых вы можете использовать ключ.
 - **Дата активации** (поле доступно только для активного ключа) – дата добавления активного ключа.
 - **Срок действия** (поле доступно только для активного ключа) – дата окончания срока использования приложения, активированного путем добавления активного ключа.
- В разделе **Настройка событий** отображаются типы событий, которые приложение сохраняет в хранилище событий, и время их хранения.
- В разделе **Дополнительно** содержится информация о плагине управления приложением.

Просмотр информации о работе приложения в командной строке

► Чтобы посмотреть информацию о приложении, выполните следующую команду:

```
kics-control --app-info [--json]
```

где `--json` – выводить данные в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

В результате выполнения команды в консоль будет выведена следующая информация:

- **Название.** Название приложения.
- **Версия.** Текущая версия приложения.
- **Политика.** Информация о том, применяется ли на устройстве политика Kaspersky Security Center (см. раздел "О политиках Kaspersky Security Center" на стр. [99](#)).
- **Информация о лицензии.** Информация о лицензии или статус лицензионного ключа.
- **Информация о лицензии EDR Optimum.** Информация о лицензии, по которой используется функциональность Kaspersky Endpoint Detection and Response Optimum, или статус лицензионного ключа EDR Optimum.
- **Дата окончания срока действия лицензии.** Дата и время окончания срока действия лицензии (см. раздел "О лицензии" на стр. [81](#)) в формате UTC.
- **Статус файла MDR BLOB.** Статус конфигурационного файла BLOB для интеграции с Kaspersky Managed Detection and Response.
- **Дата окончания срока действия лицензии на использование MDR.** Дата и время окончания срока действия лицензии на использование Kaspersky Managed Detection and Response в формате UTC.
- **Состояние резервного хранилища.** Состояние резервного хранилища (см. раздел "Резервное хранилище" на стр. [586](#)).
- **Использование резервного хранилища.** Размер резервного хранилища.
- **Дата последнего запуска задачи Scan_My_Computer.** Время последнего запуска задачи Поиск вредоносного ПО (на стр. [225](#)).
- **Дата последнего выпуска баз приложения.** Время последнего выпуска баз приложения.
- **Базы приложения загружены.** Информация о том, загружены ли базы приложения.
- **Использование Kaspersky Security Network.** Информация об использовании Kaspersky Security Network: [Расширенный режим KSN](#), [Стандартный режим KSN](#) или [Выключен](#).
- **Инфраструктура Kaspersky Security Network.** Информация об инфраструктурном решении, которое используется для работы с репутационными базами "Лаборатории Касперского": [Kaspersky Security Network](#) или [Kaspersky Private Security Network](#).
- **Интеграция с Kaspersky Managed Detection and Response.** Статус интеграции с Kaspersky Managed Detection and Response: [Включена](#), [Выключена](#).
- **Интеграция с Kaspersky Endpoint Detection and Response Optimum.** Статус интеграции с Kaspersky Endpoint Detection and Response Optimum (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response Optimum" на стр. [610](#)).

- **Защита от файловых угроз.** Статус защиты от файловых угроз (см. раздел "Защита от файловых угроз" на стр. [172](#)) в реальном времени.
- **Мониторинг контейнеров.** Статус проверки контейнеров в реальном времени (см. раздел "Мониторинг контейнеров" на стр. [322](#)).
- **Контроль целостности системы.** Статус компонента Контроль целостности системы. (см. раздел "Контроль целостности системы в реальном времени" на стр. [516](#))
- **Управление сетевым экраном.** Статус компонента Управление сетевым экраном.
- **Защита от шифрования.** Статус компонента Защита от шифрования (см. раздел "Защита от удаленного вредоносного шифрования" на стр. [404](#)).
- **Защита от веб-угроз.** Статус компонента Защита от веб-угроз (на стр. [378](#)).
- **Контроль устройств.** Статус компонента Контроль устройств (на стр. [464](#)).
- **Проверка съемных дисков.** Статус компонента Проверка съемных дисков (на стр. [314](#)).
- **Защита от сетевых угроз.** Статус компонента Защита от сетевых угроз (на стр. [398](#)).
- **Анализ поведения.** Статус компонента Анализ поведения (на стр. [544](#)).
- **Контроль приложений.** Статус компонента Контроль приложений (на стр. [431](#)).
- **Веб-Контроль.** Статус компонента Веб-Контроль (на стр. [489](#)).
- **Интеграция с Kaspersky Industrial CyberSecurity for Networks.** Статус интеграции с Kaspersky Industrial CyberSecurity for Networks (см. раздел "Интеграция с Kaspersky Industrial CyberSecurity for Networks" на стр. [592](#)).
- **Действия после обновления.** Действия по обновлению приложения и действия, которые требуется выполнить пользователю.
- **Приложение работает нестабильно.** Информация о сбое в работе приложения и создании файла дампа. Это поле отображается, если при предыдущем запуске приложения произошел сбой.
- **Лечение и удаление файлов выключено.** Информация о том, что включен режим работы приложения, при котором лечение и удаление файлов на диске не выполняется, независимо настроенных в политике параметров.

В сертифицированной версии приложения интеграция с Kaspersky Managed Detection and Response не поддерживается. Включение интеграции с Kaspersky Managed Detection and Response приводит к выходу приложения из сертифицированного состояния.

Активация приложения и управление лицензионными ключами

Активация – это процедура введения в действие лицензии (см. раздел "О лицензии" на стр. [81](#)), дающей право на использование полнофункциональной версии приложения в течение срока действия лицензии.

Процедура активации приложения Kaspersky Industrial CyberSecurity for Linux Nodes заключается в добавлении на устройство активного лицензионного ключа приложения.

Если вы используете приложение по лицензии, которая не включает функциональность Kaspersky Endpoint Detection and Response Optimum (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response Optimum" на стр. [610](#)), для активации этой функциональности вам нужно добавить на устройство дополнительный лицензионный ключ Kaspersky Endpoint Detection and Response Optimum Add-on (далее также "ключ EDR Optimum").

Вы можете активировать приложение одним из следующих способов:

- Удаленно через Kaspersky Security Center (см. раздел "Активация приложения с помощью Kaspersky Security Center" на стр. [49](#)):
 - При установке приложения Kaspersky Industrial CyberSecurity for Linux Nodes. Вы можете добавить лицензионный ключ приложения в инсталляционный пакет. Приложение будет активировано автоматически после установки.
 - После установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes с помощью задачи активации приложения (см. раздел "Активация приложения с помощью Kaspersky Security Center" на стр. [49](#)).
 - После установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes путем распространения на клиентские устройства (см. раздел "Активация приложения с помощью Kaspersky Security Center" на стр. [49](#)) лицензионного ключа, размещенного на Сервере администрирования.
- С помощью командной строки:
 - Во время первоначальной настройки приложения Kaspersky Industrial CyberSecurity for Linux Nodes (см. раздел "Первоначальная настройка приложения в интерактивном режиме" на стр. [54](#)).
 - После установки приложения Kaspersky Industrial CyberSecurity for Linux Nodes с помощью команд управления.

Для добавления на устройство ключа EDR Optimum вы можете использовать задачу добавления ключа или процедуру распространения ключа на клиентские устройства. Указывать тип ключа не требуется.

Ключ EDR Optimum может быть добавлен только после добавления лицензионного ключа приложения.

Вы также можете добавить на устройство резервный ключ приложения и резервный ключ EDR Optimum. Резервный ключ становится активным либо по истечении срока действия лицензии, связанной с активным ключом, либо при удалении активного ключа. Наличие резервного ключа позволяет избежать ограничения функциональности приложения в момент окончания срока действия лицензии.

Резервный ключ может быть добавлен только после добавления активного лицензионного ключа.

Вы можете посмотреть информацию о лицензионных ключах, добавленных на устройство:

- Удаленно в Web Console (см. раздел "Просмотр информации о работе приложения в Web Console" на стр. [149](#)) или в Консоли администрирования (см. раздел "Просмотр информации о работе приложения в Консоли администрирования" на стр. [150](#)). В свойствах приложения на клиентском устройстве в разделе **Лицензии** отображается информация об активном и резервном ключах.
- В командной строке с помощью команд управления (см. раздел "Просмотр информации о лицензии и ключе в командной строке" на стр. [155](#)).

В этом разделе

Просмотр информации о лицензии и ключе в командной строке	155
Управление лицензионными ключами в командной строке	157

Просмотр информации о лицензии и ключе в командной строке

В командной строке с помощью команды `-L --query` вы можете просматривать информацию об активном и резервном лицензионных ключах, добавленных в приложение, и о лицензии, по которой активировано приложение. Если в приложение добавлен отдельный ключ для активации функциональности Kaspersky Endpoint Detection and Response Optimum, также отображается информация об активном и резервном лицензионных ключах EDR Optimum и о лицензии EDR Optimum.

- Чтобы посмотреть информацию о ключах и лицензии на устройстве, выполните следующую команду:

```
kics-control -L --query [--json]
```

где `--json` – выводить данные в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

В результате выполнения команды в консоль будет выведена следующая информация:

- Информация об активном ключе приложения, если ключ добавлен:
 - Дата и время окончания срока действия лицензии, по которой используется приложение.
 - Количество дней до окончания срока действия лицензии.
 - Информация об ограничении функций защиты.
 - Информация об ограничении функции обновления баз приложения.
 - Информация о статусе лицензионного ключа.
 - Тип лицензии, связанной с ключом.
 - Лицензионное ограничение ключа (количество единиц лицензирования).
 - Название приложения, для активации которого предназначен ключ.

- Активный лицензионный ключ (уникальная буквенно-цифровая последовательность).
- Дата активации.
- Информация о резервном ключе приложения. Отображается, если резервный ключ добавлен.
 - Дата и время окончания срока действия лицензии, по которой используется приложение.
 - Количество дней до окончания срока действия лицензии.
 - Информация об ограничении функций защиты.
 - Информация об ограничении функции обновления баз приложения.
 - Информация о статусе лицензионного ключа.
 - Тип лицензии, связанной с ключом.
 - Лицензионное ограничение ключа (количество единиц лицензирования).
 - Название приложения, для активации которого предназначен ключ.
 - Дата активации.
- Информация об активном ключе EDR Optimum, если ключ добавлен:
 - Дата и время окончания срока действия лицензии, по которой активирована функциональность Kaspersky Endpoint Detection and Response Optimum.
 - Информация об ограничении функции обновления баз приложения.
 - Информация о статусе лицензионного ключа.
 - Тип лицензии, связанной с ключом.
 - Лицензионное ограничение ключа (количество единиц лицензирования).
 - Название приложения, для активации которого предназначен ключ.
 - Активный лицензионный ключ (уникальная буквенно-цифровая последовательность).
 - Дата активации.
- Информация о резервном ключе EDR Optimum. Отображается, если резервный ключ EDR Optimum добавлен.
 - Дата и время окончания срока действия лицензии, по которой активирована функциональность Kaspersky Endpoint Detection and Response Optimum.
 - Информация об ограничении функции обновления баз приложения.
 - Информация о статусе лицензионного ключа.
 - Тип лицензии, связанной с ключом.
 - Лицензионное ограничение ключа (количество единиц лицензирования).
 - Название приложения, для активации которого предназначен ключ.
 - Дата активации.

Управление лицензионными ключами в командной строке

Для управления лицензионными ключами приложения на устройстве вы можете использовать команды управления лицензионными ключами.

- Чтобы добавить в приложение активный ключ, выполните следующую команду:

```
kics-control [-L] --add-active-key <путь к файлу ключа>
```

Если файл ключа находится в текущей директории, достаточно указать только имя файла.

- Чтобы добавить в приложение резервный ключ, выполните следующую команду:

```
kics-control [-L] --add-reserve-key <путь к файлу ключа>
```

Если активный ключ еще не добавлен в приложение на устройстве, команда завершается с ошибкой.

С помощью команды добавления ключа вы можете добавить как лицензионные ключи приложения, так и лицензионные ключи EDR Optimum. Указывать тип ключа в команде не требуется.

- Чтобы удалить активный ключ приложения, выполните следующую команду:

```
kics-control [-L] --remove-active-key
```

- Чтобы удалить резервный ключ приложения, выполните следующую команду:

```
kics-control [-L] --remove-reserve-key
```

- Чтобы удалить активный ключ EDR Optimum, выполните следующую команду:

```
kics-control [-L] --remove-active-key --edr-optimum
```

- Чтобы удалить резервный ключ EDR Optimum, выполните следующую команду:

```
kics-control [-L] --remove-reserve-key --edr-optimum
```

Обновление баз и модулей приложения

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) будет недоступна в приложении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

Обновление баз и модулей приложения Kaspersky Industrial CyberSecurity for Linux Nodes обеспечивает актуальность защиты устройства. Каждый день в мире появляются новые вирусы, вредоносные программы и другие программы, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах приложения. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули приложения.

Для регулярного обновления баз требуется действующая лицензия (см. раздел "Активация приложения и управление лицензионными ключами" на стр. 154) на использование приложения. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

В процессе обновления базы и модули приложения загружаются и устанавливаются на вашем устройстве.

Вы можете получать обновления баз и модулей приложения с серверов обновлений "Лаборатории Касперского", из хранилища Сервера администрирования, из локальных или сетевых директорий и из других источников обновлений (см. раздел "Об источниках и схемах обновления" на стр. 160).

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

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт). Объем занимаемого дискового пространства может достигать 3 ГБ.

Загрузка обновлений с серверов обновлений "Лаборатории Касперского" или с других FTP-, HTTP- или HTTPS-серверов осуществляется по стандартным сетевым протоколам. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, укажите параметры прокси-сервера (см. раздел "Настройка прокси-сервера" на стр. 560) в общих параметрах приложения.

Независимо от источника обновлений загрузка пакета обновлений и установка обновления баз и модулей приложения на устройстве выполняется с помощью задачи *Обновление*.

В приложении создается предустановленная задача *Обновление*. С помощью этой задачи вы можете выполнять обновление баз и модулей приложения по расписанию и по требованию и настраивать параметры обновления.

В Kaspersky Security Center вы можете использовать групповую задачу *Обновление*, которую мастер первоначальной настройки создает после установки mms-плагинов управления или веб-плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes.

Вы также можете создавать пользовательские задачи обновления в командной строке и в Kaspersky Security Center.

Вы можете настраивать следующие параметры обновления баз и модулей приложения:

- Выбирать источник, из которого приложение будет получать обновления, в зависимости от используемой схемы обновления (см. раздел "Об источниках и схемах обновления" на стр. [160](#)).
- Настраивать время ожидания ответа от выбранного источника обновлений при попытке соединения с ним. Если в течение указанного времени от источника обновлений не приходит ответ, приложение обращается к другому указанному источнику обновлений.
- Выбирать режим загрузки и установки модулей приложения и обновлений версии приложения: загружать и устанавливать, только загружать или не загружать.

Допускается устанавливать только обновления модулей приложения, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу приложения из сертифицированного состояния.

- Настраивать расписание запуска задачи обновления. По умолчанию приложение обновляет базы с периодичностью один раз в 60 минут.

В этом разделе

Об обновлении баз и модулей.....	159
Об источниках и схемах обновления	160
Обновление баз и модулей приложения в Web Console	161
Обновление баз и модулей приложения в Консоли администрирования	163
Обновление баз и модулей приложения в командной строке.....	166
Обновление с помощью Kaspersky Update Utility.....	169
Откат обновления баз и модулей приложения	170

Об обновлении баз и модулей

В процессе обновления на вашем устройстве загружаются и устанавливаются следующие объекты:

- Базы приложения. Базы приложения включают в себя базы сигнатур вредоносных программ, описание сетевых атак, базы вредоносных и фишинговых веб-адресов, базы баннеров, спам-базы и другие данные.

Если обновление баз на устройстве прерывается или завершается с ошибкой, приложение продолжает использовать предыдущую установленную версию баз. Если ранее базы приложения не устанавливались, приложение продолжает работу в режиме "без баз". Обновление баз и модулей приложения остается доступным.

Базы актуальны, если они были загружены менее трех дней назад. По умолчанию приложение формирует событие *Базы устарели* (*BasesAreOutOfDate*), если последние установленные

обновления баз были опубликованы на серверах "Лаборатории Касперского" более трех, но менее семи дней назад. Если базы не обновляются в течение семи дней, приложение формирует событие *Базы сильно устарели (BasesAreTotallyOutOfDate)*.

- Модули приложения. Обновление модулей предназначено для устранения уязвимостей в приложении и улучшения методов защиты устройства. Обновления модулей могут менять поведение компонентов приложения и добавлять новые возможности.

Обновление модулей приложения может быть установлено вне зависимости от состояния приложения (запущено или остановлено, управляется политикой Kaspersky Security Center) и расписания обновлений. Kaspersky Industrial CyberSecurity for Linux Nodes продолжает защищать ваше устройство во время процедуры обновления модулей приложения. В ходе обновления параметры приложения и журнал событий приложения переносятся в новую версию приложения. После обновления нужно перезапустить Kaspersky Industrial CyberSecurity for Linux Nodes. Если во время переноса параметров по какой-либо причине происходит ошибка, для приложения устанавливаются значения по умолчанию. Изменения параметров приложения, сделанные после завершения обновления и до перезапуска приложения, не сохраняются.

Допускается устанавливать только обновления модулей приложения, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу приложения из сертифицированного состояния.

Если приложение после обновления работает некорректно, оно автоматически откатывается на предыдущую версию. Рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. [661](#)).

Об источниках и схемах обновления

Источник обновлений – это ресурс, содержащий обновления баз и модулей приложения Kaspersky Industrial CyberSecurity for Linux Nodes. Источником обновлений могут быть FTP-, HTTP- или HTTPS-серверы (например, серверы обновлений "Лаборатории Касперского") и локальные или сетевые директории, смонтированные пользователем.

Основным источником обновлений служат серверы обновлений "Лаборатории Касперского". Вы можете указывать другие источники обновлений в параметрах задачи *Обновление*. Если обновление не может быть выполнено из одного источника обновлений, приложение Kaspersky Industrial CyberSecurity for Linux Nodes переключается к следующему источнику.

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes поддерживает следующие схемы обновления баз и модулей:

- Обновление с серверов обновлений "Лаборатории Касперского". Серверы обновлений "Лаборатории Касперского" расположены в разных странах по всему миру, что обеспечивает высокую надежность обновления. Если обновление не может быть выполнено с одного сервера, приложение переключается к следующему серверу. Обновления загружаются по протоколу HTTPS.
- Централизованное обновление. Централизованное обновление обеспечивает снижение внешнего интернет-трафика, а также удобство контроля за обновлением.

Централизованное обновление состоит из следующих этапов:

1. Загрузка пакета обновлений в хранилище внутри сети организации.

В качестве хранилища вы можете использовать хранилище Сервера администрирования Kaspersky Security Center.

Загрузку пакета обновлений в хранилище Сервера администрирования обеспечивает задача Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования*.

2. Распространение пакета обновлений на клиентские устройства.

Распространение пакета обновлений на клиентские устройства обеспечивает задача приложения Kaspersky Industrial CyberSecurity for Linux Nodes *Обновление*. В параметрах задачи вам нужно выбрать в качестве источника обновлений Сервер администрирования Kaspersky Security Center.

- Обновление из локальной или сетевой директории (SMB/NFS), смонтированной пользователем, или с FTP-, HTTP- или HTTPS-сервера. Вы можете указать пользовательский источник обновлений в параметрах задачи *Обновление*.

Обновление баз и модулей приложения в Web Console

В Web Console вы можете выполнять обновление баз и модулей приложения с помощью задачи *Обновление*. Вы можете использовать автоматически созданную групповую задачу *Обновление*, а также создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) пользовательские задачи обновления.

► *Чтобы настроить параметры обновления в Web Console:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.
Откроется список задач.
2. Выполните одно из следующих действий:
 - Если вы хотите изменить параметры задачи, которая выполняется на всех устройствах, входящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне группу администрирования.
В списке отобразятся только задачи, настроенные для выбранной группы администрирования.
 - Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне верхний узел с именем Сервера администрирования.
В списке отобразятся все задачи, созданные на Сервере администрирования.
3. В списке задач выберите нужную задачу **Обновление** и откройте окно свойств задачи по ссылке в названии задачи.
4. В окне свойств задачи выберите закладку **Параметры приложения**, в списке слева выберите раздел **Источники обновлений**.
5. Выберите источник обновлений, из которого приложение будет получать обновление баз и модулей, в зависимости от используемой схемы обновления (см. раздел "Об источниках и схемах обновления" на стр. [160](#)).
Вы можете сформировать список источников обновления, выбрав вариант **Другие источники в локальной или глобальной сети**. В качестве источников обновлений вы можете указывать FTP-, HTTP- или HTTPS-серверы. Если обновление не может быть выполнено из одного источника обновлений, приложение Kaspersky Industrial CyberSecurity for Linux Nodes переключается к следующему источнику. Приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице.
6. Перейдите в раздел **Параметры** и настройте другие параметры обновления.

7. Выберите закладку **Расписание** и настройте расписание запуска задачи обновления.

Если в качестве источника обновлений вы выбрали **Kaspersky Security Center**, в раскрывающемся списке **Запуск задачи** выберите **При загрузке обновлений в хранилище**. Подробнее о расписании задач см. в справке Kaspersky Security Center.

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

Задача будет запускаться в соответствии с настроенным расписанием. Вы также можете запускать задачу вручную (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)).

Таблица 8. Раздел Источники обновлений задачи Обновление

Параметр	Описание
Источники обновлений	В этом блоке вы можете выбрать источник обновлений: • Серверы обновлений "Лаборатории Касперского", на которых публикуются обновления баз для приложений "Лаборатории Касперского" (значение по умолчанию). • Kaspersky Security Center – Сервер администрирования Kaspersky Security Center. • Другие источники в локальной или глобальной сети – HTTP-, HTTPS- и FTP-серверы или директории на серверах локальной сети.
Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны	Флажок включает или выключает использование серверов обновлений "Лаборатории Касперского" в качестве источника обновлений, если выбранные источники обновлений недоступны. Флажок доступен, если в блоке Источники обновлений выбран вариант Другие источники в локальной или глобальной сети или Kaspersky Security Center. По умолчанию флажок установлен.
Пользовательские источники обновлений	Таблица содержит список пользовательских источников обновлений баз. В процессе обновления приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице. Таблица содержит следующие столбцы: • Источник обновлений – HTTP-, HTTPS- или FTP-серверы или директории на серверах локальной сети. • Переключатель показывает, будет ли источник использоваться в задаче (Включено или Выключено). Вы можете включить или выключить переключатель в таблице, а также установить или снять флажок Использовать этот источник в окне Источник обновлений, которое открывается по ссылке с названием источника. Таблица доступна, если выбран вариант Другие источники в локальной или глобальной сети. По умолчанию таблица пустая. Источники обновлений в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Таблица 9. Раздел Параметры задачи Обновление

Параметр	Описание
Максимальное время ожидания ответа от источника обновлений (сек.)	Предельный период ожидания ответа на запрос приложения от выбранного источника обновлений (в секундах). При отсутствии ответа по истечении этого времени в журнал выполнения задач записывается событие о нарушении связи с источником обновлений. Доступные значения: 0-120. Если указано значение 0, период ожидания ответа на запрос приложения от выбранного источника не ограничен. Значение по умолчанию: 10 секунд.
Режим загрузки обновлений приложения	В раскрывающемся списке вы можете выбрать режим загрузки обновлений приложения: • Не загружать обновления. При выборе этого элемента списка обновить приложение невозможно. • Только загружать обновления, но не устанавливать их на клиентские устройства (значение по умолчанию). • Загружать и устанавливать обновления на клиентские устройства. После установки обновлений приложение будет автоматически перезапущено. Для сохранения сертифицированной конфигурации приложения требуется установить значение параметра Не загружать.

Обновление баз и модулей приложения в Консоли администрирования

В Консоли администрирования вы можете выполнять обновление баз и модулей приложения с помощью задачи *Обновление*. Вы можете использовать автоматически созданную групповую задачу *Обновление*, а также создавать (см. раздел "Создание задач в Консоли администрирования" на стр. [116](#)) пользовательские задачи обновления.

► Чтобы настроить параметры обновления в Консоли администрирования:

- В Консоли администрирования выполните одно из следующих действий:
 - Если вы хотите изменить параметры задачи, которая выполняется на устройствах, входящих в определенную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите закладку **Задачи**.
 - Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), в дереве консоли выберите папку **Задачи**.
- В списке задач выберите нужную задачу **Обновление** и откройте окно свойств задачи двойным щелчком мыши.
- В окне свойств задачи в списке слева выберите раздел **Источники обновлений**.
- Выберите источник обновлений, из которого приложение будет получать обновление баз и модулей, в зависимости от используемой схемы обновления (см. раздел "Об источниках и схемах обновления" на стр. [160](#)).

Список источников обновлений содержит серверы обновлений "Лаборатории Касперского" и Сервер администрирования Kaspersky Security Center. Вы можете добавлять в список другие источники обновлений.

Вы можете сформировать список источников обновления, выбрав вариант **Другие источники в локальной или глобальной сети**. В качестве источников обновлений вы можете указывать FTP-, HTTP- или HTTPS-серверы. Если обновление не может быть выполнено с одного источника обновлений, приложение Kaspersky Industrial CyberSecurity for Linux Nodes переключается к следующему источнику. Приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице.

5. Выберите раздел **Параметры** и настройте другие параметры обновления.
6. Выберите раздел **Расписание** и настройте расписание запуска задачи обновления.

Если в качестве источника обновлений вы выбрали **Kaspersky Security Center**, в раскрывающемся списке **Запуск по расписанию** выберите **При загрузке обновлений в хранилище**. Подробнее о расписании задач см. в справке Kaspersky Security Center.

7. Нажмите на кнопку **Применить** или на кнопку **ОК** в окне **Свойства: <Название задачи>**, чтобы сохранить внесенные изменения.

Задача будет запускаться в соответствии с настроенным расписанием. Вы также можете запускать задачу вручную (см. раздел "Запуск, остановка, приостановка и возобновление задач в Консоли администрирования" на стр. [117](#)).

Таблица 10. Раздел Источники обновлений задачи Обновление

Параметр	Описание
Источники обновлений	В этом блоке вы можете выбрать источник обновлений: • Серверы обновлений "Лаборатории Касперского", на которых публикуются обновления баз для приложений "Лаборатории Касперского" (значение по умолчанию). • Kaspersky Security Center – Сервер администрирования Kaspersky Security Center. • Другие источники в локальной или глобальной сети – HTTP-, HTTPS- и FTP-серверы или директории на серверах локальной сети.
Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны	Флажок включает или выключает использование серверов обновлений "Лаборатории Касперского" в качестве источника обновлений, если выбранные источники обновлений недоступны. Флажок доступен, если в блоке Источники обновлений выбран вариант Другие источники в локальной или глобальной сети или Kaspersky Security Center. По умолчанию флажок установлен.
Пользовательские источники обновлений	Таблица содержит список пользовательских источников обновлений баз. В процессе обновления приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице. Таблица содержит следующие столбцы: • Адрес источника – HTTP-, HTTPS- или FTP-серверы или директории на серверах локальной сети. • Статус показывает, используется ли источник в задаче (Используется или Не используется). Вы можете изменить статус, установив или сняв флажок Использовать этот источник в окне Источник обновлений, которое открывается при нажатии на кнопку Изменить. Таблица доступна, если выбран вариант Другие источники в локальной или глобальной сети. Источники обновлений в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз. По умолчанию таблица пустая.

Таблица 11. Раздел Параметры задачи Обновление

Параметр	Описание
Максимальное время ожидания ответа от источника обновлений (сек.)	Предельный период ожидания ответа на запрос приложения от выбранного источника обновлений (в секундах). При отсутствии ответа по истечении этого времени в журнал выполнения задач записывается событие о нарушении связи с источником обновлений. Доступные значения: 0–120. Если указано значение 0, период ожидания ответа на запрос приложения от выбранного источника не ограничен. Значение по умолчанию: 10 секунд.
Режим загрузки обновлений	В раскрывающемся списке вы можете выбрать режим загрузки обновлений приложения: • Не загружать обновления. При выборе этого элемента списка обновить приложение невозможно. • Только загружать обновления, но не устанавливать их на клиентские устройства (значение по умолчанию). • Загружать и устанавливать обновления на клиентские устройства. После установки обновлений приложение будет автоматически перезапущено. Для сохранения сертифицированной конфигурации приложения требуется установить значение параметра Не загружать.

Обновление баз и модулей приложения в командной строке

В командной строке вы можете выполнять обновление баз и модулей приложения следующими способами:

- С помощью предустановленной задачи Обновление (*Update*). Вы можете запускать, останавливать, приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) эту задачу вручную и настраивать расписание (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)) запуска задачи. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры этой задачи.
- С помощью пользовательских задач (см. раздел "Создание задачи в командной строке" на стр. [127](#)) обновления (задач типа *Update*). Вы можете запускать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) пользовательские задачи вручную и настраивать расписание (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)) запуска задач.

Таблица 12. Параметры задачи Обновление

Параметр	Описание	Значения
SourceType	Источник, из которого приложение будет получать обновления.	KLServers (значение по умолчанию) – приложение получает обновления с одного из серверов обновлений "Лаборатории Касперского". Обновления загружаются по протоколу HTTPS. SCServer – приложение загружает обновления на защищаемое устройство с установленного в локальной сети Сервера администрирования. Вы можете выбрать этот источник обновлений, если вы используете Kaspersky Security Center для централизованного управления защитой устройств в вашей организации. Custom – приложение загружает обновления из пользовательского источника, указанного в секции [CustomSources.item_#]. Вы можете указывать директории FTP-, HTTP- и HTTPS-серверов или директории на любом смонтированном устройстве защищаемого клиентского устройства, включая директории на удаленных устройствах, смонтированные по протоколам Samba или NFS.
UseKLServersWhenUnavailable	Обращение приложения к серверам обновлений "Лаборатории Касперского" в случае, если все пользовательские источники недоступны.	Yes (значение по умолчанию) – приложение подключается к серверам обновлений "Лаборатории Касперского", если все пользовательские источники обновлений недоступны. No – приложение не подключается к серверам обновлений "Лаборатории Касперского", если все пользовательские источники обновлений недоступны.
ApplicationUpdateMode	Режим загрузки и установки обновлений приложения.	Disabled – не загружать и не устанавливать обновления приложения. DownloadOnly (значение по умолчанию) – загружать обновления приложения, но не устанавливать их. DownloadAndInstall – автоматически загружать и устанавливать обновления приложения. После установки обновлений приложение будет автоматически перезапущено. Для сохранения сертифицированной конфигурации приложения требуется установить для параметра ApplicationUpdateMode значение Disabled.

Параметр	Описание	Значения
ConnectionTimeout	Время ожидания (в секундах) ответа от источника обновлений при попытке соединения с ним. Если в течение указанного промежутка времени от источника обновлений не приходит ответ, приложение обращается к другому указанному источнику обновлений.	Вы можете указывать только целые числа в диапазоне от 0 до 120. Значение по умолчанию: 10.
Секция [CustomSources.item_#] содержит следующие параметры:		
URL	Адрес пользовательского источника обновлений в локальной сети или в интернете.	Значение по умолчанию не задано. Примеры: URL=http://example.com/bases/ – адрес HTTP-сервера, на котором расположена директория с обновлениями. URL=/home/bases/ – директория на защищаемом устройстве, в которой содержатся базы приложения.
Enabled	Использование источника обновлений, указанного в параметре URL. Для выполнения задачи требуется включить использование хотя бы одного источника обновлений.	Yes – приложение использует источник обновлений. No – приложение не использует источник обновлений. Значение по умолчанию не задано.

Обновление с помощью Kaspersky Update Utility

Для экономии интернет-трафика вы можете настроить обновление баз и модулей приложения на устройствах локальной сети организации из общей директории с помощью утилиты Kaspersky Update Utility. Для этого одно из устройств локальной сети организации должно получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или с серверов обновлений "Лаборатории Касперского" и копировать полученные пакеты обновлений в общую директорию с помощью утилиты. Остальные устройства локальной сети организации смогут получать пакет обновлений из общей директории.

► Чтобы настроить обновление баз из общей директории с помощью утилиты Kaspersky Update Utility:

1. Установите Kaspersky Update Utility на одном из устройств локальной сети организации.

Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта службы технической поддержки "Лаборатории Касперского" <https://support.kaspersky.ru/updater3>.

2. Настройте копирование пакета обновлений в общую директорию в параметрах Kaspersky Update Utility.

Выберите источник обновлений (например, хранилище Сервера администрирования) и общую директорию, в которую Kaspersky Update Utility будет копировать пакеты обновлений.

Дополнительная информация о работе с Kaspersky Update Utility приведена в Базе знаний "Лаборатории Касперского" <https://support.kaspersky.ru/updater3/linux>.

3. Настройте обновления баз и модулей приложения из указанной общей директории на остальных устройствах локальной сети организации.
 - a. Откройте свойства задачи **Обновление**, которая будет выполняться на нужном устройстве, с помощью Web Console (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) или с помощью Консоли администрирования (см. раздел "Изменение параметров задач в Консоли администрирования" на стр. [117](#)).
 - b. В свойствах задачи перейдите в раздел **Источники обновлений**.
 - c. В блоке **Источники обновлений** выберите вариант **Другие источники в локальной или глобальной сети**.
4. В таблице источников обновлений нажмите на кнопку **Добавить** и укажите путь к общей директории.

Адрес источника должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.

5. Установите флажок **Использовать этот источник** и нажмите на кнопку **ОК**.
6. В таблице источников обновлений настройте порядок их использования с помощью кнопок **Вверх** и **Вниз**.
7. Сохраните изменения параметров задачи.

Откат обновления баз и модулей приложения

После первого обновления баз приложения становится доступна функция отката баз приложения к их предыдущей версии.

Каждый раз, когда пользователь запускает процесс обновления, приложение Kaspersky Industrial CyberSecurity for Linux Nodes создает резервную копию текущих баз приложения. Это позволяет откатить базы до предыдущей версии, если требуется.

Откат последнего обновления баз используется, например, если новая версия баз приложения содержит недопустимые сигнатуры, что приводит к блокировке безопасных приложений приложением Kaspersky Industrial CyberSecurity for Linux Nodes.

В командной строке для отката обновлений вы можете запускать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) предустановленную задачу *Откат обновления баз (Rollback)* или создавать (см. раздел "Создание задачи в командной строке" на стр. [127](#)) и запускать пользовательские задачи отката обновления (задачи типа *Rollback*).

В Kaspersky Security Center вы можете создавать задачи отката обновления для групп администрирования или отдельных устройств с помощью Web Console (см. раздел "Создание задач в Web Console" на стр. [113](#)) или Консоли администрирования (см. раздел "Создание задач в Консоли администрирования" на стр. [116](#)).

Задача *Откат обновления баз* не имеет параметров.

Защита от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы устройства. Если компонент включен, он постоянно находится в оперативной памяти устройства и проверяет все открываемые, сохраняемые и запускаемые файлы в режиме реального времени.

При обнаружении вредоносного ПО приложение Kaspersky Industrial CyberSecurity for Linux Nodes может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

Если при установке приложения был выбран режим работы приложения по умолчанию, Защита от файловых угроз по умолчанию выключена.

Чтобы обеспечить защиту ваших устройств, рекомендуется применить на устройствах политику (см. раздел "О политиках Kaspersky Security Center" на стр. [99](#)) с помощью Web Console (см. раздел "Настройка защиты от файловых угроз в Web Console" на стр. [173](#)) или Консоли администрирования (см. раздел "Настройка защиты от файловых угроз в Консоли администрирования" на стр. [190](#)), или настроить параметры защиты с помощью командной строки (см. раздел "Управление приложением через командную строку" на стр. [118](#)).

На работу компонента влияет режим перехвата файловых операций (см. раздел "Выбор режима перехвата файловых операций" на стр. [574](#)), который вы можете выбрать в общих параметрах приложения. По умолчанию блокировка доступа к файлам, которые проверяет компонент Защита от файловых угроз, выключена.

Если включена защита от файловых угроз и включен Мониторинг контейнеров (на стр. [322](#)), приложение также проверяет все пространства имен и контейнеры во всех поддерживаемых операционных системах.

Вы можете включать и выключать защиту от файловых угроз, а также настраивать параметры защиты:

- Выбирать режим проверки файлов (при открытии, при открытии и изменении).
- Включать и выключать проверку архивов, почтовых баз, сообщений электронной почты в текстовом формате.
- Временно исключать из повторной проверки файлы в текстовом формате.
- Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
- Выбирать действия, которые приложение будет выполнять над зараженными объектами.
- Настраивать области проверки. Приложение будет проверять объекты в указанной области файловой системы.
- Настраивать исключения объектов из проверки. *Исключение из проверки* – это совокупность условий, при выполнении которых приложение не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете исключать из проверки:
 - объекты по именам или маскам;
 - объекты по названиям обнаруженных в объектах угроз;
 - файлы и директории в указанных областях файловой системы;
 - процесс и файлы, изменяемые указанным процессом.

- Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
- Включать и выключать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.

Для оптимизации работы компонента Защита от файловых угроз вы можете настроить исключение из проверки файлов, копируемых из сетевых директорий. Файлы будут проверяться только после завершения копирования в локальную директорию. Для исключения из проверки файлов в сетевых директориях вам нужно настроить исключение по процессам для утилиты, предназначенной для копирования из сетевых директорий (например, для утилиты `cp`). Если вы управляете приложением с помощью Kaspersky Security Center, вы можете настроить исключение по процессам в Web Console (см. раздел "Исключения Защиты от файловых угроз" на стр. [182](#)) или в Консоли администрирования (см. раздел "Исключения Защиты от файловых угроз" на стр. [201](#)). Если вы управляете приложением с помощью командной строки, вы можете настроить исключение по процессам, добавив в параметры задачи (см. раздел "Оптимизация проверки сетевых директорий" на стр. [222](#)) типа OAS секцию `[ExcludedForProgram.item_#]`.

В этом разделе

Настройка защиты от файловых угроз в Web Console.....	173
Настройка защиты от файловых угроз в Консоли администрирования	190
Настройка защиты от файловых угроз в командной строке	210
Особенности проверки символических и жестких ссылок	223

Настройка защиты от файловых угроз в Web Console

В Web Console вы можете управлять защитой от файловых угроз в политике (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Базовая защита** → **Защита от файловых угроз**).

Таблица 13. Параметры компонента Защита от файловых угроз

Параметр	Описание
Защита от файловых угроз включена / выключена	Переключатель включает или выключает компонент Защита от файловых угроз на всех управляемых устройствах. По умолчанию переключатель включен.
Режим Защиты от файловых угроз	В раскрывающемся списке вы можете выбрать режим работы компонента Защита от файловых угроз: • Интеллектуальный режим (значение по умолчанию) – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс в течение определенного времени многократно обращается к файлу и изменяет его, приложение повторно проверяет файл только при последнем закрытии файла этим процессом. • При открытии – проверять файл при попытке открытия на чтение, исполнение или изменение. • При открытии и изменении – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Блокировать доступ к объекту. • Пропускать объект (значение по умолчанию).
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Блокировать доступ к объекту (значение по умолчанию).
Области защиты	По ссылке Настроить области проверки открывается окно Области защиты (см. раздел "Окно Области проверки" на стр. 191).

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, включив и настроив параметры Пропускать файл, если его проверка длится более (сек.) и Пропускать файл, если его размер более (МБ). Если флажок снят, приложение не проверяет архивы. По умолчанию флажок снят.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку <i>самораспаковывающихся архивов</i>. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок Проверять архивы. По умолчанию флажок снят.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook®, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать текстовые файлы	Временное исключение из проверки файлов в текстовом формате. Если флажок установлен, приложение не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов работы приложений. Если флажок снят, приложение проверяет текстовые файлы. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 60.

Параметр	Описание
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал события <i>ObjectProcessed</i>. Если флажок установлен, приложение записывает в журнал событие <i>ObjectProcessed</i> для всех проверяемых объектов. Если флажок снят, приложение не записывает событие в журнал. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал события <i>ObjectNotProcessed</i>, если не удастся обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал событие <i>ObjectNotProcessed</i>. Если флажок снят, приложение не записывает событие в журнал. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал события <i>PackedObjectDetected</i> для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал событие <i>PackedObjectDetected</i>. Если флажок снят, приложение не записывает событие в журнал. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке объектов. По умолчанию флажок установлен.

Параметр	Описание
Уровень эвристического анализа	Если флажок Использовать эвристический анализ установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • Поверхностный – наименее детализированная проверка, минимальная нагрузка на систему. • Средний – средняя детализация при проверке, сбалансированная нагрузка на систему. • Глубокий – наиболее детализированная проверка, максимальная нагрузка на систему. • Рекомендованный (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.

В этом разделе

Окно Области защиты	178
Окно добавления области защиты.....	178
Исключения Защиты от файловых угроз.....	182

Окно Области защиты

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область защиты, включающую все директории локальной файловой системы.

Таблица 14. Параметры области защиты

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Industrial CyberSecurity for Linux Nodes проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно добавления области защиты

В этом окне вы можете добавить или настроить область защиты.

Таблица 15. Параметры области защиты

Параметр	Описание
Название области	Поле ввода названия области защиты. Это название будет отображаться в таблице окна Области проверки (см. раздел "Окно Области проверки" на стр. 191). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область защиты во время работы. Если флажок снят, приложение не обрабатывает эту область защиты во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • Локальная (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • Смонтированная – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • Общая – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • Все общие – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип Общая или Смонтированная.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите включить в область защиты. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: [container-id:<идентификатор>]/<путь к локальной директории> [container-name:<название>]/<путь к локальной директории> [image-id:<идентификатор>]/<путь к локальной директории> [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Локальная. Если в раскрывающемся списке файловых систем выбран тип Локальная и не указан путь, приложение проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область защиты. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке Протокол доступа выбран элемент Пользовательский.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Исключения Защиты от файловых угроз

Исключение из защиты – это совокупность условий, при выполнении которых приложение Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет объекты на наличие вирусов и других вредоносных программ. Вы также можете исключать из защиты объекты по маскам и названиям угроз и настраивать исключения для процессов.

В Web Console вы можете настроить исключения Защиты от файловых угроз в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Базовая защита** → **Исключения Защиты от файловых угроз**).

Таблица 16. Параметры исключений из защиты

Параметр	Описание
Области исключения	По ссылке Настроить области исключения открывается окно Области исключения (см. раздел "Окно Области исключения" на стр. 182). В этом окне вы можете задать список исключений из защиты.
Исключения по маске	По ссылке Настроить исключения по маске открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 186). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	По ссылке Настроить исключения по названию угрозы открывается окно Исключения по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 186). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Исключения по процессам	По ссылке Настроить исключения по процессам открывается окно Исключения по процессам . В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 17. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

Таблица 18. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 182). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки или защиты во время своей работы. Если флажок снят, приложение включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • Локальная – локальные директории. • Смонтированная – удаленные директории, смонтированные на устройстве. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип Смонтированная.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: [container-id:<идентификатор>]/<путь к локальной директории> [container-name:<название>]/<путь к локальной директории> [image-id:<идентификатор>]/<путь к локальной директории> [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Локальная.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке Протокол доступа выбран элемент Пользовательский.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле Путь. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса и файлов, изменяемых указанным процессом, из проверки. По умолчанию таблица содержит две области исключения, содержащие пути к Агентам администрирования. Вы можете удалить эти исключения, если требуется.

Таблица 19. Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Таблица 20. Параметры области исключения

Параметр	Описание
Название области исключения по процессам	Поле ввода названия области исключения по процессам. Это название будет отображаться в таблице окна Исключения по процессам . Поле ввода не должно быть пустым.
Использовать / Не использовать это исключение	Переключатель включает или выключает исключение этой области во время работы приложения. По умолчанию переключатель включен.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром Путь к исключаемому процессу . По умолчанию флажок снят.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать исключения из проверки для файлов, которые изменяет процесс. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • Локальная – локальные директории. • Смонтированная – смонтированные директории. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список Протокол доступа доступен, если в раскрывающемся списке файловых систем выбран тип Смонтированная .

Параметр	Описание
Путь	В поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, <code>/dir/*/file</code> или <code>/dir/**/file</code>. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, <code>/dir/**/file*/</code> или <code>/dir/file**/</code>. Маску ** можно использовать в имени директории только один раз. Например, <code>/dir/**/**/file</code> – это неправильная маска. Для исключения точки монтирования <code>/dir</code> требуется указывать именно <code>/dir</code> (без звездочек). Маска <code>/dir/*</code> исключает все точки монтирования на уровень ниже от <code>/dir</code>, но не саму точку монтирования <code>/dir</code>. Маска <code>/dir/**</code> исключает все точки монтирования на любом уровне вложенности под <code>/dir</code>, но не саму точку монтирования <code>/dir</code>. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Локальная.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке Протокол доступа выбран элемент Пользовательский.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в блоке Файловая система, протокол доступа и путь. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Настройка защиты от файловых угроз в Консоли администрирования

В Консоли администрирования вы можете управлять защитой от файловых угроз в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Базовая защита** → **Защита от файловых угроз**).

Таблица 21. Параметры компонента Защита от файловых угроз

Параметр	Описание
Включить Защиту от файловых угроз	Флажок включает или выключает компонент Защита от файловых угроз на всех управляемых устройствах. По умолчанию флажок установлен.
Режим Защиты от файловых угроз	В раскрывающемся списке вы можете выбрать режим работы компонента Защита от файловых угроз: • Интеллектуальный режим (значение по умолчанию) – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс в течение определенного времени многократно обращается к файлу и изменяет его, приложение повторно проверяет файл только при последнем закрытии файла этим процессом. • При открытии – проверять файл при попытке открытия на чтение, исполнение или изменение. • При открытии и изменении – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки (см. раздел "Окно Области проверки" на стр. 191) и параметры проверки (см. раздел "Окно Параметры проверки" на стр. 196).
Действие при обнаружении угрозы	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Действие при обнаружении угрозы (см. раздел "Окно Действие при обнаружении угрозы" на стр. 200), в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В этом разделе

Окно Области проверки	191
Окно <Новая область проверки>.....	192
Окно Параметры проверки	196
Окно Действие при обнаружении угрозы.....	200
Исключения Защиты от файловых угроз.....	201

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Таблица 22. Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки.

Таблица 23. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна Области проверки (см. раздел "Окно Области проверки" на стр. 191). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • Локальная (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • Смонтированная – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • Общая – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • Все общие – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип Общая или Смонтированная, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательская – ресурсы файловой системы устройства, указанные в поле ниже.

Параметр	Описание
	Если в раскрывающемся списке файловых систем выбран тип Локальная, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип Локальная и не указан путь, приложение проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке справа выбран элемент Пользовательская.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы Защиты от файловых угроз.

Таблица 24. Параметры Защиты от файловых угроз

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, включив и настроив параметры Пропускать файл, если его проверка длится более (сек.) и Пропускать файл, если его размер более (МБ) в блоке Общие параметры проверки. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет архивы. По умолчанию флажок снят.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку <i>самораспаковывающихся архивов</i>. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет самораспаковывающиеся архивы. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок Проверять архивы. По умолчанию флажок снят.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет файлы почтовых баз. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет сообщения в текстовом формате. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать текстовые файлы	Временное исключение из проверки файлов в текстовом формате. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов работы приложений. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет текстовые файлы. По умолчанию флажок снят.

Параметр	Описание
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени Kaspersky Industrial CyberSecurity for Linux Nodes прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 60.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectProcessed</i>. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не записывает в журнал события типа <i>ObjectProcessed</i>. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectNotProcessed</i>, если не удастся обработать файл во время проверки. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes записывает в журнал события типа <i>ObjectNotProcessed</i>. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не записывает в журнал события типа <i>ObjectNotProcessed</i>. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа <i>PackedObjectDetected</i> для всех обнаруженных упакованных объектов. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes записывает в журнал события типа <i>PackedObjectDetected</i>. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не записывает в журнал события типа <i>PackedObjectDetected</i>. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.

Параметр	Описание
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок Использовать эвристический анализ установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • Поверхностный – наименее детализированная проверка, минимальная нагрузка на систему. • Средний – средняя детализация при проверке, сбалансированная нагрузка на систему. • Глубокий – наиболее детализированная проверка, максимальная нагрузка на систему. • Рекомендованный (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действие при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Industrial CyberSecurity for Linux Nodes будет выполнять над обнаруженным зараженным объектом.

Таблица 25. Параметры Защиты от файловых угроз

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Блокировать доступ к объекту. • Пропускать объект (значение по умолчанию).
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Блокировать доступ к объекту (значение по умолчанию).

Исключения Защиты от файловых угроз

Исключение из защиты – это совокупность условий, при выполнении которых приложение Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет объекты на наличие вирусов и других вредоносных программ. Вы также можете исключать из защиты объекты по маскам и названиям угроз и настраивать исключения для процессов.

В Консоли администрирования вы можете настроить исключения Защиты от файловых угроз в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Базовая защита** → **Исключения Защиты от файловых угроз**).

Таблица 26. Параметры исключений из проверки

Блок параметров	Описание
Исключения	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области исключения (см. раздел "Окно Области исключения" на стр. 182). В этом окне вы можете задать список областей исключения из проверки.
Исключения по маске	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 206). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 206). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Исключения по процессам	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по процессам . В этом окне вы можете настроить исключение активности процессов из проверки.

В этом разделе

Окно Области исключения.....	202
Окно <Новая область исключения>	202
Окно Исключения по маске	206
Окно Исключения по названию угрозы	206
Окно Исключения по процессам.....	206
Окно Доверенный процесс.....	207

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 27. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Таблица 28. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 182). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • Локальная – локальные директории. • Смонтированная – смонтированные директории. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип Смонтированная, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже.

Параметр	Описание
	Если в раскрывающемся списке файловых систем выбран тип Локальная, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке справа выбран элемент Пользовательская.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса и файлов, изменяемых указанным процессом, из проверки. По умолчанию таблица содержит две области исключения, содержащие пути к Агентам администрирования. Вы можете удалить эти исключения, если требуется.

Таблица 29. Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять (см. раздел "Окно Доверенный процесс" на стр. [207](#)), изменять (см. раздел "Окно Доверенный процесс" на стр. [207](#)) и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Таблица 30. Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Исключения по процессам . Поле ввода не должно быть пустым.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром Путь к исключаемому процессу . По умолчанию флажок снят.
Использовать эту область	Флажок включает или выключает исключение этой области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Путь к изменяемым файлам	Блок параметров позволяет задать исключения из проверки для файлов, которые изменяет процесс. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • Локальная – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • Смонтированная – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • Общая – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • Все общие – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип Смонтированная или Общая , то в раскрывающемся списке протоколов доступа вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип Локальная , то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски. Поле ввода не должно быть пустым.

Параметр	Описание
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке справа выбран элемент Пользовательская .
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в блоке Путь к изменяемым файлам . Вы можете добавлять, изменять и удалять маски.

Настройка защиты от файловых угроз в командной строке

В командной строке вы можете управлять защитой от файловых угроз с помощью предустановленной задачи Защита от файловых угроз (*File_Threat_Protection*).

Если приложение установлено в режиме работы приложения по умолчанию (см. раздел "О режимах работы приложения" на стр. [19](#)), задача Защита от файловых угроз не запущена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) эту задачу вручную.

Для запуска и остановки задачи Защита от файловых угроз из командной строки требуются права роли Администратор (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. [77](#)).

Вы можете настраивать параметры (см. раздел "Параметры задачи Защита от файловых угроз" на стр. [210](#)) защиты от файловых угроз, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи Защита от файловых угроз.

В этом разделе

Параметры задачи Защита от файловых угроз	210
Оптимизация проверки сетевых директорий	222

Параметры задачи Защита от файловых угроз

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Защита от файловых угроз.

Таблица 31. Параметры задачи Защита от файловых угроз

Параметр	Описание	Значения
ScanArchived	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	Yes – проверять архивы. Если указано значение FirstAction=Recommended, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. No (значение по умолчанию) – не проверять архивы.
ScanSfxArchived	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	Yes – проверять самораспаковывающиеся архивы. No (значение по умолчанию) – не проверять самораспаковывающиеся архивы.
ScanMailBases	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	Yes – проверять файлы почтовых баз. No (значение по умолчанию) – не проверять файлы почтовых баз.
ScanPlainMail	Включение проверки сообщений электронной почты в текстовом формате (plain text).	Yes – проверять сообщения электронной почты в текстовом формате. No (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
SkipPlainTextFiles	Временное исключение из проверки файлов в текстовом формате. Если значение этого параметра SkipPlainTextFiles=Yes, приложение не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов работы приложений.	Yes – не проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. No (значение по умолчанию) – проверять файлы в текстовом формате.
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.

Параметр	Описание	Значения
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 60.
FirstAction	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	Disinfect (лечить) – приложение пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано Disinfect, рекомендуется задать второе действие в параметре SecondAction. Remove (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Industrial CyberSecurity for Linux Nodes сразу удаляет троянские приложения, так как они не заражают другие файлы и поэтому не предполагают лечения. Block (блокировать) – приложение блокирует доступ к зараженному объекту. Информация о зараженном объекте сохраняется в журнале. Skip (пропускать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Skip.

Параметр	Описание	Значения
SecondAction	Выбор второго действия, которое приложение будет выполнять над зараженными объектами. Приложение выполняет второе действие, если не удалось выполнить первое действие.	Значения параметра SecondAction такие же, как значения параметра FirstAction. Если в качестве первого действия выбрано Block (блокировать) или Remove (удалять), то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия. Если вы не указали второе действие, приложение в качестве второго действия выполняет Block (блокировать). Значение по умолчанию: Block.
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.item_#.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks.item_#. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.item_#.
ExcludeMasks.item_#	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.	Значение по умолчанию не задано. Пример: UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar 1.* ExcludeMasks.item_0001=eicar 2.*
UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром ExcludeThreats.item_#.	Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#. No (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#.

Параметр	Описание	Значения
ExcludeThreats.item_#	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр UseExcludeThreats. Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным. Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки. Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на сайте https://threats.kaspersky.com.	Значение параметра чувствительно к регистру. Значение по умолчанию не задано. Пример: <pre>UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux</pre>
ReportCleanObjects	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	Yes – записывать в журнал информацию о незараженных объектах. No (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.

Параметр	Описание	Значения
ReportUnprocessedObjects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор. No – выключить эвристический анализатор.
HeuristicLevel	Уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная загрузка системы. Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. Deep – наиболее тщательная проверка, максимальная загрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.
UseIChecker	Включение использования технологии iChecker.	Yes (значение по умолчанию) – включить использование технологии iChecker. No – выключить использование технологии iChecker.
ScanByAccessType	Режим работы задачи Защита от файловых угроз. Этот параметр ScanByAccessType применяется только в задаче Защита от файловых угроз.	SmartCheck (значение по умолчанию) – проверять файл при попытке открытия, и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс во время своей работы многократно обращается к файлу в течение некоторого времени и изменяет его, повторно проверять файл только при последней попытке закрытия файла этим процессом. OpenAndModify – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Open – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.
Секция [ScanScope.item_#] содержит следующие параметры:		

Параметр	Описание	Значения
AreaDesc	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects. Пример: AreaDesc="Проверка почтовых баз"
UseScanArea	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	Yes (значение по умолчанию) – проверять указанную область. No – не проверять указанную область.
AreaMask.item_#	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты). Пример: AreaMask_item_<номер элемента>=*doc

Path	Путь к директории с проверяемыми объектами.	<путь к локальной директории> – проверять объекты в указанной директории. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>] / <путь к локальной директории> • [container-name:<название>] / <путь к локальной директории> • [image-id:<идентификатор>] / <путь к локальной директории> • [image-name:<название>] / <путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>] / <путь к локальной директории>. Shared:NFS – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. Shared:SMB – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. Mounted:NFS – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. Mounted:SMB – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. AllRemoteMounted – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. AllShared – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS.

Параметр	Описание	Значения
		<тип файловой системы> – проверять все ресурсы указанной файловой системы устройства.
Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.
AreaMask.item_#	Ограничение области исключения из проверки. В области исключения приложение не проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает из проверки все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (исключать из проверки все объекты).

Параметр	Описание	Значения
Path	Путь к директории с исключаемыми объектами.	<путь к локальной директории> – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>] / <путь к локальной директории> • [container-name:<название>] / <путь к локальной директории> • [image-id:<идентификатор>] / <путь к локальной директории> • [image-name:<название>] / <путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>] / <путь к локальной директории>. Mounted:NFS – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. Mounted:SMB – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. <тип файловой системы> – исключать из проверки все ресурсы указанной файловой системы устройства.
Секция [ExcludedForProgram.item_#] содержит следующие параметры:		
ProgramPath	Путь к исключаемому процессу.	<полный путь к процессу> – исключать из проверки процесс в указанной локальной директории.

Параметр	Описание	Значения
<code>ApplyToDescendants</code>	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром <code>ProgramPath</code> .	<code>Yes</code> – исключать из проверки указанный процесс и все его дочерние процессы. <code>No</code> (значение по умолчанию) – исключать из проверки только указанный процесс, не исключать из проверки дочерние процессы.
<code>AreaDesc</code>	Описание области исключения процессов.	Значение по умолчанию: <code>All objects</code> .
<code>UseExcludedForProgram</code>	Исключение указанной области из проверки.	<code>Yes</code> (значение по умолчанию) – исключать указанную область. <code>No</code> – не исключать указанную область.
<code>AreaMask.item_#</code>	Ограничение области исключения процессов. В области исключения процессов приложение не проверяет только файлы, указанные помощью масок в формате <code>shell</code> . Если параметр не указан, приложение исключает из проверки все объекты в области исключения процессов. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: <code>*</code> (исключать из проверки все объекты).

Параметр	Описание	Значения
Path	Путь к директории с файлами, которые изменяет процесс.	<путь к локальной директории> – исключать из проверки объекты в указанной директории. Для указания пути можно использовать маски. Shared:NFS – исключать из проверки ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. Shared:SMB – исключать из проверки ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. Mounted:NFS – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. Mounted:SMB – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. AllShared – исключать из проверки все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. <тип файловой системы> – исключать из проверки все ресурсы указанной файловой системы устройства.

Оптимизация проверки сетевых директорий

Для оптимизации защиты от файловых угроз вы можете настроить исключение из проверки файлов, копируемых из сетевых директорий в локальную директорию. Для этого вам нужно настроить исключение по процессам для утилиты, предназначенной для копирования из сетевых директорий (например, для утилиты `cp`).

► Чтобы настроить исключение сетевых директорий из проверки:

1. Выведите (см. раздел "Вывод параметров задачи в командной строке" на стр. 129) параметры задачи Защита от файловых угроз (*File_Threat_Protection*, ID:1) в конфигурационный файл с помощью команды:


```
kics-control --get-settings 1 --file <полный путь к конфигурационному файлу> [--json]
```
2. Откройте конфигурационный файл и добавьте секцию `[ExcludedForProgram.item_#]` со следующими параметрами:

- `ProgramPath` – путь к исключаемому процессу или к директории с исключаемыми процессам.
- `ApplyToDescendants` – параметр, показывающий, нужно ли исключать из проверки дочерние процессы исключаемого процесса (возможные значения: `Yes` или `No`).
- `AreaDesc` – описание области исключения по процессам, содержащее дополнительную информацию об области исключения.
- `UseExcludedForProgram` – включить исключение указанной области при работе задачи (возможные значения: `Yes` или `No`).
- `Path` – путь к файлам или к директории с файлами, которые изменяет процесс.
- `AreaMask.item_#` – маска имени файла для файлов, которые вы хотите исключить из проверки. Вы также можете указать полный путь к файлу.

Пример:

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/cp
ApplyToDescendants=No
AreaDesc=
UseExcludedForProgram=Yes
Path=AllRemoteMounted
AreaMask.item_0000=*
```

3. Выполните команду:

```
kics-control --set-settings 1 --file <полный путь к конфигурационному файлу> [--json]
```

Укажите ключ `--json`, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Приложение не будет проверять файлы в сетевых директориях, при этом сама команда `cp` (для приведенного выше примера) и локальные файлы будут проверяться.

Особенности проверки символических и жестких ссылок

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes позволяет проверять символические и жесткие ссылки на файлы.

Проверка символических ссылок

Приложение проверяет символические ссылки, только если файл, на который ссылается символическая ссылка, входит в область проверки компонента Защита от файловых угроз.

Если файл, обращение к которому происходит по символической ссылке, не входит в область проверки компонента Защита от файловых угроз, приложение не проверяет этот файл. Если такой файл содержит вредоносный код, безопасность устройства окажется под угрозой.

Проверка жестких ссылок

При обработке файла, имеющего больше одной жесткой ссылки, приложение выбирает действие в зависимости от заданного действия над объектами:

- Если выбрано действие **Выполнять рекомендованное действие**, приложение автоматически подбирает и выполняет действие над объектом на основе данных об опасности угрозы, обнаруженной в объекте, и возможности его лечения.
- Если выбрано действие **Удалять**, приложение удаляет обрабатываемую жесткую ссылку. Остальные жесткие ссылки на этот файл обработаны не будут.
- Если выбрано действие **Лечить**, приложение лечит исходный файл. Если лечение невозможно, приложение удаляет жесткую ссылку и создает вместо нее копию исходного файла с именем удаленной жесткой ссылки.

Когда вы восстанавливаете файл с жесткой ссылкой из резервного хранилища (см. раздел "Резервное хранилище" на стр. [586](#)), приложение создает копию исходного файла с именем жесткой ссылки, которая была помещена в резервное хранилище. Связи с остальными жесткими ссылками на исходный файл восстановлены не будут.

Поиск вредоносного ПО

Поиск вредоносного ПО – это однократная полная или выборочная проверка файлов на устройстве по требованию. Приложение Kaspersky Industrial CyberSecurity for Linux Nodes может выполнять несколько задач поиска вредоносного ПО одновременно.

В приложении создается предустановленная задача *Поиск вредоносного ПО (Scan_My_Computer)*. Вы можете использовать эту задачу для выполнения полной проверки устройства. При полной проверке приложение проверяет все объекты, расположенные на локальных дисках устройства, а также все смонтированные и общие объекты, доступ к которым предоставляется по протоколам Samba и NFS, с рекомендуемыми параметрами безопасности.

В Kaspersky Security Center мастер первоначальной настройки Kaspersky Security Center автоматически создает групповую задачу поиска вредоносного ПО после установки mms-плагинов управления или веб-плагинов управления Kaspersky Industrial CyberSecurity for Linux Nodes.

Во время полной проверки диска процессор будет занят. Рекомендуется запускать задачу полной проверки в нерабочее время.

Вы можете настраивать параметры автоматически созданных задач в Kaspersky Security Center и в командной строке, а также создавать пользовательские задачи поиска вредоносного ПО.

При обнаружении вредоносного ПО приложение Kaspersky Industrial CyberSecurity for Linux Nodes может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

Если во время поиска вредоносного ПО приложение было перезапущено контрольной службой или вручную пользователем, выполнение задачи прерывается. В журнале приложения сохраняется событие *OnDemandTaskInterrupted*.

Вы можете запускать задачи поиска вредоносного ПО и настраивать параметры проверки:

- Выбирать объекты операционной системы, которые нужно проверять: файлы, архивы, загрузочные секторы, память процессов и память ядра, объекты автозапуска.
- Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
- Выбирать действия, которые приложение будет выполнять над зараженными объектами.
- Настраивать исключения объектов из проверки:
 - по именам или маскам;
 - по названиям обнаруженных в объектах угроз.
- Включать и выключать использование глобальных исключений и исключений Защиты от файловых угроз при проверке.
- Включать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.
- Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
- Ограничивать набор устройств, загрузочные секторы которых нужно проверять.
- Настраивать области проверки и области исключения из проверки.

В этом разделе

Поиск вредоносного ПО в Web Console.....	226
Поиск вредоносного ПО в Консоли администрирования	238
Поиск вредоносного ПО в командной строке	254

Поиск вредоносного ПО в Web Console

В Web Console вы можете выполнять проверку на наличие вредоносного ПО с помощью задачи *Поиск вредоносного ПО*.

Вы можете запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)) автоматически созданную групповую задачу, а также создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) и запускать пользовательские задачи проверки. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) параметры задач поиска вредоносного ПО.

Таблица 32. Параметры проверки задачи Поиск вредоносного ПО

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры Пропускать файл, если его проверка длится более (сек.) и Пропускать файл, если его размер более (МБ) в блоке Общие параметры проверки. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку <i>самораспаковывающихся архивов</i>. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок Проверять архивы. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.

Параметр	Описание
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectProcessed</i>. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectNotProcessed</i>, если не удастся обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectNotProcessed</i>. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectNotProcessed</i>. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа <i>PackedObjectDetected</i> для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа <i>PackedObjectDetected</i>. Если флажок снят, приложение не записывает в журнал события типа <i>PackedObjectDetected</i>. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок Использовать эвристический анализ установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • Поверхностный – наименее детализированная проверка, минимальная нагрузка на систему. • Средний – средняя детализация при проверке, сбалансированная нагрузка на систему. • Глубокий – наиболее детализированная проверка, максимальная нагрузка на систему. • Рекомендованный (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).
Области проверки	Таблица, содержащая области, проверяемые задачей. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы. Области проверки в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.

В этом разделе

Окно добавления области проверки	230
Раздел Области проверки	233
Окно Области проверки	234
Раздел Области исключения	234
Окно Области исключения	235
Окно добавления области исключения	235
Окно Исключения по маске	238
Окно Исключения по названию угрозы	238

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Таблица 33. Параметры области проверки

Параметр	Описание
Название области	Поле ввода названия области проверки. Это название будет отображаться в таблице Области проверки в разделе Параметры проверки. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • Локальная (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • Смонтированная – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • Общая – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • Все общие – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип Общая или Смонтированная.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. По умолчанию указан путь / – приложение проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Локальная. Если в раскрывающемся списке файловых систем выбран тип Локальная и не указан путь, приложение проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке Протокол доступа выбран элемент Пользовательский.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Раздел Области проверки

Вы можете настроить параметры области проверки для задачи Поиск вредоносного ПО. Приложение позволяет проверять файлы, загрузочные секторы, память клиентского устройства и объекты автозапуска.

Таблица 34. Параметры области проверки задачи Поиск вредоносного ПО

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, приложение проверяет файлы. Если флажок снят, приложение не проверяет файлы. По умолчанию флажок установлен.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, приложение проверяет загрузочные секторы. Если флажок снят, приложение не проверяет загрузочные секторы. По умолчанию флажок снят.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти клиентского устройства. Если флажок установлен, приложение проверяет память ядра и запущенные процессы. Если флажок снят, приложение не проверяет память ядра и запущенные процессы. По умолчанию флажок снят.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, приложение проверяет объекты автозапуска. Если флажок снят, приложение не проверяет объекты автозапуска. По умолчанию флажок снят.
Устройства для проверки	По ссылке Настроить маски устройств открывается окно Области проверки , в котором вы можете указать устройства, загрузочные секторы которых нужно проверить.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Раздел Области исключения

В разделе **Области исключения** для задачи Поиск вредоносного ПО вы можете настроить области исключения (см. раздел "Окно Области исключения" на стр. [182](#)), исключения по маске (см. раздел "Окно Исключения по маске" на стр. [186](#)) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. [186](#)), а также использование глобальных исключений и исключений Защиты от файловых угроз во время работы задачи.

Таблица 35. Параметры исключений из проверки

Параметр	Описание
Настроить области исключения	По ссылке Настроить области исключения открывается окно Области исключения (см. раздел "Окно Области исключения" на стр. 182). В этом окне вы можете задать список исключений из проверки.
Настроить исключения по маске	По ссылке Настроить исключения по маске открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 186). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Настроить исключения по названию угрозы	По ссылке Настроить исключения по названию угрозы открывается окно Исключения по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 186). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях (см. раздел "Настройка глобальных исключений" на стр. 566), во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз (см. раздел "Исключения Защиты от файловых угроз" на стр. 182) во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 36. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

Таблица 37. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 182). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки или защиты во время своей работы. Если флажок снят, приложение включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • Локальная – локальные директории. • Смонтированная – удаленные директории, смонтированные на устройстве. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип Смонтированная.
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Локальная.

Параметр	Описание
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке Протокол доступа выбран элемент Пользовательский .
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле Путь . По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_??*.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Поиск вредоносного ПО в Консоли администрирования

В Консоли администрирования вы можете выполнять проверку на наличие вредоносного ПО с помощью задачи *Поиск вредоносного ПО*.

Вы можете запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Консоли администрирования" на стр. [117](#)) автоматически созданную групповую задачу, а также создавать (см. раздел "Создание задач в Консоли администрирования" на стр. [116](#)) и запускать пользовательские задачи

проверки. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задач в Консоли администрирования" на стр. [117](#)) параметры задач поиска вредоносного ПО.

В разделе **Параметры** в свойствах задачи Поиск вредоносного ПО вы можете настроить параметры, приведенные в таблице ниже.

Таблица 38. Параметры задачи Поиск вредоносного ПО

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки (см. раздел "Окно Области проверки" на стр. 191), параметры области проверки и параметры проверки (см. раздел "Окно Параметры проверки" на стр. 196).
Действие при обнаружении угрозы	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Действие при обнаружении угрозы (см. раздел "Окно Действие при обнаружении угрозы" на стр. 249), в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В разделе **Исключения** (см. раздел "Раздел Исключения" на стр. [341](#)) в свойствах задачи Поиск вредоносного ПО вы можете настроить области исключения (см. раздел "Окно Области исключения" на стр. [202](#)), исключения по маске (см. раздел "Окно Исключения по маске" на стр. [206](#)) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. [206](#)).

В этом разделе

Окно Области проверки	239
Окно <Новая область проверки>	240
Окно Параметры области проверки.....	243
Окно Области проверки	244
Окно Параметры проверки.....	245
Окно Действие при обнаружении угрозы	249
Раздел Исключения	249
Окно Области исключения	250
Окно <Новая область исключения>	250
Окно Исключения по маске	254
Окно Исключения по названию угрозы	254

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Таблица 39. Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Industrial CyberSecurity for Linux Nodes проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки.

Таблица 40. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна Области проверки (см. раздел "Окно Области проверки" на стр. 191). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • Локальная (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • Смонтированная – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • Общая – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • Все общие – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип Общая или Смонтированная, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательская – ресурсы файловой системы устройства, указанные в поле ниже.

Параметр	Описание
	Если в раскрывающемся списке файловых систем выбран тип Локальная, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. По умолчанию указан путь / – приложение проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип Локальная и не указан путь, приложение проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке справа выбран элемент Пользовательская.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Параметры области проверки

В этом окне вы можете настроить параметры проверки во время работы задачи Поиск вредоносного ПО. Приложение позволяет проверять файлы, загрузочные секторы, память устройства и объекты автозапуска.

Таблица 41. Параметры области проверки

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, приложение проверяет файлы. Если флажок снят, приложение не проверяет файлы. По умолчанию флажок установлен.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, приложение проверяет загрузочные секторы. Если флажок снят, приложение не проверяет загрузочные секторы. По умолчанию флажок снят.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти устройства. Если флажок установлен, приложение проверяет память ядра и запущенные процессы. Если флажок снят, приложение не проверяет ядра и запущенные процессы. По умолчанию флажок снят.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, приложение проверяет объекты автозапуска. Если флажок снят, приложение не проверяет объекты автозапуска. По умолчанию флажок снят.
Устройства для проверки	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области проверки (см. раздел "Окно Области проверки" на стр. 234), в котором вы можете указать устройства, загрузочные секторы которых нужно проверить.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях (см. раздел "Настройка глобальных исключений" на стр. 566), во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз (см. раздел "Исключения Защиты от файловых угроз" на стр. 201) во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Таблица 42. Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры Пропускать файл, если его проверка длится более (сек.) и Пропускать файл, если его размер более (МБ) в блоке Общие параметры проверки. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку <i>самораспаковывающихся архивов</i>. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок Проверять архивы. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.

Параметр	Описание
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectProcessed</i>. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectNotProcessed</i>, если не удастся обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectNotProcessed</i>. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectNotProcessed</i>. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа <i>PackedObjectDetected</i> для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа <i>PackedObjectDetected</i>. Если флажок снят, приложение не записывает в журнал события типа <i>PackedObjectDetected</i>. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок Использовать эвристический анализ установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • Поверхностный – наименее детализированная проверка, минимальная нагрузка на систему. • Средний – средняя детализация при проверке, сбалансированная нагрузка на систему. • Глубокий – наиболее детализированная проверка, максимальная нагрузка на систему. • Рекомендованный (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действие при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Industrial CyberSecurity for Linux Nodes будет выполнять над обнаруженным зараженным объектом.

Таблица 43. Действия при обнаружении угрозы

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).

Раздел Исключения

Исключение из проверки – это совокупность условий, при выполнении которых приложение Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете также исключать объекты из проверки по маскам и названиям угроз.

Таблица 44. Параметры исключений из проверки

Блок параметров	Описание
Области исключения	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области исключения . В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 206). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 206). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 45. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Таблица 46. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 182). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • Локальная – локальные директории. • Смонтированная – смонтированные директории. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип Смонтированная, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже.

Параметр	Описание
	Если в раскрывающемся списке файловых систем выбран тип Локальная, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке справа выбран элемент Пользовательская.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Поиск вредоносного ПО в командной строке

В командной строке вы можете выполнять проверку на наличие вредоносного ПО следующими способами:

- С помощью предустановленной задачи Поиск вредоносного ПО (*Scan_My_Computer*). Вы можете запускать, останавливать, приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) эту задачу вручную и настраивать расписание (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)) запуска задачи. Вы можете настраивать параметры (см. раздел "Параметры предустановленной задачи Поиск вредоносного ПО" на стр. [255](#)) проверки, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры этой задачи.
- С помощью пользовательских задач (см. раздел "Создание задачи в командной строке" на стр. [127](#)) поиска вредоносного ПО (задач типа *ODS*). Вы можете запускать, останавливать, приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) пользовательские задачи вручную и настраивать расписание (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)) запуска задач.
- С помощью команды `kics-control --scan-file` вы можете выполнять *выборочную проверку* (см. раздел "*Выборочная проверка файлов и директорий*" на стр. [265](#)) указанных файлов и директорий.

В этом разделе

Параметры предустановленной задачи Поиск вредоносного ПО	255
Выборочная проверка файлов и директорий	265

Параметры предустановленной задачи Поиск вредоносного ПО

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Поиск вредоносного ПО.

Таблица 47. Параметры задачи Поиск вредоносного ПО

Параметр	Описание	Значения
ScanFiles	Включение проверки файлов.	Yes (значение по умолчанию) – проверять файлы. No – не проверять файлы.
ScanBootSectors	Включение проверки загрузочных секторов.	Yes (значение по умолчанию) – проверять загрузочные секторы. No – не проверять загрузочные секторы.
ScanComputerMemory	Включение проверки памяти процессов и памяти ядра.	Yes (значение по умолчанию) – проверять память процессов и память ядра. No – не проверять память процессов и память ядра.
ScanStartupObjects	Включение проверки объектов автозапуска.	Yes (значение по умолчанию) – проверять объекты автозапуска. No – не проверять объекты автозапуска.
ScanArchived	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	Yes (значение по умолчанию) – проверять архивы. Если указано значение FirstAction=Recommended, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. No – не проверять архивы.
ScanSfxArchived	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	Yes (значение по умолчанию) – проверять самораспаковывающиеся архивы. No – не проверять самораспаковывающиеся архивы.
ScanMailBases	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	Yes – проверять файлы почтовых баз. No (значение по умолчанию) – не проверять файлы почтовых баз.
ScanPlainMail	Включение проверки сообщений электронной почты в текстовом формате (plain text).	Yes – проверять сообщения электронной почты в текстовом формате. No (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.

Параметр	Описание	Значения
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
FirstAction	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	Disinfect (лечить) – приложение пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано Disinfect , рекомендуется задать второе действие в параметре SecondAction . Remove (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Industrial CyberSecurity for Linux Nodes сразу удаляет троянские приложения, так как они не заражают другие файлы и поэтому не предполагают лечения. Skip (пропускать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Skip .

Параметр	Описание	Значения
SecondAction	Выбор второго действия, которое приложение будет выполнять над зараженными объектами. Приложение выполняет второе действие, если не удалось выполнить первое действие.	Значения параметра SecondAction такие же, как значения параметра FirstAction. Если в качестве первого действия выбрано Skip (пропускать) или Remove (удалять), то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия. Если вы не указали второе действие, приложение в качестве второго действия выполняет Skip (пропускать). Значение по умолчанию: Skip.
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.item_#.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks.item_#. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.item_#.
ExcludeMasks.item_#	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр UseExcludeMasks.	Значение по умолчанию не задано. Пример: UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar 1.* ExcludeMasks.item_0001=eicar 2.*
UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром ExcludeThreats.item_#.	Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#. No (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#.

Параметр	Описание	Значения
ExcludeThreats.item_#	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр UseExcludeThreats. Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным. Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки. Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на сайте https://threats.kaspersky.com.	Значение параметра чувствительно к регистру. Значение по умолчанию не задано. Пример: <pre>UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux</pre>
UseGlobalExclusions	Включение использования глобальных исключений (см. раздел "Настройка глобальных исключений" на стр. 566) при проверке.	Yes (значение по умолчанию) – использовать глобальные исключения. No – не использовать глобальные исключения.
UseOASExclusions	Включение использования исключений Защиты от файловых угроз (см. раздел "Защита от файловых угроз" на стр. 172) при проверке.	Yes (значение по умолчанию) – использовать исключения Защиты от файловых угроз. No – не использовать исключения Защиты от файловых угроз.
ReportCleanObjects	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	Yes – записывать в журнал информацию о незараженных объектах. No (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.

Параметр	Описание	Значения
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
ReportUnprocessedObjects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор. No – выключить эвристический анализатор.
HeuristicLevel	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная загрузка системы. Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. Deep – наиболее тщательная проверка, максимальная загрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.
UseIChecker	Включение использования технологии iChecker.	Yes (значение по умолчанию) – включить использование технологии iChecker. No – выключить использование технологии iChecker.

Параметр	Описание	Значения
DeviceNameMask s.item_#	Список названий устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску названия устройства.	AllObjects – проверять загрузочные секторы всех устройств. <маска названия устройства> – проверять загрузочные секторы устройств, названия которых содержат указанную маску. Значение по умолчанию: /** – любой набор символов в названии устройства, включая символ /.
Секция [ScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects. Пример: AreaDesc="Mail bases scan"
UseScanArea	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	Yes (значение по умолчанию) – проверять указанную область. No – не проверять указанную область.
AreaMask.item_#	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты). Пример: AreaMask.item_<номер элемента>=*doc

Параметр	Описание	Значения
Path	Путь к директории с проверяемыми объектами.	<путь к локальной директории> – проверять объекты в указанной директории. Shared:NFS – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. Shared:SMB – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. Mounted:NFS – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. Mounted:SMB – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. AllRemoteMounted – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. AllShared – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. <тип файловой системы> – проверять все ресурсы указанной файловой системы устройства.
Секция [ExcludedFromScanScope.item_#] содержит следующие параметры.		
AreaDesc	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.

Параметр	Описание	Значения
AreaMask.item_ #	Ограничение области исключения из проверки. В области исключения приложение исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (исключать все объекты).
Path	Путь к директории с исключаемыми объектами.	<путь к локальной директории> – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски. В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида <code>/.snapshots/*/snapshot/</code>. Mounted:NFS – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. Mounted:SMB – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. <тип файловой системы> – исключать из проверки все ресурсы указанной файловой системы устройства. Удаленные директории исключаются из проверки приложением, только если они были смонтированы до запуска задачи. Удаленные директории, смонтированные после запуска задачи, из проверки не исключаются.

Выборочная проверка файлов и директорий

Вы можете выполнять выборочную проверку указанных файлов и директорий с помощью команды (см. раздел "Команды управления задачами" на стр. [682](#)) `kics-control --scan-file`.

Выборочная проверка выполняется с параметрами, которые хранятся в предустановленной задаче *Scan_File* (ID:3). Вы можете настраивать параметры выборочной проверки файлов, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры этой задачи (см. таблицу ниже).

- Чтобы запустить выборочную проверку указанных файлов и директорий, выполните следующую команду:

```
kics-control --scan-file <путь> [--action <действие>]
```

где:

- `<путь>` – путь к файлу или директории, которые вы хотите проверить. Вы можете указать несколько путей, разделяя их пробелами.
- `--action <действие>` – действие, которое приложение будет выполнять над зараженными объектами. Если вы не укажете ключ `--action`, приложение будет выполнять действие `Skip`.

В результате выполнения команды создается временная задача проверки файлов, которая автоматически удаляется после завершения. При этом в консоль выводятся результаты проверки.

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи *Scan_File*.

Секции `[ScanScope.item_#]` и `[ExcludedFromScanScope.item_#]`, заданные в задаче *Scan_File*, не учитываются при выполнении выборочной проверки.

Таблица 48. Параметры задачи Scan_File

Параметр	Описание	Значения
ScanFiles	Включение проверки файлов.	Yes (значение по умолчанию) – проверять файлы. No – не проверять файлы.
ScanBootSectors	Включение проверки загрузочных секторов.	Yes – проверять загрузочные секторы. No (значение по умолчанию) – не проверять загрузочные секторы.
ScanComputerMemory	Включение проверки памяти процессов и памяти ядра.	Yes – проверять память процессов и память ядра. No (значение по умолчанию) – не проверять память процессов и память ядра.
ScanStartupObjects	Включение проверки объектов автозапуска.	Yes – проверять объекты автозапуска. No (значение по умолчанию) – не проверять объекты автозапуска.
ScanArchived	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	Yes (значение по умолчанию) – проверять архивы. Если указано значение FirstAction=Recommended, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. No – не проверять архивы.
ScanSfxArchived	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	Yes (значение по умолчанию) – проверять самораспаковывающиеся архивы. No – не проверять самораспаковывающиеся архивы.
ScanMailBases	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других.	Yes – проверять файлы почтовых баз. No (значение по умолчанию) – не проверять файлы почтовых баз.
ScanPlainMail	Включение проверки сообщений электронной почты в текстовом формате (plain text).	Yes – проверять сообщения электронной почты в текстовом формате. No (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.

Параметр	Описание	Значения
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
FirstAction	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	Disinfect (лечить) – приложение пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано Disinfect , рекомендуется задать второе действие в параметре SecondAction . Remove (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Industrial CyberSecurity for Linux Nodes сразу удаляет троянские приложения, так как они не заражают другие файлы и поэтому не предполагают лечения. Skip (пропускать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Skip .
SecondAction	Выбор второго действия, которое приложение будет выполнять над зараженными объектами. Приложение выполняет второе действие, если не удалось выполнить первое действие.	Значения параметра SecondAction такие же, как значения параметра FirstAction . Если в качестве первого действия выбрано Skip (пропускать) или Remove (удалять), то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия. Если вы не указали второе действие, приложение в качестве второго действия выполняет Skip (пропускать). Значение по умолчанию: Skip .

Параметр	Описание	Значения
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.item_#.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks.item_#. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.item_#.
ExcludeMasks.item_#	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.	Значение по умолчанию не задано. Пример: UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром ExcludeThreats.item_#.	Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#. No (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#.
ExcludeThreats.item_#	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр UseExcludeThreats. Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным. Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки. Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на сайте https://threats.kaspersky.com .	Значение параметра чувствительно к регистру. Значение по умолчанию не задано. Пример: UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux

Параметр	Описание	Значения
UseGlobalExclusions	Включение использования глобальных исключений (см. раздел "Настройка глобальных исключений" на стр. 566) при проверке.	Yes (значение по умолчанию) – использовать глобальные исключения. No – не использовать глобальные исключения.
UseOASExclusions	Включение использования исключений Защиты от файловых угроз (см. раздел "Защита от файловых угроз" на стр. 172) при проверке.	Yes (значение по умолчанию) – использовать исключения Защиты от файловых угроз. No – не использовать исключения Защиты от файловых угроз.
ReportCleanObjects	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	Yes – записывать в журнал информацию о незараженных объектах. No (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
ReportUnprocessedObjects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор. No – выключить эвристический анализатор.

Параметр	Описание	Значения
HeuristicLevel	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная загрузка системы. Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. Deep – наиболее тщательная проверка, максимальная загрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.
UseIChecker	Включение использования технологии iChecker.	Yes (значение по умолчанию) – включить использование технологии iChecker. No – выключить использование технологии iChecker.
DeviceNameMasks.item_#	Список названий устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску названия устройства.	AllObjects – проверять загрузочные секторы всех устройств. <маска названия устройства> – проверять загрузочные секторы устройств, названия которых содержат указанную маску. Значение по умолчанию: /* – любой набор символов в названии устройства, включая символ /.
Секция [ScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects. Пример: AreaDesc="Проверка почтовых баз"
UseScanArea	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	Yes (значение по умолчанию) – проверять указанную область. No – не проверять указанную область.

Параметр	Описание	Значения
AreaMask.item_#	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты). Пример: <pre>AreaMask.item_<номер элемента>=*doc</pre>
Path	Путь к директории с проверяемыми объектами.	<путь к локальной директории> – проверять объекты в указанной директории. Shared:NFS – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. Shared:SMB – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. Mounted:NFS – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. Mounted:SMB – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. AllRemoteMounted – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. AllShared – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. <тип файловой системы> – проверять все ресурсы указанной файловой системы устройства.
Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.

Параметр	Описание	Значения
AreaMask.item_ #	Ограничение области исключения из проверки. В области исключения приложение исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (исключать все объекты).
Path	Путь к директории с исключаемыми объектами.	<путь к локальной директории> – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски. В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида /.snapshots/*/snapshot/. Mounted:NFS – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. Mounted:SMB – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. <тип файловой системы> – исключать из проверки все ресурсы указанной файловой системы устройства. Удаленные директории исключаются из проверки приложением, только если они были смонтированы до запуска задачи. Удаленные директории, смонтированные после запуска задачи, из проверки не исключаются.

Проверка важных областей

Во время проверки важных областей приложение Kaspersky Industrial CyberSecurity for Linux Nodes может проверять загрузочные секторы, объекты автозапуска, память процессов и память ядра.

При обнаружении вредоносного ПО приложение может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

Вы можете запускать проверку важных областей и настраивать параметры проверки:

- Выбирать объекты операционной системы, которые нужно проверять. По умолчанию включена проверка загрузочных секторов, памяти процессов и памяти ядра, объектов автозапуска и архивов. Файлы по умолчанию не проверяются во время проверки важных областей.
- Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
- Выбирать действия, которые приложение будет выполнять над зараженными объектами.
- Настраивать исключения объектов из проверки:
 - по именам или маскам;
 - по названиям обнаруженных в объектах угроз.
- Включать и выключать использование при проверке глобальных исключений и исключений Защиты от файловых угроз.
- Включать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.
- Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
- Ограничивать набор устройств, загрузочные секторы которых нужно проверять.
- Настраивать области проверки и области исключения из проверки.

В этом разделе

Проверка важных областей в Web Console.....	274
Проверка важных областей в Консоли администрирования	287
Проверка важных областей в командной строке	304

Проверка важных областей в Web Console

В Web Console вы можете выполнять проверку важных областей операционной системы защищаемого устройства с помощью задачи *Проверка важных областей*.

Вы можете создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)) пользовательские задачи проверки важных областей. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) параметры задач.

Таблица 49. Параметры задачи Проверка важных областей

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры Пропускать файл, если его проверка длится более (сек.) и Пропускать файл, если его размер более (МБ) в блоке Общие параметры проверки. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку <i>самораспаковывающихся архивов</i>. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок Проверять архивы. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.

Параметр	Описание
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectProcessed</i>. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectNotProcessed</i>, если не удастся обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectNotProcessed</i>. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectNotProcessed</i>. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа <i>PackedObjectDetected</i> для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа <i>PackedObjectDetected</i>. Если флажок снят, приложение не записывает в журнал события типа <i>PackedObjectDetected</i>. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок Использовать эвристический анализ установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • Поверхностный – наименее детализированная проверка, минимальная нагрузка на систему. • Средний – средняя детализация при проверке, сбалансированная нагрузка на систему. • Глубокий – наиболее детализированная проверка, максимальная нагрузка на систему. • Рекомендованный (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).
Области проверки	Таблица, содержащая области, проверяемые задачей. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы. Области проверки в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.

В этом разделе

Окно добавления области проверки	278
Раздел Области проверки.....	282
Окно Области проверки	282
Раздел Области исключения	282
Окно Области исключения	283
Окно добавления области исключения	283
Окно Исключения по маске	287
Окно Исключения по названию угрозы	287

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Таблица 50. Параметры области проверки

Параметр	Описание
Название области	Поле ввода названия области проверки. Это название будет отображаться в таблице Области проверки в разделе Параметры проверки. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • Локальная (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • Смонтированная – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • Общая – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • Все общие – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип Общая или Смонтированная.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Локальная. Если в раскрывающемся списке файловых систем выбран тип Локальная и не указан путь, приложение проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке Протокол доступа выбран элемент Пользовательский.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Раздел Области проверки

Таблица 51. Параметры области проверки задачи Проверка важных областей

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, приложение проверяет файлы. Если флажок снят, приложение не проверяет файлы. По умолчанию флажок снят.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, приложение проверяет загрузочные секторы. Если флажок снят, приложение не проверяет загрузочные секторы. По умолчанию флажок установлен.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти клиентского устройства. Если флажок установлен, приложение проверяет память ядра и запущенные процессы. Если флажок снят, приложение не проверяет память ядра и запущенные процессы. По умолчанию флажок установлен.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, приложение проверяет объекты автозапуска. Если флажок снят, приложение не проверяет объекты автозапуска. По умолчанию флажок установлен.
Устройства для проверки	По ссылке Настроить маски устройств открывается окно Области проверки , в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

Раздел Области исключения

В разделе **Области исключения** для задачи Проверка важных областей вы можете настроить области исключения (см. раздел "Окно Области исключения" на стр. [182](#)), исключения по маске (см. раздел "Окно Исключения по маске" на стр. [186](#)) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. [186](#)), а также использование глобальных исключений и исключений Защиты от файловых угроз во время работы задачи.

Таблица 52. Параметры исключений из проверки

Параметр	Описание
Настроить области исключения	По ссылке Настроить области исключения открывается окно Области исключения (см. раздел "Окно Области исключения" на стр. 182). В этом окне вы можете задать список исключений из проверки.
Настроить исключения по маске	По ссылке Настроить исключения по маске открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 186). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Настроить исключения по названию угрозы	По ссылке Настроить исключения по названию угрозы открывается окно Исключения по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 186). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях (см. раздел "Настройка глобальных исключений" на стр. 566), во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз (см. раздел "Исключения Защиты от файловых угроз" на стр. 182) во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 53. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

Таблица 54. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 182). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки или защиты во время своей работы. Если флажок снят, приложение включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • Локальная – локальные директории. • Смонтированная – удаленные директории, смонтированные на устройстве. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип Смонтированная.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Локальная.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке Протокол доступа выбран элемент Пользовательский.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле Путь. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Удалить** Kaspersky Industrial CyberSecurity for Linux Nodes удаляет выбранную угрозу из списка исключений.

Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Проверка важных областей в Консоли администрирования

В Консоли администрирования вы можете выполнять проверку важных областей операционной системы защищаемого устройства с помощью задачи *Проверка важных областей*.

Вы можете создавать (см. раздел "Создание задач в Консоли администрирования" на стр. [116](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Консоли администрирования" на стр. [117](#)) пользовательские задачи проверки важных областей. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задач в Консоли администрирования" на стр. [117](#)) параметры задач.

В разделе **Параметры** в свойствах задачи Проверка важных областей вы можете настроить параметры, приведенные в таблице ниже.

Таблица 55. Параметры задачи Проверка важных областей

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки (см. раздел "Окно Области проверки" на стр. 191), параметры области проверки и параметры проверки (см. раздел "Окно Параметры проверки" на стр. 196).
Действие при обнаружении угрозы	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Действие при обнаружении угрозы , в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В разделе **Исключения** (см. раздел "**Раздел Исключения**" на стр. [341](#)) в свойствах задачи Проверка важных областей вы можете настроить области исключения (см. раздел "Окно Области исключения" на стр. [202](#)), исключения по маске (см. раздел "Окно Исключения по маске" на стр. [206](#)) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. [206](#)).

В этом разделе

Окно Области проверки	288
Окно <Новая область проверки>	289
Окно Параметры области проверки	293
Окно Области проверки	295
Окно Параметры проверки	295
Окно Действие при обнаружении угрозы	299
Раздел Исключения	299
Окно Области исключения	300
Окно <Новая область исключения>	300
Окно Исключения по маске	304
Окно Исключения по названию угрозы	304

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Таблица 56. Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Industrial CyberSecurity for Linux Nodes проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки.

Таблица 57. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна Области проверки (см. раздел "Окно Области проверки" на стр. 191). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • Локальная (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • Смонтированная – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • Общая – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • Все общие – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип Общая или Смонтированная, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательская – ресурсы файловой системы устройства, указанные в поле ниже.

Параметр	Описание
	Если в раскрывающемся списке файловых систем выбран тип Локальная, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип Локальная и не указан путь, приложение проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке справа выбран элемент Пользовательская.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Параметры области проверки

В этом окне вы можете настроить параметры проверки во время работы задачи Проверка важных областей. Приложение позволяет проверять файлы, загрузочные секторы, объекты автозапуска, память процесса и память ядра.

Таблица 58. Параметры области проверки

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет файлы. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет файлы. По умолчанию флажок снят.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет загрузочные секторы. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет загрузочные секторы. По умолчанию флажок установлен.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти устройства. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет память ядра и запущенные процессы. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет память ядра и запущенные процессы. По умолчанию флажок установлен.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет объекты автозапуска. Если флажок снят, Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет объекты автозапуска. По умолчанию флажок установлен.
Устройства для проверки	Блок параметров содержит кнопку Настроить, по нажатию на которую открывается окно Области проверки (см. раздел "Окно Области проверки" на стр. 234), в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях (см. раздел "Настройка глобальных исключений" на стр. 566), во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз (см. раздел "Исключения Защиты от файловых угроз" на стр. 201) во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Таблица 59. Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры Пропускать файл, если его проверка длится более (сек.) и Пропускать файл, если его размер более (МБ) в блоке Общие параметры проверки. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку <i>самораспаковывающихся архивов</i>. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок Проверять архивы. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.

Параметр	Описание
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectProcessed</i>. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectNotProcessed</i>, если не удастся обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectNotProcessed</i>. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectNotProcessed</i>. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа <i>PackedObjectDetected</i> для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа <i>PackedObjectDetected</i>. Если флажок снят, приложение не записывает в журнал события типа <i>PackedObjectDetected</i>. По умолчанию флажок снят.
	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок Использовать эвристический анализ установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • Поверхностный – наименее детализированная проверка, минимальная нагрузка на систему. • Средний – средняя детализация при проверке, сбалансированная нагрузка на систему. • Глубокий – наиболее детализированная проверка, максимальная нагрузка на систему. • Рекомендованный (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действие при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Industrial CyberSecurity for Linux Nodes будет выполнять над обнаруженным зараженным объектом.

Таблица 60. Действия при обнаружении угрозы

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).

Раздел Исключения

Исключение из проверки – это совокупность условий, при выполнении которых приложение Kaspersky Industrial CyberSecurity for Linux Nodes не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете также исключать объекты из проверки по маскам и названиям угроз.

Таблица 61. Параметры исключений из проверки

Блок параметров	Описание
Области исключения	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области исключения . В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 206). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 206). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 62. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Таблица 63. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 182). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • Локальная – локальные директории. • Смонтированная – смонтированные директории. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип Смонтированная, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже.

Параметр	Описание
	Если в раскрывающемся списке файловых систем выбран тип Локальная, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке справа выбран элемент Пользовательская.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Проверка важных областей в командной строке

В командной строке вы можете выполнять проверку важных областей операционной системы защищаемого устройства с помощью предустановленной задачи Проверка важных областей (*Critical_Areas_Scan*).

Вы можете запускать, останавливать, приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) эту задачу вручную и настраивать расписание (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)) запуска задачи. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры этой задачи.

Таблица 64. Параметры задачи Проверка важных областей

Параметр	Описание	Значения
ScanFiles	Включение проверки файлов.	Yes – проверять файлы. No (значение по умолчанию) – не проверять файлы.
ScanBootSectors	Включение проверки загрузочных секторов.	Yes (значение по умолчанию) – проверять загрузочные секторы. No – не проверять загрузочные секторы.
ScanComputerMemory	Включение проверки памяти процессов и памяти ядра.	Yes (значение по умолчанию) – проверять память процессов и память ядра. No – не проверять память процессов и память ядра.
ScanStartupObjects	Включение проверки объектов автозапуска.	Yes (значение по умолчанию) – проверять объекты автозапуска. No – не проверять объекты автозапуска.
ScanArchived	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	Yes (значение по умолчанию) – проверять архивы. Если указано значение FirstAction=Recommended, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. No – не проверять архивы.
ScanSfxArchived	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	Yes (значение по умолчанию) – проверять самораспаковывающиеся архивы. No – не проверять самораспаковывающиеся архивы.
ScanMailBases	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	Yes – проверять файлы почтовых баз. No (значение по умолчанию) – не проверять файлы почтовых баз.
ScanPlainMail	Включение проверки сообщений электронной почты в текстовом формате (plain text).	Yes – проверять сообщения электронной почты в текстовом формате. No (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.

Параметр	Описание	Значения
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
FirstAction	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	Disinfect (лечить) – приложение пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано Disinfect , рекомендуется задать второе действие в параметре SecondAction . Remove (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Industrial CyberSecurity for Linux Nodes сразу удаляет троянские приложения, так как они не заражают другие файлы и поэтому не предполагают лечения. Skip (пропускать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Skip .

Параметр	Описание	Значения
SecondAction	Выбор второго действия, которое приложение будет выполнять над зараженными объектами. Приложение выполняет второе действие, если не удалось выполнить первое действие.	Значения параметра SecondAction такие же, как значения параметра FirstAction. Если в качестве первого действия выбрано Skip (пропускать) или Remove (удалять), то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия. Если вы не указали второе действие, приложение в качестве второго действия выполняет Skip (пропускать). Значение по умолчанию: Skip.
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.item_#.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks.item_#. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.item_#.
ExcludeMasks.item_#	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр UseExcludeMasks.	Значение по умолчанию не задано. Пример: UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar 1.* ExcludeMasks.item_0001=eicar 2.*
UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром ExcludeThreats.item_#.	Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#. No (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#.

Параметр	Описание	Значения
ExcludeThreats.item_#	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр UseExcludeThreats. Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным. Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки. Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на сайте https://threats.kaspersky.com.	Значение параметра чувствительно к регистру. Значение по умолчанию не задано. Пример: <pre>UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux</pre>
UseGlobalExclusions	Включение использования глобальных исключений (см. раздел "Настройка глобальных исключений" на стр. 566) при проверке.	Yes (значение по умолчанию) – использовать глобальные исключения. No – не использовать глобальные исключения.
UseOASExclusions	Включение использования исключений Защиты от файловых угроз (см. раздел "Защита от файловых угроз" на стр. 172) при проверке.	Yes (значение по умолчанию) – использовать исключения Защиты от файловых угроз. No – не использовать исключения Защиты от файловых угроз.
ReportCleanObjects	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	Yes – записывать в журнал информацию о незараженных объектах. No (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.

Параметр	Описание	Значения
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
ReportUnprocessedObjects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор. No – выключить эвристический анализатор.
HeuristicLevel	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная загрузка системы. Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. Deep – наиболее тщательная проверка, максимальная загрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.
UseIChecker	Включение использования технологии iChecker.	Yes (значение по умолчанию) – включить использование технологии iChecker. No – выключить использование технологии iChecker.

Параметр	Описание	Значения
DeviceNameMask s.item_#	Список названий устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску названия устройства.	AllObjects – проверять загрузочные секторы всех устройств. <маска имени устройства> – проверять загрузочные секторы устройств, названия которых содержат указанную маску. Значение по умолчанию: /** – любой набор символов в названии устройства, включая символ /.
Секция [ScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects. Пример: AreaDesc="Mail bases scan"
UseScanArea	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	Yes (значение по умолчанию) – проверять указанную область. No – не проверять указанную область.
AreaMask.item_#	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты). Пример: AreaMask.item_<номер элемента>=*doc

Параметр	Описание	Значения
Path	Путь к директории с проверяемыми объектами.	<путь к локальной директории> – проверять объекты в указанной директории. Shared:NFS – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. Shared:SMB – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. Mounted:NFS – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. Mounted:SMB – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. AllRemoteMounted – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. AllShared – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. <тип файловой системы> – проверять все ресурсы указанной файловой системы устройства.
Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.

Параметр	Описание	Значения
AreaMask.item_ #	Ограничение области исключения из проверки. В области исключения приложение исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (исключать все объекты).
Path	Путь к директории с исключаемыми объектами.	<путь к локальной директории> – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски. В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида <pre>/.snapshots/*/snapshot/.</pre> Mounted:NFS – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. Mounted:SMB – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. <тип файловой системы> – исключать из проверки все ресурсы указанной файловой системы устройства. Удаленные директории исключаются из проверки приложением, только если они были смонтированы до запуска задачи. Удаленные директории, смонтированные после запуска задачи, из проверки не исключаются.

Проверка съемных дисков

Kaspersky Industrial CyberSecurity for Linux Nodes может проверять следующие съемные диски при подключении их к защищаемому устройству: CD/DVD-приводы, Blu-ray диски, флеш-накопители (включая USB-модемы), внешние жесткие диски и дискеты.

Если проверка съемных дисков включена, приложение Kaspersky Industrial CyberSecurity for Linux Nodes контролирует подключение съемных дисков к защищаемому устройству и при обнаружении подключенного съемного диска проверяет диск и его загрузочные секторы на вирусы и другие вредоносные программы.

По умолчанию приложение не контролирует подключение съемных дисков и не проверяет их.

В этом разделе

Настройка проверки съемных дисков в Web Console.....	314
Настройка проверки съемных дисков в Консоли администрирования	316
Настройка проверки съемных дисков в командной строке	318

Настройка проверки съемных дисков в Web Console

В Web Console вы можете настраивать параметры проверки съемных дисков в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения → Локальные задачи → Проверка съемных дисков**).

Таблица 65. Параметры компонента Проверка съемных дисков

Параметр	Описание
Проверка съемных дисков включена / выключена	Переключатель включает или выключает проверку съемных дисков при подключении их к устройству пользователя. По умолчанию переключатель выключен.
Действие при подключении съемного диска	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять приложение при подключении съемных дисков к устройству пользователя: • Не проверять съемные диски при подключении (значение по умолчанию). • Быстрая проверка – проверять на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков) только файлы определенных типов и не распаковывать составные объекты. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи <i>Проверка важных областей</i>. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • Подробная проверка – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи <i>Поиск вредоносного ПО</i>.
Действие при подключении CD/DVD-привода	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять приложение при подключении CD/DVD-приводов и Blu-ray дисков к устройству пользователя: • Не проверять CD/DVD-приводы и Blu-ray диски при подключении (значение по умолчанию). • Быстрая проверка – проверять на CD/DVD-приводах и Blu-ray дисках только файлы определенных типов. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи <i>Проверка важных областей</i>. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • Подробная проверка – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи <i>Поиск вредоносного ПО</i>.
Блокировать доступ к съемному диску во время проверки	Флажок включает или выключает блокировку файлов на подключенном диске во время выполнения проверки. По умолчанию флажок снят.

Настройка проверки съемных дисков в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры проверки съемных дисков в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Локальные задачи → Проверка съемных дисков**).

Таблица 66. Параметры компонента Проверка съемных дисков

Параметр	Описание
Включить проверку съемных дисков при подключении к устройству	Флажок включает или выключает проверку съемных дисков при подключении их к устройству пользователя. По умолчанию флажок снят.
Действие при подключении съемного диска	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять приложение при подключении съемных дисков к устройству пользователя: • Не проверять съемные диски при подключении (значение по умолчанию). • Быстрая проверка – проверять на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков) только файлы определенных типов и не распаковывать составные объекты. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи <i>Проверка важных областей</i>. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • Подробная проверка – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи <i>Поиск вредоносного ПО</i>.
Действие при подключении CD/DVD-привода	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять приложение при подключении CD/DVD-приводов и Blu-ray дисков к устройству пользователя: • Не проверять CD/DVD-приводы и Blu-ray диски при подключении (значение по умолчанию). • Быстрая проверка – проверять на CD/DVD-приводах и Blu-ray дисках только файлы определенных типов. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи <i>Проверка важных областей</i>. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • Подробная проверка – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи <i>Поиск вредоносного ПО</i>.
Блокировать доступ к съемному диску во время проверки	Флажок включает или выключает блокировку файлов на подключенном диске во время выполнения проверки. По умолчанию флажок снят.

Настройка проверки съемных дисков в командной строке

В командной строке вы можете управлять проверкой съемных дисков с помощью предустановленной задачи Проверка съемных дисков (*Removable_Drives_Scan*).

По умолчанию задача Проверка съемных дисков не запущена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) эту задачу вручную. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры этой задачи.

Если задача запущена, приложение контролирует подключение съемных дисков к устройству и при подключении съемного диска создает и запускает временную задачу проверки загрузочных секторов (задачу типа (см. раздел "Управление задачами в командной строке" на стр. [119](#)) ODS). Эту задачу остановить невозможно. После завершения выполнения задачи приложение автоматически ее удаляет.

Если в параметрах задачи Проверка съемных дисков вы включили проверку файлов, приложение также запускает одну или несколько временных задач выборочной проверки файлов (задачи типа (см. раздел "Управление задачами в командной строке" на стр. [119](#)) ODS). Если требуется, пользователь с правами администратора может останавливать выполнение таких задач.

При изменении параметров задачи Проверка съемных дисков новые значения не применяются к уже запущенным временным задачам. При остановке задачи Проверка съемных дисков уже запущенные временные задачи не останавливаются.

Таблица 67. Параметры задачи Проверка съемных дисков

Параметр	Описание	Значения
ScanRemovableDrives	Включение проверки съемных дисков при подключении к устройству. Этот параметр не применяется к CD/DVD-приводам и Blu-ray дискам (см. параметр ScanOpticalDrives).	DetailedScan – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). Детализированная проверка выполняется с параметрами, которые заданы по умолчанию (см. раздел "Параметры по умолчанию задачи Scan_File (ID:3)" на стр. 714) для задачи Scan_File (ID:3). QuickScan – проверять на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков) только файлы определенных типов. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию (см. раздел "Параметры по умолчанию задачи Critical_Areas_Scan (ID:4)" на стр. 715) для задачи Critical_Areas_Scan (ID:4). NoScan (значение по умолчанию) – не проверять съемные диски при подключении.

Параметр	Описание	Значения
ScanOpticalDrives	Включение проверки CD/DVD-приводов и Blu-ray дисков при подключении к устройству.	DetailedScan – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. Детализированная проверка выполняется с параметрами, которые заданы по умолчанию (см. раздел "Параметры по умолчанию задачи Scan_File (ID:3)" на стр. 714) для задачи Scan_File (ID:3). QuickScan – проверять на CD/DVD-приводах и Blu-ray дисках только файлы определенных типов. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию (см. раздел "Параметры по умолчанию задачи Critical_Areas_Scan (ID:4)" на стр. 715) для задачи Critical_Areas_Scan (ID:4). NoScan (значение по умолчанию) – не проверять CD/DVD-приводы и Blu-ray диски при подключении.
BlockDuringScan	Включение блокировки файлов на подключенном диске при проверке. При проверке загрузочных секторов файлы не блокируются.	Yes – блокировать файлы при проверке. No (значение по умолчанию) – не блокировать файлы при проверке.

Проверка контейнеров

Вы можете выполнять проверку контейнеров и образов на наличие вредоносного ПО в режиме реального времени и по требованию:

- Компонент *Мониторинг контейнеров* (на стр. [322](#)) позволяет проверять запускаемые контейнеры и пространства имен в реальном времени.
- С помощью задач *Проверка контейнеров* (см. раздел "*Проверка контейнеров и образов по требованию*" на стр. [328](#)) вы можете выполнять проверку контейнеров и образов по требованию.

Приложение поддерживает интеграцию с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

В этом разделе

Мониторинг контейнеров.....	322
Проверка контейнеров и образов по требованию	328

Мониторинг контейнеров

Компонент Мониторинг контейнеров может проверять в реальном времени запущенные контейнеры и пространства имен.

Для работы компонента Мониторинг контейнеров должен быть включен компонент Защита от файловых угроз (на стр. [172](#)). Во время проверки контейнеров и пространств имен используются параметры защиты от файловых угроз.

Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен. При этом статус компонента (см. раздел "*Просмотр состояния защиты устройства и параметров приложения*" на стр. [147](#)) Мониторинг контейнеров в командной строке отображается как "Задача доступна и не выполняется", в Kaspersky Security Center отображается как "Остановлена".

Вы можете включать и выключать компонент Мониторинг контейнеров, а также настраивать параметры проверки контейнеров и пространств имен в реальном времени:

- Выбирать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта.
- Настраивать интеграцию приложения Kaspersky Industrial CyberSecurity for Linux Nodes с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

В этом разделе

Настройка мониторинга контейнеров в Web Console.....	323
Настройка мониторинга контейнеров в Консоли администрирования	325
Настройка мониторинга контейнеров в командной строке	326

Настройка мониторинга контейнеров в Web Console

В Web Console вы можете управлять работой компонента *Мониторинг контейнеров* в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры проверки контейнеров**).

Таблица 68. Параметры мониторинга контейнеров

Параметр	Описание
Проверка пространств имен и контейнеров включена / выключена	Переключатель включает или выключает проверку пространств имен и контейнеров в реальном времени. По умолчанию переключатель включен.
Действие с контейнером при обнаружении угрозы	Вы можете выбрать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта: • Пропустить контейнер (значение по умолчанию) – при обнаружении зараженного объекта приложение не выполняет никаких действий над контейнером. • Остановить контейнер – при обнаружении зараженного объекта приложение останавливает контейнер. • Остановить контейнер, если не удалось вылечить – если не удалось вылечить зараженный объект, приложение останавливает контейнер.
Использовать Docker	Флажок включает или выключает использование среды Docker. По умолчанию флажок установлен.
Путь Docker-сокета	Поле ввода пути или URI (универсальный идентификатор ресурса) Docker-сокета. Значение по умолчанию: /var/run/docker.sock.
Использовать CRI-O	Флажок включает или выключает использование среды CRI-O. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к конфигурационному файлу CRI-O. Значение по умолчанию: /etc/crio/crio.conf.
Использовать Podman	Флажок включает или выключает использование утилиты Podman. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты Podman. Значение по умолчанию: /usr/bin/podman.
Корневая директория	Поле ввода пути к корневой директории хранилища контейнеров. Значение по умолчанию: /var/lib/containers/storage.
Использовать runc	Флажок включает или выключает использование утилиты runc. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты runc. Значение по умолчанию: /usr/bin/runc.
Корневая директория	Поле ввода пути к корневой директории хранилища состояний контейнеров. Значение по умолчанию: /run/runc.

Настройка мониторинга контейнеров в Консоли администрирования

В Консоли администрирования вы можете управлять работой компонента Мониторинг контейнеров в политике (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры проверки контейнеров**).

Таблица 69. Параметры мониторинга контейнеров

Параметр	Описание
Включить проверку пространств имен и контейнеров	Флажок включает или выключает проверку пространств имен и контейнеров в реальном времени. По умолчанию флажок установлен.
Действие с контейнером при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта: • Пропустить контейнер (значение по умолчанию) – при обнаружении зараженного объекта приложение не выполняет никаких действий над контейнером. • Остановить контейнер – при обнаружении зараженного объекта приложение останавливает контейнер. • Остановить, если не удалось вылечить – если не удалось вылечить зараженный объект, приложение останавливает контейнер.
Параметры проверки контейнеров	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Параметры проверки контейнеров (см. раздел "Окно Параметры проверки контейнеров" на стр. 325).

Окно Параметры проверки контейнеров

В этом окне вы можете настроить параметры интеграции приложения Kaspersky Industrial CyberSecurity for Linux Nodes с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Таблица 70. Параметры проверки контейнеров

Параметр	Описание
Использовать Docker	Флажок включает или выключает использование среды Docker. По умолчанию флажок установлен.
Путь Docker-сокета	Поле ввода пути или URI (универсальный идентификатор ресурса) Docker-сокета. Значение по умолчанию: /var/run/docker.sock.
Использовать CRI-O	Флажок включает или выключает использование среды CRI-O. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к конфигурационному файлу CRI-O. Значение по умолчанию: /etc/crio/crio.conf.
Использовать Podman	Флажок включает или выключает использование утилиты Podman. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты Podman. Значение по умолчанию: /usr/bin/podman
Корневая директория	Поле ввода пути к корневой директории хранилища контейнеров.
Использовать runc	Флажок включает или выключает использование утилиты runc. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты runc. Значение по умолчанию: /usr/bin/runc
Корневая директория	Поле ввода пути к корневой директории хранилища состояний контейнеров. Значение по умолчанию: /run/runc.

Настройка мониторинга контейнеров в командной строке

В командной строке вы можете включать и выключать проверку пространств имен и контейнеров в реальном времени с помощью параметра `NamespaceMonitoring=Yes/No` из общих параметров приложения.

Вы можете изменять значение параметра (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) `NamespaceMonitoring` с помощью конфигурационного файла, который содержит все общие параметры приложения, или с помощью ключей командной строки.

При проверке пространств имен и контейнеров в реальном времени используются общие параметры проверки контейнеров (на стр. [728](#)). Вы можете просматривать и изменять эти параметры с помощью специальных команд управления Kaspersky Industrial CyberSecurity for Linux Nodes (см. раздел "Команды управления общими параметрами проверки контейнеров" на стр. [685](#)):

- Вы можете выводить текущие значения общих параметров проверки контейнеров в консоль или в конфигурационный файл. Этот файл вы можете использовать для изменения параметров.
- Вы можете изменять все общие параметры проверки контейнеров, используя конфигурационный файл, который содержит параметры. Конфигурационный файл вы можете получить с помощью команды вывода общих параметров проверки контейнеров.

- Вы можете изменять отдельные параметры, используя ключи командной строки в формате `<имя параметра>=<значение параметра>`. Текущие значения параметров вы можете получить с помощью команды вывода общих параметров проверки контейнеров.

- Чтобы вывести в консоль текущие значения общих параметров проверки контейнеров, выполните следующую команду:

```
kics-control --get-container-settings [--json]
```

где `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

- Чтобы вывести в файл текущие значения общих параметров проверки контейнеров, выполните следующую команду:

```
kics-control --get-container-settings --file <путь к конфигурационному файлу> [--json]
```

где:

- `--file <путь к конфигурационному файлу>` – путь к файлу, в который будут сохранены общие параметры проверки контейнеров. Если вы укажете имя файла, не указав путь к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, файл не будет создан.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

- Чтобы изменить значения общих параметров проверки контейнеров с помощью конфигурационного файла:

1. Выведите общие параметры проверки контейнеров в конфигурационный файл, как описано выше.
2. Измените значения нужных параметров в файле и сохраните изменения.
3. Выполните команду:

```
kics-control --set-container-settings --file <путь к конфигурационному файлу> [--json]
```

где:

- `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу с общими параметрами проверки контейнеров.
- `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения общих параметров проверки контейнеров, заданные в файле, будут импортированы в приложение.

- Чтобы изменить значения общих параметров проверки контейнеров с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-container-settings <имя параметра>=<значение параметра>
[<имя параметра>=<значение параметра>]
```

где <имя параметра>=<значение параметра> – имя и значение одного из общих параметров проверки контейнеров (см. раздел "Общие параметры проверки контейнеров" на стр. [728](#)).

Проверка контейнеров и образов по требованию

Во время выполнения задачи *Проверка контейнеров* приложение Kaspersky Industrial CyberSecurity for Linux Nodes проверяет контейнеры и образы на наличие вирусов и других вредоносных программ. Приложение может выполнять одновременно несколько задач проверки контейнеров.

Поддерживается интеграция с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Вы можете запускать проверку контейнеров и настраивать параметры проверки:

- Указывать контейнеры и образы, которые нужно проверять, по имени или маске имени.
- Включать проверку всех слоев образов и контейнеров.
- Выбирать действие, которое приложение будет выполнять над контейнером, и действие, которое приложение будет выполнять над образом при обнаружении зараженного объекта.
- Настраивать параметры проверки объектов внутри контейнеров или образов:
 - Включать и выключать проверку архивов, почтовых баз, сообщений электронной почты в текстовом формате.
 - Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
 - Выбирать действия, которые приложение будет выполнять над зараженными объектами.
 - Настраивать исключения объектов из проверки: по именам или маскам и по названиям обнаруженных в объектах угроз.
 - Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
 - Включать и выключать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.

В этом разделе

Проверка контейнеров в Web Console	328
Проверка контейнеров в Консоли администрирования	334
Проверка контейнеров в командной строке	342

Проверка контейнеров в Web Console

Таблица 71. Параметры задачи Проверка контейнеров

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры Пропускать файл, если его проверка длится более (сек.) и Пропускать файл, если его размер более (МБ) в блоке Общие параметры проверки. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку <i>самораспаковывающихся архивов</i>. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок Проверять архивы. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.

Параметр	Описание
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectProcessed</i>. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectNotProcessed</i>, если не удастся обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectNotProcessed</i>. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectNotProcessed</i>. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа <i>PackedObjectDetected</i> для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа <i>PackedObjectDetected</i>. Если флажок снят, приложение не записывает в журнал события типа <i>PackedObjectDetected</i>. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок Использовать эвристический анализ установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • Поверхностный – наименее детализированная проверка, минимальная нагрузка на систему. • Средний – средняя детализация при проверке, сбалансированная нагрузка на систему. • Глубокий – наиболее детализированная проверка, максимальная нагрузка на систему. • Рекомендованный (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).
Проверять контейнеры	Флажок включает или выключает проверку контейнеров. Если флажок установлен, вы можете указать имя или маску имени проверяемых контейнеров. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых контейнеров. По умолчанию указана маска * – выполняется проверка всех контейнеров.
Действие при обнаружении угрозы	Вы можете выбрать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта: • Пропустить контейнер – не выполнять никаких действий над контейнером при обнаружении зараженного объекта. • Остановить контейнер – остановить контейнер при обнаружении зараженного объекта. • Остановить контейнер, если не удалось вылечить (значение по умолчанию) – остановить контейнер, если не удалось вылечить зараженный объект или устранить угрозу. Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие Остановить контейнер.

Параметр	Описание
Проверять образы	Флажок включает или выключает проверку образов. Если флажок установлен, вы можете указать имя или маску имени проверяемых образов. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых образов. По умолчанию указана маска * – выполняется проверка всех образов.
Действие при обнаружении угрозы	Вы можете выбрать действие, которое приложение будет выполнять над образом при обнаружении зараженного объекта: • Пропустить образ (значение по умолчанию) – не выполнять никаких действий над образом при обнаружении зараженного объекта. • Удалить образ при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.
Проверять каждый слой	Флажок включает или выключает проверку всех слоев образов и запущенных контейнеров. По умолчанию флажок снят.

В этом разделе

Раздел Области исключения	333
Окно Исключения по маске	334
Окно Исключения по названию угрозы	334

Раздел Области исключения

В разделе **Области исключения** для задачи Проверка контейнеров вы можете настроить исключения по маске (см. раздел "Окно Исключения по маске" на стр. [186](#)) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. [186](#)), а также использование глобальных исключений во время работы задачи.

Таблица 72. Параметры исключений из проверки

Параметр	Описание
Настроить исключения по маске	По ссылке Настроить исключения по маске открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 186). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Настроить исключения по названию угрозы	По ссылке Настроить исключения по названию угрозы открывается окно Исключения по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 186). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях (см. раздел "Настройка глобальных исключений" на стр. 566), во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска `*.txt` – все текстовые файлы.

Маска `*_my_file_?.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, `2020_my_file_09.html`).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Проверка контейнеров в Консоли администрирования

В Консоли администрирования вы можете выполнять проверку контейнеров и образов с помощью задачи *Проверка контейнеров*. Вы можете создавать (см. раздел "Создание задач в Консоли

администрирования" на стр. [116](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Консоли администрирования" на стр. [117](#)) пользовательские задачи проверки контейнеров. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задач в Консоли администрирования" на стр. [117](#)) параметры задач.

В разделе **Параметры** в свойствах задачи Проверка контейнеров вы можете настроить параметры, приведенные в таблице ниже.

Таблица 73. Параметры задачи Проверка контейнеров

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить параметры проверки контейнеров (см. раздел "Окно Параметры проверки контейнеров" на стр. 335) и общие параметры проверки (см. раздел "Окно Параметры проверки" на стр. 245).
Действие при обнаружении угрозы	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Действие при обнаружении угрозы , в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В разделе **Исключения** в свойствах задачи Проверка контейнеров вы также можете настроить исключения по маске (см. раздел "Окно Исключения по маске" на стр. [206](#)) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. [206](#)).

Окно Параметры проверки контейнеров

В этом окне вы можете настроить параметры проверки контейнеров и образов.

Таблица 74. Параметры проверки контейнеров и образов

Параметр	Описание
Проверять контейнеры	Флажок включает или выключает проверку контейнеров. Если флажок установлен, вы можете указать имя или маску имени проверяемых контейнеров. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых контейнеров. По умолчанию указана маска * – выполняется проверка всех контейнеров.
Действие при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта: • Пропустить контейнер – не выполнять никаких действий над контейнером при обнаружении зараженного объекта. • Остановить контейнер – остановить контейнер при обнаружении зараженного объекта. • Остановить, если не удалось вылечить (значение по умолчанию) – остановить контейнер, если не удалось вылечить зараженный объект или устранить угрозу. Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие Остановить контейнер.
Проверять образы	Флажок включает или выключает проверку образов. Если флажок установлен, вы можете указать имя или маску имени проверяемых образов. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых образов. По умолчанию указана маска * – выполняется проверка всех образов.
Действие при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять над образом при обнаружении зараженного объекта: • Пропустить образ (значение по умолчанию) – не выполнять никаких действий над образом при обнаружении зараженного объекта. • Удалить образ при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.
Проверять каждый слой	Флажок включает или выключает проверку всех слоев образов и запущенных контейнеров. По умолчанию флажок снят.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Таблица 75. Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры Пропускать файл, если его проверка длится более (сек.) и Пропускать файл, если его размер более (МБ) в блоке Общие параметры проверки. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку <i>самораспаковывающихся архивов</i>. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок Проверять архивы. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.

Параметр	Описание
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectProcessed</i>. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectProcessed</i> для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа <i>ObjectNotProcessed</i>, если не удастся обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа <i>ObjectNotProcessed</i>. Если флажок снят, приложение не записывает в журнал события типа <i>ObjectNotProcessed</i>. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа <i>PackedObjectDetected</i> для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа <i>PackedObjectDetected</i>. Если флажок снят, приложение не записывает в журнал события типа <i>PackedObjectDetected</i>. По умолчанию флажок снят.
	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок Использовать эвристический анализ установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • Поверхностный – наименее детализированная проверка, минимальная нагрузка на систему. • Средний – средняя детализация при проверке, сбалансированная нагрузка на систему. • Глубокий – наиболее детализированная проверка, максимальная нагрузка на систему. • Рекомендованный (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действие при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Industrial CyberSecurity for Linux Nodes будет выполнять над обнаруженным зараженным объектом.

Таблица 76. Действия при обнаружении угрозы

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • Лечить объект. Копия зараженного объекта будет помещена в резервное хранилище. • Удалять объект. Копия зараженного объекта будет помещена в резервное хранилище. • Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • Пропускать объект (значение по умолчанию).

Раздел Исключения

Таблица 77. Параметры исключений из проверки

Блок параметров	Описание
Исключения по маске	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 206). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 206). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях (см. раздел "Настройка глобальных исключений" на стр. 566), во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Проверка контейнеров в командной строке

В командной строке вы можете выполнять проверку контейнеров и образов следующими способами:

- С помощью предустановленной задачи Проверка контейнеров (см. раздел "Параметры задачи Проверка контейнеров" на стр. [342](#)) (*Container_Scan*). Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) эту задачу вручную и настраивать расписание (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)) запуска задачи. Вы можете настраивать параметры (см. раздел "Параметры задачи Проверка контейнеров" на стр. [342](#)) проверки, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры этой задачи.
- С помощью пользовательских задач (см. раздел "Создание задачи в командной строке" на стр. [127](#)) проверки контейнеров (задач типа *ContainerScan*). Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) пользовательские задачи вручную и настраивать расписание (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)) запуска задач.
- С помощью команды `kics-control --scan-container` вы можете выполнять *выборочную проверку* (см. раздел "*Выборочная проверка контейнеров и образов*" на стр. [352](#)) указанных контейнеров и образов.

В этом разделе

Параметры задачи Проверка контейнеров	342
Выборочная проверка контейнеров и образов	352
Интеграция с Jenkins	352

Параметры задачи Проверка контейнеров

В таблице описаны все доступные значения и значения по умолчанию для всех параметров проверки контейнеров и образов.

Таблица 78. Параметры задачи Проверка контейнеров

Параметр	Описание	Значения
ScanContainers	Проверка контейнеров, заданных по маске. Вы можете указать маски с помощью параметра ContainerNameMask.	Yes (значение по умолчанию) – проверять контейнеры, заданные по маске. No – не проверять контейнеры, заданные по маске.
ContainerNameMask	Имя или маска имени проверяемого контейнера. Маски указываются в формате командной оболочки. Вы можете использовать символы ? и *. Прежде чем указать этот параметр, убедитесь, что значение параметра ScanContainers=Yes.	Значение по умолчанию: * (выполнять проверку всех контейнеров). Примеры: Проверять контейнер с именем my_container: ContainerNameMask=my_container Проверять все контейнеры, имена которых начинаются с my_container: ContainerNameMask=my_container* Проверять все контейнеры, имена которых начинаются с my_, затем содержат пять любых символов, затем слово _container и заканчиваются любой последовательностью символов: ContainerNameMask=my_?????_container*
ScanImages	Проверка образов, заданных по маске. Вы можете указать маски с помощью параметра ImageNameMask.	Yes (значение по умолчанию) – проверять образы, заданные по маске. No – не проверять образы, заданные по маске.
ImageNameMask	Имя или маска имени проверяемых образов. Прежде чем указать этот параметр, убедитесь, что для параметра ScanImages выбрано значение Yes. Маски указываются в формате командной оболочки. Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом.	Значение по умолчанию: * (выполнять проверку всех образов). Примеры: Проверять образы с именем my_image и значением tera latest: ImageNameMask=my_image:latest Проверять все образы, имена которых начинаются с my_image_, имеющие любое значения тега: ImageNameMask=my_image*
DeepScan	Проверка всех слоев образов и запущенных контейнеров.	Yes – проверять все слои. No (значение по умолчанию) – не проверять все слои.

Параметр	Описание	Значения
ContainerScanAction	Действие над контейнером при обнаружении зараженного объекта. Действия над зараженным объектом внутри контейнера описаны ниже.	StopContainerIfFailed (значение по умолчанию) – приложение останавливает контейнер, если не удалось вылечить или удалить зараженный объект. Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие StopContainer. StopContainer – приложение останавливает контейнер при обнаружении зараженного объекта. Skip – приложение не выполняет никаких действий над контейнерами при обнаружении зараженного объекта.
ImageAction	Действие над образом при обнаружении зараженного объекта. Действия над зараженным объектом внутри образа описаны ниже.	Skip (значение по умолчанию) – приложение не выполняет никаких действий над образами при обнаружении зараженного объекта. Delete – приложение удаляет образ при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.

Ниже описаны параметры, которые применяются к объектам внутри контейнеров и образов.

Таблица 79. Параметры задачи Проверка контейнеров

Параметр	Описание	Значения
ScanArchived	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	Yes (значение по умолчанию) – проверять архивы. Если указано значение FirstAction=Recommended, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. No – не проверять архивы.
ScanSfxArchived	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	Yes (значение по умолчанию) – проверять самораспаковывающиеся архивы. No – не проверять самораспаковывающиеся архивы.
ScanMailBases	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	Yes – проверять файлы почтовых баз. No (значение по умолчанию) – не проверять файлы почтовых баз.

Параметр	Описание	Значения
ScanPlainMail	Включение проверки сообщений электронной почты в текстовом формате (plain text).	Yes – проверять сообщения электронной почты в текстовом формате. No (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.

Параметр	Описание	Значения
FirstAction	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	Disinfect (лечить) – приложение пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано Disinfect, рекомендуется задать второе действие в параметре SecondAction. Remove (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Industrial CyberSecurity for Linux Nodes сразу удаляет троянские приложения, так как они не заражают другие файлы и поэтому не предполагают лечения. Skip (пропускать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Skip.
SecondAction	Выбор второго действия, которое приложение будет выполнять над зараженными объектами. Приложение выполняет второе действие, если не удалось выполнить первое действие.	Значения параметра SecondAction такие же, как значения параметра FirstAction. Если в качестве первого действия выбрано Skip (пропускать) или Remove (удалять), то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия. Если вы не указали второе действие, приложение в качестве второго действия выполняет Skip (пропускать). Значение по умолчанию: Skip.

Параметр	Описание	Значения
UseExcludeMasks	Использование исключения из проверки объектов, указанных параметром ExcludeMasks.item_#.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks.item_#. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.item_#.
ExcludeMasks.item_#	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.	Значение по умолчанию не задано. Пример: UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	Использование исключения из проверки объектов с угрозами, указанными параметром ExcludeThreats.item_#.	Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#. No (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#.

Параметр	Описание	Значения
ExcludeThreats.item_#	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр UseExcludeThreats. Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным. Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки. Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на сайте https://threats.kaspersky.com.	Значение параметра чувствительно к регистру. Значение по умолчанию не задано. Пример: <pre>UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux</pre>
UseGlobalExclusions	Включение использования глобальных исключений (см. раздел "Настройка глобальных исключений" на стр. 566) при проверке.	Yes (значение по умолчанию) – использовать глобальные исключения. No – не использовать глобальные исключения.
ReportCleanObjects	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	Yes – записывать в журнал информацию о незараженных объектах. No (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.

Параметр	Описание	Значения
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
ReportUnprocessedObjects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор; No – выключить эвристический анализатор.
HeuristicLevel	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная нагрузка системы. Medium – средний уровень эвристического анализа, сбалансированная нагрузка системы. Deep – наиболее тщательная проверка, максимальная нагрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.
UseIChecker	Включение использования технологии iChecker.	Yes (значение по умолчанию) – включить использование технологии iChecker. No – выключить использование технологии iChecker.

Выборочная проверка контейнеров и образов

Вы можете выполнять выборочную проверку указанных контейнеров и образов с помощью команды (см. раздел "Команды управления общими параметрами проверки контейнеров" на стр. [685](#)) `kics-control --scan-container`.

Выборочная проверка выполняется с параметрами, которые хранятся в предустановленной задаче *Custom_Container_Scan* (ID:19). Вы можете настраивать параметры выборочной проверки контейнеров и образов, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры этой задачи. По умолчанию для задачи *Custom_Container_Scan* заданы такие же параметры, как для задачи *Container_Scan* (см. раздел "Параметры задачи Проверка контейнеров" на стр. [342](#)) (ID:18).

► Чтобы запустить выборочную проверку контейнеров, выполните следующую команду:

```
kics-control --scan-container <контейнер/образ[:тег]>
```

где <контейнер/образ[:тег]> – имя или идентификатор контейнера или образа. Для проверки нескольких объектов вы можете использовать маски.

Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/**/*.file`.

Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file*` или `/dir/file**/`.

Маску ** можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

Если существует несколько элементов с одинаковым именем, приложение проверяет их все.

В результате выполнения команды создается временная задача проверки контейнеров и образов, которая автоматически удаляется после завершения. При этом в консоль выводятся результаты проверки.

Примеры:

Проверка контейнера с именем `my_container`:

```
kics-control --scan-container my_container
```

Проверка образа с именем `my_image` (все теги):

```
kics-control --scan-container my_image*
```

Интеграция с Jenkins

Kaspersky Industrial CyberSecurity for Linux Nodes поддерживает интеграцию с Jenkins. Плагины Jenkins Pipeline можно использовать для проверки Docker-образов на разных этапах. Например, можно проверять Docker-образы в репозитории в процессе разработки или перед публикацией.

► Чтобы интегрировать Kaspersky Industrial CyberSecurity for Linux Nodes с Jenkins:

1. Установите Kaspersky Industrial CyberSecurity for Linux Nodes на узле Jenkins.

2. Установите Docker Engine на узле Jenkins.

Дополнительная информация приведена в документации Docker Engine (<https://docs.docker.com/install/>).

3. Предоставьте пользователю Jenkins права администратора приложения Kaspersky Industrial CyberSecurity for Linux Nodes:

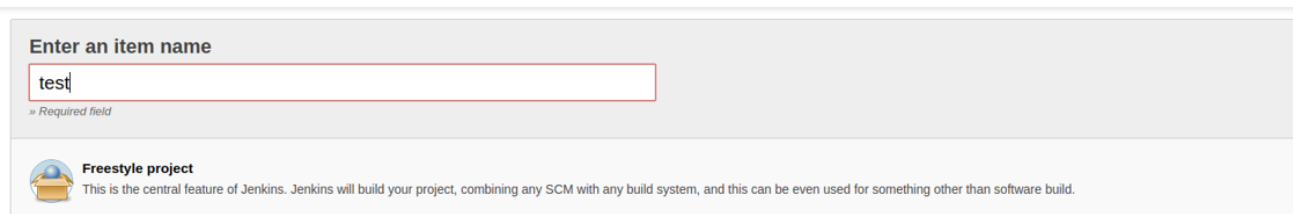
```
kics-control --grant-role admin <ИМЯ ПОЛЬЗОВАТЕЛЯ Jenkins>
```

4. Добавьте пользователя Jenkins в группу docker:

```
sudo usermod -aG docker <ИМЯ ПОЛЬЗОВАТЕЛЯ Jenkins>
```

Обычно используется имя jenkins.

5. В Jenkins создайте новое задание на сборку с названием test (New Item → Enter an item name).

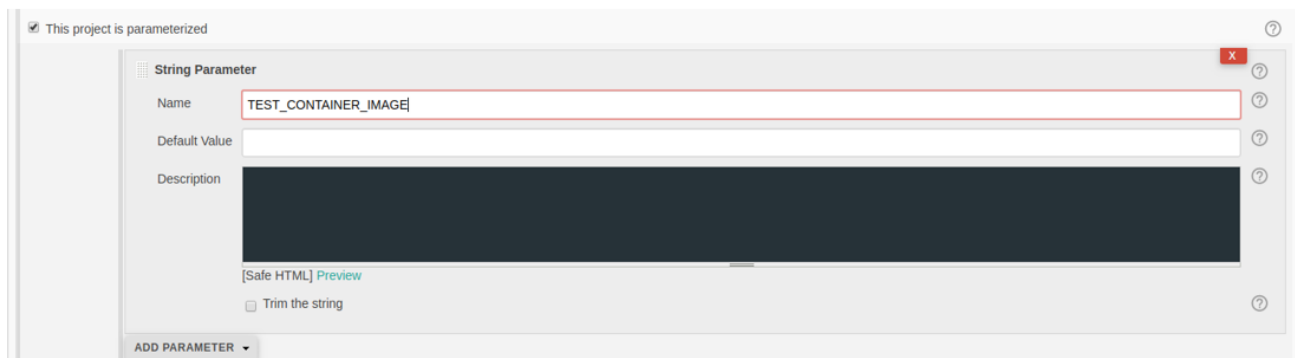


6. Настройте проект в соответствии с вашими требованиями. Предполагается, что в результате настройки вы получите образ или запущенный контейнер, который нужно проверить.

7. Чтобы запустить Docker-контейнер, добавьте следующий скрипт в процедуру сборки Jenkins. Если вы используете плагины Jenkins или другой способ запуска Docker-контейнеров, сохраните идентификатор запущенного Docker-контейнера в файл /tmp/kics_cs_info для дальнейшей проверки:

```
TMP_FILE="/tmp/kics_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage
${TEST_CONTAINER_IMAGE} /storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
    echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
    exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
```

```
exit ${EXIT_CODE}
```



- После создания артефактов добавьте следующий сценарий к шагам создания jenkins.

Этот скрипт поддерживает проверку одного контейнера. Если требуется, измените скрипт в соответствии с вашими требованиями.

```
TMP_FILE="/tmp/kics_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
    echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
    exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
    echo "Cannot find container ID in the temporary file:
    '${TMP_FILE}'"
    exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kics-control --scan-container ${CONTAINER_ID}|grep
'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
    echo "ATTENTION! ${THREATS_AMOUNT} threats detected at:
    '${CONTAINER_ID}'"
    EXIT_CODE=1
else
    echo "Not threats found"
fi
echo "Remove container: ${CONTAINER_ID}"
docker kill ${CONTAINER_ID}
```

```
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. Чтобы выполнить проверку Docker-образа из репозитория, выполните следующий скрипт:

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-
dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=${$.Dockerfile}
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
    echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
    echo "Dockerfile not fetched"
    exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kics/bin/kics-control --scan-container
${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. Сохраните задание на сборку.

Управление сетевым экраном

Задача Управление сетевым экраном предоставляет графическую оболочку для управления межсетевым экраном, входящим в состав операционной системы.

Во время работы в локальных сетях и интернете устройство подвержено не только заражению вирусами и другими вредоносными приложениями, но и различного рода атакам, использующим уязвимости операционных систем и программного обеспечения. Сетевой экран операционной системы защищает данные, которые хранятся на устройстве пользователя, блокируя большую часть угроз для операционной системы, когда устройство подключено к интернету или локальной сети.

Сетевой экран операционной системы позволяет обнаружить все сетевые соединения на устройстве пользователя и предоставить список их IP-адресов. Компонент Управление сетевым экраном позволяет задать статус этих сетевых соединений при помощи настройки сетевых пакетных правил (см. раздел "О сетевых пакетных правилах" на стр. [357](#)).

С помощью сетевых пакетных правил вы можете задать нужный уровень защиты устройства, от полной блокировки доступа в интернет для всех приложений до разрешения неограниченного доступа. Все исходящие соединения по умолчанию разрешены за исключением случаев, когда указаны соответствующие запрещающие правила компонента Управление сетевым экраном.

По умолчанию компонент Управление сетевым экраном выключен.

Перед включением компонента Управление сетевым экраном рекомендуется выключить другие средства управления сетевым экраном операционной системы.

При включении компонента Управление сетевым экраном приложение Kaspersky Industrial CyberSecurity for Linux Nodes автоматически удаляет все пользовательские правила, настроенные для сетевого экрана средствами операционной системы. После выключения компонента эти правила не восстанавливаются. Если требуется, сохраните пользовательские правила сетевого экрана до включения компонента Управление сетевым экраном.

Если управление сетевым экраном включено, Kaspersky Industrial CyberSecurity for Linux Nodes проверяет сетевой экран операционной системы и блокирует любую попытку изменить параметры сетевого экрана, например, когда какое-либо приложение или утилита пытается добавить или удалить какое-либо правило сетевого экрана. Kaspersky Industrial CyberSecurity for Linux Nodes проверяет сетевой экран операционной системы каждые 60 секунд и, если требуется, восстанавливает набор правил сетевого экрана, созданных с помощью приложения. Периодичность проверки изменить невозможно.

В операционных системах Red Hat Enterprise Linux и CentOS 8 правила сетевого экрана, созданные в приложении Kaspersky Industrial CyberSecurity for Linux Nodes, можно просмотреть только с помощью команд управления (см. раздел "Команды управления сетевым экраном" на стр. [691](#)) (команда `kics-control -F --query`).

Kaspersky Industrial CyberSecurity for Linux Nodes по-прежнему проверяет сетевой экран операционной системы, когда управление сетевым экраном выключено. Это позволяет приложению восстанавливать динамические правила (см. раздел "О динамических правилах" на стр. [358](#)).

Вы можете включать и выключать управление сетевым экраном, а также настраивать следующие параметры:

- Настраивать список сетевых пакетных правил, которые приложение Kaspersky Industrial CyberSecurity for Linux Nodes будет применять при обнаружении попытки установить сетевое соединение. Вы можете добавлять и удалять сетевые пакетные правила, а также изменять приоритет выполнения сетевого пакетного правила.
- Выбирать действия по умолчанию, применяемые к входящим соединениям и пакетам, если другие сетевые пакетные правила не применяются к этому виду соединений.
- Устанавливать соответствие сетевых адресов предустановленным сетевым зонам. Вы можете добавлять IP-адреса или подсети в сетевые зоны и удалять адреса из сетевых зон.
- Включать и выключать автоматическое добавление разрешающих правил для портов Агента администрирования.

Во избежание возможных проблем на системах с nftables приложение Kaspersky Industrial CyberSecurity for Linux Nodes использует системные утилиты iptables и iptables-restore при добавлении правил для сетевого экрана операционной системы. Приложение создает специальную разрешающую цепочку правил kics_bypass и добавляет ее первой в список таблицы mangle утилит iptables и ip6tables. Правила цепочки kics_bypass позволяют исключать трафик из проверки приложением Kaspersky Industrial CyberSecurity for Linux Nodes. Изменение правил в этой цепочке выполняется средствами операционной системы. При удалении приложения цепочка правил kics_bypass в iptables и ip6tables удаляется, только если она была пустая.

В этом разделе

О сетевых пакетных правилах	357
О динамических правилах	358
О предустановленных именах сетевых зон	358
Управление сетевым экраном в Web Console	359
Управление сетевым экраном в Консоли администрирования	364
Управление сетевым экраном в командной строке	370

О сетевых пакетных правилах

Сетевое пакетное правило представляет собой разрешающее или запрещающее действие, которое совершает Kaspersky Industrial CyberSecurity for Linux Nodes, обнаружив попытку сетевого соединения.

Правила используются для ввода ограничений на сетевые пакеты независимо от приложения. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных.

Все исходящие соединения разрешены по умолчанию (параметр действие по умолчанию) за исключением случаев, когда указаны соответствующие запрещающие правила Управления сетевым экраном. Действие по умолчанию выполняется с самым низким приоритетом: если не сработало никакое другое сетевое пакетное правило или другие сетевые пакетные правила не указаны, соединение разрешается.

Управление сетевым экраном задает по умолчанию некоторые сетевые пакетные правила. Вы можете создавать собственные сетевые пакетные правила и указывать приоритетность выполнения для каждого сетевого пакетного правила.

О динамических правилах

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes позволяет добавлять и удалять в сетевой экран *динамические правила*, необходимые для правильной работы приложения. Например, Агент администрирования добавляет динамические правила, которые разрешают соединение с Kaspersky Security Center, иницилируемые как приложением, так и Kaspersky Security Center. Правила Защиты от шифрования тоже являются динамическими.

Kaspersky Industrial CyberSecurity for Linux Nodes не контролирует динамические правила и не блокирует доступ к сетевым ресурсам для компонентов приложения. Динамические правила не зависят от состояния компонента Управление сетевым экраном (включен/выключен) или от изменения параметров работы компонента. Приоритет выполнения динамических правил выше приоритета сетевых пакетных правил (см. раздел "О сетевых пакетных правилах" на стр. [357](#)). Приложение восстанавливает набор динамических правил, если какие-либо из них были удалены, например, с помощью утилиты iptables.

Вы можете просмотреть набор динамических правил (с помощью команды (см. раздел "Команды управления сетевым экраном" на стр. [691](#)) `kics-control -F --query`), но не можете изменить параметры динамических правил.

О предустановленных именах сетевых зон

Заданная сетевая зона представляет собой конкретную группу IP-адресов или подсетей. С помощью заданной сетевой зоны вы можете использовать одно и то же правило для нескольких IP-адресов или подсетей, не создавая отдельное правило для каждого IP-адреса или подсети. Сетевую зону можно использовать в качестве значения параметра "удаленный адрес" при создании сетевого пакетного правила. В Kaspersky Industrial CyberSecurity for Linux Nodes есть три заданные сетевые зоны с конкретными именами:

- **Публичные.** Добавьте сетевой адрес или подсеть в эту зону, если они назначены сетям, не защищенным антивирусным приложением, брандмауэром или фильтрами (таким как сети интернет-кафе).
- **Локальные.** Добавьте сетевой адрес или подсеть в эту зону, если они назначены сетям, у пользователей которых есть право доступа к файлам и принтерам на этом устройстве (таким как локальные или домашние сети).
- **Доверенные.** Эта зона предназначена для безопасных сетей, в которых устройства не подвержены атакам или несанкционированным попыткам доступа к данным.

Вы не можете создать или удалить сетевую зону. Вы можете добавлять IP-адреса и подсети в сетевую зону или удалять их из нее.

Управление сетевым экраном в Web Console

В Web Console вы можете настраивать параметры управления сетевым экраном в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Базовая защита** → **Управление сетевым экраном**).

Таблица 80. Параметры компонента Управление сетевым экраном

Параметр	Описание
Управление сетевым экраном включено / выключено	Переключатель включает или выключает Управление сетевым экраном. По умолчанию переключатель выключен.
Сетевые пакетные правила	По ссылке Настроить сетевые пакетные правила открывается окно Сетевые пакетные правила (см. раздел "Окно Сетевые пакетные правила" на стр. 365). В этом окне вы можете настроить список сетевых пакетных правил, которые будет применять компонент Управление сетевым экраном при обнаружении попытки установления сетевого соединения.
Доступные сети	По ссылке Настроить доступные сети открывается окно Доступные сети (см. раздел "Окно Доступные сети" на стр. 363). В этом окне вы можете настроить список сетей, которые будет контролировать компонент Управление сетевым экраном.
Входящие соединения	В раскрывающемся списке вы можете выбрать действие для входящих сетевых соединений: • Разрешать сетевые соединения (значение по умолчанию). • Блокировать сетевые соединения.
Входящие пакеты	В раскрывающемся списке вы можете выбрать действие для входящих пакетов: • Разрешать входящие пакеты (значение по умолчанию). • Блокировать входящие пакеты.
Всегда добавлять разрешающие правила для портов Агента администрирования	Флажок включает или выключает автоматическое добавление разрешающих правил для портов Агента администрирования. По умолчанию флажок установлен.

Окно Сетевые пакетные правила

Таблица **Сетевые пакетные правила** содержит сетевые пакетные правила, используемые компонентом Управление сетевым экраном для контроля сетевой активности. Для сетевых пакетных правил вы можете настроить параметры, описанные в таблице ниже.

Таблица 81. Параметры сетевых пакетных правил

Параметр	Описание
Название	Название сетевого пакетного правила.
Действие	Действие, выполняемое компонентом Управление сетевым экраном при обнаружении сетевой активности.
Локальный адрес	Сетевые адреса устройств с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes, которые могут передавать и получать сетевые пакеты.
Удаленный адрес	Сетевые адреса удаленных устройств, которые могут передавать и/или получать сетевые пакеты.
Направление	Направление отслеживаемой сетевой активности.
Протокол	Тип протокола передачи данных, для которого отслеживается сетевая активность.
Локальные порты	Номера портов локальных устройств, между которыми контролируется соединение.
Удаленные порты	Номера портов удаленных устройств, между которыми контролируется соединение.
ICMP-тип	Тип ICMP. Компонент Управление сетевым экраном контролирует сообщения указанного типа, отправляемые узлом или шлюзом.
ICMP-код	Код ICMP. Компонент Управление сетевым экраном контролирует сообщения указанного в поле ICMP-тип типа и с указанным в поле ICMP-код кодом, отправляемые узлом или шлюзом.
Запись в отчет	В столбце указано, будет ли приложение записывать в отчет действия по сетевому пакетному правилу. Если в столбце указано Да , приложение записывает в журнал действия по сетевому пакетному правилу. Если в столбце указано Нет , приложение не записывает в журнале действия по сетевому пакетному правилу.

Окно Сетевое пакетное правило

В этом окне вы можете настроить сетевое пакетное правило.

Таблица 82. Параметры сетевого пакетного правила

Параметр	Описание
Название правила	Поле ввода названия сетевого пакетного правила.
Действие	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять компонент Управление сетевым экраном при обнаружении сетевой активности: • Блокировать сетевую активность. • Разрешать сетевую активность (значение по умолчанию).
Протокол	В раскрывающемся списке вы можете выбрать тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность: • Любой (значение по умолчанию) • GRE • ICMP • ICMPv6 • IGMP • TCP • UDP
Указать ICMP-тип	Флажок позволяет указать тип ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного типа, отправляемые узлом или шлюзом. Если флажок установлен, отображается поле для ввода типа ICMP. Флажок отображается, если в раскрывающемся списке Протокол выбран протокол передачи данных ICMP или ICMPv6 . По умолчанию флажок снят.
Указать ICMP-код	Флажок позволяет указать код ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного (в поле под флажком Указать ICMP-тип) типа и с указанным (в поле под флажком Указать ICMP-код) кодом, отправляемые узлом или шлюзом. Если флажок установлен, отображается поле для ввода кода ICMP. Флажок отображается, если в раскрывающемся списке Протокол выбран протокол передачи данных ICMP или ICMPv6 , и доступен, если установлен флажок Указать ICMP-тип . По умолчанию флажок снят.
Направление	В раскрывающемся списке вы можете указать направление отслеживаемой сетевой активности: • Входящие пакеты (значение по умолчанию). Если выбран этот элемент, компонент Управление сетевым экраном контролирует входящие пакеты. • Входящие. Если выбран этот элемент, компонент Управление сетевым экраном контролирует входящую сетевую активность. • Входящие / Исходящие. Если выбран этот элемент, компонент Управление сетевым экраном контролирует входящую и исходящую сетевую активность. • Входящие / Исходящие пакеты. Если выбран этот элемент, компонент Управление сетевым экраном контролирует входящие и исходящие пакеты. • Исходящие пакеты. Если выбран этот элемент, компонент Управление сетевым экраном контролирует исходящие пакеты. • Исходящие. Если выбран этот элемент, компонент Управление сетевым экраном контролирует исходящую сетевую активность.

Параметр	Описание
Удаленный адрес	В раскрывающемся списке вы можете указать сетевые адреса удаленных устройств, которые могут передавать и получать сетевые пакеты: • Любой адрес (значение по умолчанию). Если выбран этот элемент, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с любым IP-адресом. • Все адреса подсети. Если выбран этот элемент, сетевое правило контролирует сетевые пакеты, отправляемые и получаемые удаленными устройствами с IP-адресами, которые относятся к выбранному ниже типу сети: Публичные сети, Локальные сети или Доверенные сети. • Определенный адрес. Если выбран этот элемент, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с IP-адресами, указанными в поле ввода Адрес.
Указать удаленные порты	Флажок позволяет указать номера портов удаленных устройств, между которыми требуется контролировать соединение. Если флажок установлен, отображается поле для ввода номеров портов. Флажок отображается, если в раскрывающемся списке Протокол выбран протокол передачи данных TCP или UDP. По умолчанию флажок снят.
Локальный адрес	В раскрывающемся списке вы можете указать сетевые адреса устройств с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes, которые могут передавать и получать сетевые пакеты: • Любой адрес (значение по умолчанию). Если выбран этот элемент, сетевое правило контролирует отправку и получение сетевых пакетов устройствами с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes и любым IP-адресом. • Определенный адрес. Если выбран этот элемент, сетевое правило контролирует указанные в поле Адрес сетевые адреса устройств с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes, которые могут передавать и получать сетевые пакеты.
Указать локальные порты	Флажок позволяет указать номера портов локальных устройств, между которыми требуется контролировать соединение. Если флажок установлен, отображается поле для ввода номеров портов. Флажок отображается, если в раскрывающемся списке Протокол выбран протокол передачи данных TCP или UDP. По умолчанию флажок снят.
Записывать в отчет	Флажок позволяет указать, будут ли действия по сетевому правилу записываться в отчет. Если флажок установлен, приложение записывает в отчет действия по сетевому правилу. Если флажок снят, приложение не записывает в отчет действия по сетевому правилу. По умолчанию флажок снят.

Окно Доступные сети

Таблица **Доступные сети** содержит сети, контролируемые компонентом Управление сетевым экраном. По умолчанию таблица доступных сетей пустая.

Таблица 83. Параметры доступных сетей

Параметр	Описание
IP-адрес	IP-адрес сети.
Тип сети	Тип сети (Публичная сеть , Локальная сеть или Доверенная сеть).

Вы можете добавлять, изменять и удалять доступные сети.

Окно Сетевое соединение

В этом окне вы можете настроить сетевое соединение, которое будет контролировать компонент Управление сетевым экраном.

Таблица 84. Сетевое соединение

Параметр	Описание
IP-адрес	Поле ввода IP-адреса сети.
Тип сети	Вы можете выбрать тип сети: • Публичная сеть. • Локальная сеть. • Доверенная сеть.

Управление сетевым экраном в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры управления сетевым экраном в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Базовая защита** → **Управление сетевым экраном**).

Таблица 85. Параметры компонента Управление сетевым экраном

Параметр	Описание
Включить Управление сетевым экраном	Флажок включает или выключает компонент Управление сетевым экраном. По умолчанию флажок снят.
Сетевые пакетные правила	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Сетевые пакетные правила (см. раздел "Окно Сетевые пакетные правила" на стр. 365). В этом окне вы можете настроить сетевые пакетные правила, которые будет применять компонент Управление сетевым экраном при обнаружении попытки установления сетевого соединения.
Доступные сети	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Доступные сети (см. раздел "Окно Доступные сети" на стр. 369). В этом окне вы можете настроить список сетей, которые будет контролировать компонент Управление сетевым экраном.
Входящие соединения	В раскрывающемся списке вы можете выбрать действие для входящих сетевых соединений: • Разрешать сетевые соединения (значение по умолчанию). • Блокировать сетевые соединения.
Входящие пакеты	В раскрывающемся списке вы можете выбрать действие для входящих пакетов: • Разрешать входящие пакеты (значение по умолчанию). • Блокировать входящие пакеты.
Всегда добавлять разрешающие правила для портов Агента администрирования	Флажок включает или выключает автоматическое добавление разрешающих правил для портов Агента администрирования. По умолчанию флажок установлен.

Окно Сетевые пакетные правила

Таблица **Сетевые пакетные правила** содержит сетевые пакетные правила, используемые компонентом Управление сетевым экраном для контроля сетевой активности. Для сетевых пакетных правил вы можете настроить параметры, описанные в таблице ниже. По умолчанию таблица сетевых пакетных правил пуста.

Таблица 86. Параметры сетевых пакетных правил

Параметр	Описание
Название	Название сетевого пакетного правила.
Действие	Действие, выполняемое компонентом Управление сетевым экраном при обнаружении сетевой активности.
Локальный адрес	Сетевые адреса устройств с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes, которые могут передавать и получать сетевые пакеты.
Удаленный адрес	Сетевые адреса удаленных устройств, которые могут передавать и/или получать сетевые пакеты.
Запись в отчет	В столбце указано, будет ли приложение записывать в отчет действия по сетевому пакетному правилу. Если в столбце указано Да, приложение записывает в журнал действия по сетевому пакетному правилу. Если в столбце указано Нет, приложение не записывает в журнале действия по сетевому пакетному правилу.

Окно Добавление сетевого пакетного правила

В этом окне вы можете настроить параметры добавляемого сетевого пакетного правила.

Таблица 87. Параметры сетевого пакетного правила

Параметр	Описание
Протокол	Вы можете выбрать тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность: • Любой (значение по умолчанию) • GRE • ICMP • ICMPv6 • IGMP • TCP • UDP
Направление	Вы можете указать направление отслеживаемой сетевой активности: • Входящие пакеты. Если выбран этот вариант, компонент Управление сетевым экраном контролирует входящие пакеты. • Входящие. Если выбран этот вариант, компонент Управление сетевым экраном контролирует входящую сетевую активность. • Входящие / Исходящие. Если выбран этот вариант, компонент Управление сетевым экраном контролирует входящую и исходящую сетевую активность. • Входящие / Исходящие пакеты. Если выбран этот вариант, компонент Управление сетевым экраном контролирует входящие и исходящие пакеты. • Исходящие пакеты. Если выбран этот вариант, компонент Управление сетевым экраном контролирует исходящие пакеты. • Исходящие. Если выбран этот вариант, компонент Управление сетевым экраном контролирует исходящую сетевую активность.
ICMP-тип	Вы можете указать тип ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного типа, отправляемые узлом или шлюзом. Если выбран вариант Определенный, отображается поле для ввода типа ICMP. Окно отображается, если в раскрывающемся списке Протокол выбран протокол передачи данных ICMP или ICMPv6.
ICMP-код	Вы можете указать код ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного в поле ICMP-тип типа и с указанным в поле ICMP-код кодом, отправляемые узлом или шлюзом. Если выбран вариант Определенный, отображается поле для ввода кода ICMP. Окно отображается, если в раскрывающемся списке Протокол выбран протокол передачи данных ICMP или ICMPv6.
Удаленные порты	Вы можете указать номера портов удаленных устройств, между которыми требуется контролировать соединение. Если выбран вариант Определенный, отображается поле для ввода номеров портов. Окно отображается, если в раскрывающемся списке Протокол выбран протокол передачи данных TCP или UDP.
Локальные порты	Вы можете указать номера портов локальных устройств, между которыми требуется контролировать соединение. Если выбран вариант Определенный, отображается поле для ввода номеров портов. Окно отображается, если в раскрывающемся списке Протокол выбран протокол передачи данных TCP или UDP.

Параметр	Описание
Удаленные адреса	Вы можете указать сетевые адреса удаленных устройств, которые могут передавать и получать сетевые пакеты: • Любой адрес (значение по умолчанию). Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с любым IP-адресом. • Определенный адрес. Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с IP-адресами, указанными в поле ввода ниже. • По типу сети. Если выбран этот вариант, сетевое правило контролирует сетевые пакеты, отправляемые и получаемые удаленными устройствами с IP-адресами, которые относятся к выбранному ниже типу сетей: Публичные сети, Локальные сети или Доверенные сети.
Локальные адреса	Вы можете указать сетевые адреса устройств с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes, которые могут передавать и получать сетевые пакеты: • Любой адрес (значение по умолчанию). Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов устройствами с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes и любым IP-адресом. • Определенный адрес. Если выбран этот вариант, сетевое правило контролирует указанные в поле ниже сетевые адреса устройств с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes, которые могут передавать и получать сетевые пакеты.
Действие	Вы можете выбрать действие, которое будет выполнять компонент Управление сетевым экраном при обнаружении сетевой активности: • Блокировать сетевую активность. • Разрешать сетевую активность (значение по умолчанию).
Запись в отчет	Вы можете указать, будут ли действия по сетевому правилу записываться в отчет.
Название правила	Поле ввода названия сетевого пакетного правила.

Окно Доступные сети

Таблица **Доступные сети** содержит сети, контролируемые компонентом Управление сетевым экраном. По умолчанию таблица доступных сетей пустая.

Таблица 88. Параметры доступных сетей

Параметр	Описание
IP-адрес	IP-адрес сети.
Тип сети	Тип сети (Публичная сеть , Локальная сеть или Доверенная сеть).

Вы можете добавлять, изменять и удалять доступные сети.

Окно Сетевое соединение

В этом окне вы можете настроить сетевое соединение, которое будет контролировать компонент Управление сетевым экраном.

Таблица 89. Сетевое соединение

Параметр	Описание
IP-адрес	Поле ввода IP-адреса сети.
Тип сети	Вы можете выбрать тип сети: • Публичная сеть. • Локальная сеть. • Доверенная сеть.

Управление сетевым экраном в командной строке

В командной строке вы можете настраивать управление сетевым экраном с помощью предустановленной задачи Управление сетевым экраном (*Firewall_Management*).

По умолчанию задача Управление сетевым экраном не запущена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) эту задачу вручную.

Вы можете настраивать параметры управления сетевым экраном, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи с помощью команды управления параметрами задач.

Вы также можете настраивать параметры управления сетевым экраном с помощью команд управления сетевым экраном (см. раздел «Команды управления сетевым экраном» на стр. [691](#)):

- Создавать и удалять сетевые пакетные правила и изменять приоритет их выполнения (см. раздел "Настройка списка сетевых пакетных правил в командной строке" на стр. [376](#)).
- Формировать список IP-адресов или подсетей в сетевых зонах (см. раздел "Настройка сетевых зон в командной строке" на стр. [377](#)).
- Просматривать созданные в приложении Kaspersky Industrial CyberSecurity for Linux Nodes правила сетевого экрана с помощью команды `kics-control -F --query` (см. раздел "Команды управления сетевым экраном" на стр. [691](#)).

Таблица 90. Параметры задачи Управление сетевым экраном

Параметр	Описание	Значения
<code>DefaultIncomingAction</code>	Действие по умолчанию, применяемое ко входящему соединению, если другие сетевые правила не применяются к этому виду соединения.	<code>Allow</code> (значение по умолчанию) – разрешать входящие соединения. <code>Block</code> – запрещать входящие соединения.
<code>DefaultIncomingPacketAction</code>	Действие по умолчанию, применяемое ко входящему пакету, если другие сетевые пакетные правила не применяются к этому виду соединения.	<code>Allow</code> (значение по умолчанию) – разрешать входящие пакеты. <code>Block</code> – запрещать входящие пакеты.
<code>OpenNagentPorts</code>	Добавление динамических правил для Агента администрирования в пакетные правила.	<code>Yes</code> (значение по умолчанию) – добавлять динамические правила для Агента администрирования в пакетные правила. <code>No</code> – не добавлять динамические правила для Агента администрирования в пакетные правила.
Секция [PacketRules.item_#] содержит сетевые пакетные правила для задачи Управление сетевым экраном. Вы можете указать несколько секций <code>[PacketRules.item_#]</code> в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Каждая секция <code>[PacketRules.item_#]</code> содержит следующие параметры:		
<code>Name</code>	Имя сетевого пакетного правила.	Значение по умолчанию: <code>Packet rule #<n></code> , где <code>n</code> – это индекс.
<code>FirewallAction</code>	Действие, применяемое к соединениям, указанным в сетевом пакетном правиле.	<code>Allow</code> (значение по умолчанию) – разрешать сетевые соединения. <code>Block</code> – запрещать сетевые соединения.
<code>Protocol</code>	Тип протокола, для которого необходим мониторинг сетевой активности.	<code>Any</code> (значение по умолчанию) – задача Управление сетевым экраном контролирует всю сетевую активность. <code>TCP</code> <code>UDP</code> <code>ICMP</code> <code>ICMPv6</code> <code>IGMP</code> <code>GRE</code>
<code>RemotePorts</code>	Номера портов удаленных устройств, соединение между которыми отслеживается. Вы можете указать значение в виде целого числа или в виде интервала. Этот параметр можно указать, только если для параметра <code>Protocol</code> установлено значение <code>TCP</code> или <code>UDP</code> .	<code>Any</code> (значение по умолчанию) – контролировать все удаленные порты. <code>0 – 65535</code> .

Параметр	Описание	Значения
LocalPorts	Номера портов локальных устройств, соединение между которыми отслеживается. Вы можете указать значение в виде целого числа или в виде интервала. Этот параметр можно указать, только если для параметра Protocol установлено значение TCP или UDP.	Any (значение по умолчанию) – контролировать все локальные порты. 0 – 65535.
ICMPType	Тип пакета ICMP. Этот параметр можно указать, только если для параметра Protocol установлено значение ICMP или ICMPv6.	Any (значение по умолчанию) – контролировать все типы пакетов ICMP. Целое число согласно спецификации протокола передачи данных.
ICMPCode	Код пакета ICMP. Этот параметр можно указать, только если для параметра Protocol установлено значение ICMP или ICMPv6.	Any (значение по умолчанию) – контролировать все коды пакетов ICMP. Целое число согласно спецификации протокола передачи данных.
Direction	Направление отслеживаемой сетевой активности.	IncomingOutgoing или InOut (значение по умолчанию) – контролировать как входящие, так и исходящие соединения. Incoming или In – контролировать входящие соединения. Outgoing или Out – контролировать исходящие соединения. IncomingPacket или InPacket – контролировать входящие пакеты. OutgoingPacket или OutPacket – контролировать исходящие пакеты. IncomingOutgoingPacket или InOutPacket – контролировать как входящие, так и исходящие пакеты.

Параметр	Описание	Значения
RemoteAddress	Сетевые адреса удаленных устройств, которые могут передавать и получать сетевые пакеты.	Any (значение по умолчанию) – контролируется отправка и / или получение сетевых пакетов удаленными устройствами с любым IP-адресом. Trusted – заданная сетевая зона для доверенных сетей. Local – заданная сетевая зона для локальных сетей. Public – заданная сетевая зона для публичных сетей. d.d.d.d – адреса IPv4, где d – десятичное число от 0 до 255. d.d.d.d/p – подсеть адресов IPv4, где p – число от 0 до 32. x:x:x:x:x:x:x:x – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. x:x:x:x::0/p – подсеть адресов IPv6, где p – число от 0 до 64.
LocalAddress	Сетевые адреса устройств с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes, которые могут передавать и получать сетевые пакеты.	Any (значение по умолчанию) – контролируется отправка и / или получение сетевых пакетов локальными устройствами с любым IP-адресом. d.d.d.d – адреса IPv4, где d – десятичное число от 0 до 255. d.d.d.d/p – подсеть адресов IPv4, где p – число от 0 до 32. x:x:x:x:x:x:x:x – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. x:x:x:x::0/p – подсеть адресов IPv6, где p – число от 0 до 64.
LogAttempts	Включение записи в отчет действия сетевого правила.	Yes – записывать действия в отчет. No (значение по умолчанию) – не записывать действия в отчет.
Секция [NetworkZonesPublic] содержит сетевые адреса, связанные с публичными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		

Параметр	Описание	Значения
Address.item_#	Указывает IP-адрес или IP-подсеть.	d.d.d.d – адреса IPv4, где d – десятичное число от 0 до 255. d.d.d.d/p – подсеть адресов IPv4, где p – число от 0 до 32. x:x:x:x:x:x:x:x – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. x:x:x:x::0/p – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию: "" (в этой зоне нет сетевых адресов).
Секция [NetworkZonesLocal] содержит сетевые адреса, связанные с локальными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		
Address.item_#	Указывает IP-адрес или IP-подсеть.	d.d.d.d – адреса IPv4, где d – десятичное число от 0 до 255. d.d.d.d/p – подсеть адресов IPv4, где p – число от 0 до 32. x:x:x:x:x:x:x:x – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. x:x:x:x::0/p – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию: "" (в этой зоне нет сетевых адресов).
Секция [NetworkZonesTrusted] содержит сетевые адреса, связанные с доверенными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		
Address.item_#	Указывает IP-адрес или IP-подсеть.	d.d.d.d – адреса IPv4, где d – десятичное число от 0 до 255. d.d.d.d/p – подсеть адресов IPv4, где p – число от 0 до 32. x:x:x:x:x:x:x:x – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. x:x:x:x::0/p – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию: "" (в этой зоне нет сетевых адресов).

В этом разделе

- Настройка списка сетевых пакетных правил в командной строке[376](#)
- Настройка сетевых зон в командной строке[377](#)

Настройка списка сетевых пакетных правил в командной строке

► Чтобы добавить сетевое пакетное правило, выполните следующую команду:

```
kics-control --add-rule [--name <название правила>] [--action <действие>] [--protocol <протокол>] [--direction <направление>] [--remote <удаленный адрес>[:<диапазон портов>]] [--local <локальный адрес>[:<диапазон портов>]] [--at <индекс>]
```

где:

- `--name <название правила>` – название сетевого пакетного правила.
- `--action <действие>` – действие, применяемое к соединениям, указанным в сетевом пакетном правиле.
- `--protocol <протокол>` – тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность.
- `--direction <направление>` – направление отслеживаемой сетевой активности.
- `--remote <удаленный адрес>[:<диапазон портов>]` – сетевой адрес удаленного устройства. Вы можете указать имя предустановленной сетевой зоны в качестве удаленного адреса.
- `--local <локальный адрес>[:<диапазон портов>]` – сетевой адрес устройства с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes.
- `--at <индекс>` – индекс правила в списке сетевых пакетных правил. Если ключ `--at` не указан или его значение больше количества правил в списке, новое правило добавляется в конец списка.

Для параметров, значения которых вы не указали в команде, устанавливаются значения по умолчанию (см. раздел "Управление сетевым экраном в командной строке" на стр. [370](#)).

Примеры:

Чтобы создать правило, блокирующее все входящие и создаваемые соединения по протоколу TCP через порт 23, выполните следующую команду:

```
kics-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote any
```

Чтобы создать правило, блокирующее входящие и создаваемые соединения по протоколу TCP через порт 23 для сетевой зоны Публичные, выполните следующую команду:

```
kics-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote Public
```

► Чтобы удалить сетевое пакетное правило, выполните одну из следующих команд:

- `kics-control --del-rule --name <название правила>`
- `kics-control --del-rule --index <индекс>`

где:

- `--name <название правила>` – название сетевого пакетного правила.

- `--index <индекс>` – текущий индекс правила в списке сетевых пакетных правил.

Если список сетевых пакетных правил содержит несколько правил с одинаковым именем или не содержит правило с указанным именем или индексом, происходит ошибка.

► Чтобы изменить приоритет выполнения сетевого пакетного правила, выполните одну из следующих команд:

- `kics-control --move-rule --name <название правила> --at <индекс>`
- `kics-control --move-rule --index <индекс> --at <индекс>`

где:

- `--name <название правила>` – название сетевого пакетного правила.
- `--index <индекс>` – текущий индекс правила в списке сетевых пакетных правил.
- `--at <индекс>` – новый индекс правила в списке сетевых пакетных правил.

Настройка сетевых зон в командной строке

► Чтобы добавить сетевой адрес в зону, выполните следующую команду:

```
kics-control --add-zone --zone <зона> --address <адрес>
```

где:

- `--zone <зона>` – предустановленное имя сетевой зоны. Возможные значения: `Public`, `Local`, `Trusted`.
- `--address <адрес>` – сетевой адрес или подсеть.

► Чтобы удалить сетевой адрес из зоны, выполните одну из следующих команд:

- `kics-control --del-zone --zone <зона> --address <адрес>`
- `kics-control --del-zone --zone <зона> --index <индекс адреса в зоне>`

Если зона содержит несколько элементов с одинаковым сетевым адресом, команда `--del-zone` не будет выполнена.

Если указанный сетевой адрес или индекс не существует, отображается сообщение об ошибке.

Защита от веб-угроз

Компонент Защита от веб-угроз позволяет проверять входящий трафик, передаваемый по протоколам HTTP, HTTPS и FTP, веб-сайты и IP-адреса, предотвращать загрузку вредоносных файлов из интернета, а также блокировать доступ к фишинговым, рекламным и прочим опасным веб-сайтам.

Текущие соединения для перехватываемых TCP-портов сбрасываются при включении Защиты от сетевых угроз.

По умолчанию Защита от веб-угроз выключена. При этом она включается автоматически, если на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в политике не установлен) и в системе обнаружен один из следующих исполняемых файлов браузеров, в том числе и snap-формата:

- chrome;
- chromium;
- chromium-browser;
- firefox;
- firefox-esr;
- google-chrome;
- opera;
- yandex-browser.

Вы можете включать и выключать Защиту от веб-угроз, а также настраивать параметры защиты:

- Выбирать действие, которое приложение будет выполнять над веб-ресурсом, на котором обнаружен опасный объект.
- Настраивать список доверенных веб-адресов. Приложение не проверяет содержание веб-сайтов, веб-адреса которых указаны в этом списке.
- Выбирать объекты, которые приложение будет обнаруживать во время проверки входящего трафика.
- Настраивать проверку защищенных соединений (см. раздел "Проверка защищенных соединений" на стр. [388](#)) для проверки HTTPS-трафика.

Для проверки FTP-трафика в параметрах проверки защищенных соединений должен быть настроен контроль всех сетевых портов.

При открытии веб-сайта приложение выполняет следующие действия:

1. Проверяет надежность веб-сайта с помощью загруженных баз приложения.
2. Проверяет надежность веб-сайта с помощью эвристического анализа, если он включен. Во время эвристического анализа приложение Kaspersky Industrial CyberSecurity for Linux Nodes анализирует активность приложений в операционной системе. Эвристический анализ может обнаружить опасные объекты, о которых нет записей в базах приложения Kaspersky Industrial CyberSecurity for Linux Nodes.
3. Проверяет надежность веб-сайта с помощью репутационных баз "Лаборатории Касперского", если включено использование Kaspersky Security Network.

Рекомендуется включить использование Kaspersky Security Network, чтобы увеличить эффективность защиты от веб-угроз.

4. Запрещает или разрешает открыть веб-сайт.

При попытке открытия опасного веб-сайта приложение выполняет следующие действия:

- Для HTTP- или FTP-трафика приложение блокирует доступ и показывает предупреждение.
- Для HTTPS-трафика в браузере отображается страница с ошибкой.

Удаление сертификатов приложения может привести к некорректной работе компонента Защита от веб-угроз.

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes добавляет в список таблицы mangle утилит iptables и ip6tables специальную разрешающую цепочку правил kics_bypass, которая позволяет исключать трафик из проверки приложением. Если в цепочке настроены правила исключения трафика, они влияют на работу компонента Защита от веб-угроз.

В этом разделе

Настройка защиты от веб-угроз в Web Console	379
Настройка защиты от веб-угроз в Консоли администрирования	381
Настройка защиты от веб-угроз в командной строке	383

Настройка защиты от веб-угроз в Web Console

В Web Console вы можете настраивать параметры защиты от веб-угроз в политике (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (Параметры приложения → Базовая защита → Защита от веб-угроз).

Таблица 91. Параметры компонента Защита от веб-угроз

Параметр	Описание
Защита от веб-угроз включена / выключена	Переключатель включает или выключает компонент Защита от веб-угроз. По умолчанию переключатель выключен.
Действие при обнаружении угрозы	В этом разделе вы можете указать действие, которое приложение будет выполнять над веб-ресурсом, на котором обнаружен опасный объект: • Информировать пользователя при обнаружении опасного объекта в веб-трафике (значение по умолчанию). Защита от веб-угроз позволяет выполнить загрузку объекта на устройство. При этом приложение записывает в журнал и добавляет в список активных угроз информацию об опасном объекте. • Блокировать доступ ко всем опасным объектам, обнаруженным в веб-трафике, показывать уведомление о заблокированных попытках доступа и записывать в журнал информацию об опасных объектах.
Обнаруживать вредоносные объекты	Флажок включает или выключает проверку ссылок по базе вредоносных веб-адресов. По умолчанию флажок установлен.
Обнаруживать фишинговые ссылки	Флажок включает или выключает проверку ссылок по базе фишинговых веб-адресов. По умолчанию флажок установлен.
Использовать эвристический анализ для обнаружения фишинговых ссылок	Флажок включает или выключает использование эвристического анализа для обнаружения фишинговых ссылок. Флажок доступен и установлен по умолчанию, если установлен флажок Обнаруживать фишинговые ссылки .
Обнаруживать рекламные приложения	Флажок включает или выключает проверку ссылок по базе рекламных веб-адресов. По умолчанию флажок снят.
Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным	Флажок включает или выключает проверку ссылок по базе легальных приложений, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. По умолчанию флажок снят.
Доверенные веб-адреса	Таблица содержит веб-адреса и веб-страницы, содержимое которых вы считаете доверенным. В список доверенных веб-адресов вы можете добавлять только веб-адреса HTTP/HTTPS. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается. По умолчанию таблица пуста. Вы можете добавлять, изменять и удалять веб-адреса в таблице.

Окно Веб-адрес

В этом окне вы можете добавить веб-адрес или маску веб-адресов в список доверенных веб-адресов.

В список доверенных веб-адресов можно добавлять только веб-адреса HTTP / HTTPS. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается.

При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html).

Настройка защиты от веб-угроз в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от веб-угроз в политике (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Базовая защита** → **Защита от веб-угроз**).

Таблица 92. Параметры компонента Защита от веб-угроз

Параметр	Описание
Включить Защиту от веб-угроз	Флажок включает или выключает компонент Защита от веб-угроз. По умолчанию флажок снят.
Доверенные веб-адреса	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Доверенные веб-адреса (см. раздел "Окно Доверенные веб-адреса" на стр. 381), в котором вы можете указать список доверенных веб-адресов. Приложение не проверяет содержание веб-сайтов, веб-адреса которых указаны в этом списке.
Действие при обнаружении угрозы	Действие, которое приложение будет выполнять над веб-ресурсом, на котором обнаружен опасный объект: • Блокировать доступ ко всем опасным объектам, обнаруженным в веб-трафике, показывать уведомление о заблокированных попытках доступа и записывать в журнал информацию об опасных объектах. • Информировать пользователя при обнаружении опасного объекта в веб-трафике (значение по умолчанию). Защита от веб-угроз позволяет выполнить загрузку объекта на устройство. При этом приложение записывает в журнал и добавляет в список активных угроз информацию об опасном объекте.
Параметры проверки	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Параметры проверки (см. раздел "Окно Параметры проверки" на стр. 382), в котором вы можете настроить параметры проверки входящего трафика.

Окно Доверенные веб-адреса

В этом окне вы можете добавить веб-адреса и веб-страницы, содержимое которых вы считаете доверенным.

В список доверенных веб-адресов вы можете добавлять только веб-адреса HTTP / HTTPS. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается. По умолчанию список пустой.

При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html).

Вы можете добавлять, изменять и удалять веб-адреса в списке.

Окно Веб-адрес

В этом окне вы можете добавить веб-адрес или маску веб-адресов в список доверенных веб-адресов.

В список доверенных веб-адресов можно добавлять только веб-адреса HTTP / HTTPS. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается.

При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html).

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки входящего трафика во время работы компонента Защита от веб-угроз.

Таблица 93. Параметры Защиты от веб-угроз

Параметр	Описание
Обнаруживать вредоносные объекты	Флажок включает или выключает проверку ссылок по базе вредоносных веб-адресов. По умолчанию флажок установлен.
Обнаруживать фишинговые ссылки	Флажок включает или выключает проверку ссылок по базе фишинговых веб-адресов. По умолчанию флажок установлен.
Использовать эвристический анализ для обнаружения фишинговых ссылок	Флажок включает или выключает использование эвристического анализа для обнаружения фишинговых ссылок. Флажок доступен и установлен по умолчанию, если установлен флажок Обнаруживать фишинговые ссылки .
Обнаруживать рекламные приложения	Флажок включает или выключает проверку ссылок по базе рекламных веб-адресов. По умолчанию флажок снят.
Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным	Флажок включает или выключает проверку ссылок по базе легальных приложений, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. По умолчанию флажок снят.

Настройка защиты от веб-угроз в командной строке

В командной строке вы можете управлять защитой от веб-угроз с помощью предустановленной задачи Защита от веб-угроз (*Web_Threat_Protection*).

Задача запускается автоматически, если в системе обнаружен один из поддерживаемых браузеров (см. раздел "Защита от веб-угроз" на стр. [378](#)) и на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в политике не установлен).

Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачу вручную. Вы можете настраивать параметры защиты от веб-угроз, изменяя параметры предустановленной задачи Защита от веб-угроз (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)).

Таблица 94. Параметры задачи Защита от веб-угроз

Параметр	Описание	Значения
ActionOnDetect	Действия, выполняемые при обнаружении зараженного объекта в веб-трафике.	Notify (значение по умолчанию) – разрешить загрузку обнаруженного объекта, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте. Block – запретить доступ к обнаруженному объекту, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.
CheckMalicious	Включает или выключает проверку ссылок по базе вредоносных веб-адресов.	Yes (значение по умолчанию) – проверять ссылки на вхождение в базу вредоносных веб-адресов. No – не проверять ссылки на вхождение в базу вредоносных веб-адресов.
CheckPhishing	Включает или выключает проверку ссылок по базе фишинговых веб-адресов.	Yes (значение по умолчанию) – проверять ссылки на вхождение в базу фишинговых веб-адресов. No – не проверять ссылки на вхождение в базу фишинговых веб-адресов.
UseHeuristicForPhishing	Включает или выключает использование эвристического анализа для проверки веб-страниц на наличие фишинговых ссылок.	Yes (значение по умолчанию) – использовать эвристический анализ для обнаружения фишинговых ссылок. Если выбрано это значение, используется поверхностный уровень эвристического анализа – Light (наименее тщательная проверка, минимальная загрузка системы). Для задачи Защита от веб-угроз невозможно изменить уровень эвристического анализа. No – не использовать эвристический анализ для обнаружения фишинговых ссылок.
CheckAdware	Включает или выключает проверку ссылок по базе рекламных веб-адресов.	Yes – проверять ссылки на вхождение в базу рекламных веб-адресов. No (значение по умолчанию) – не проверять ссылки на вхождение в базу рекламных веб-адресов.

Параметр	Описание	Значения
CheckOther	Включает или выключает проверку ссылок по базе веб-адресов, содержащих легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.	Yes – проверять ссылки на вхождение в базу веб-адресов, содержащих легальные приложения, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. No (значение по умолчанию) – не проверять ссылки на вхождение в базу веб-адресов, содержащих легальные приложения, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным.
UseTrustedAddresses	Включает или выключает использование списка доверенных веб-адресов. Приложение не проверяет доверенные веб-адреса на вирусы и другие вредоносные объекты. Вы можете указать доверенные веб-адреса с помощью параметра <code>TrustedAddresses.item_#</code> .	Yes (значение по умолчанию) – использовать список доверенных веб-адресов. No – не использовать список доверенных веб-адресов.
<code>TrustedAddresses.item_#</code>	Доверенные веб-адреса.	Значение по умолчанию не задано. Для указания веб-адресов вы можете использовать маски. При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, <code>www.virus.com/download_virus/page_0-9abcdef.html</code>). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска <code>www.virus.com/**/page_0-9abcdef.html</code> означает <code>www.virus.com/*/page_0-9abcdef.html</code>). Использование масок для указания IP-адресов не поддерживается.

Проверка защищенных соединений

Параметры проверки защищенных соединений используются в работе компонентов Защита от веб-угроз (на стр. [378](#)) и Веб-Контроль (на стр. [489](#)). Компонент Защита от веб-угроз может расшифровывать и проверять сетевой трафик, передаваемый по защищенным соединениям. По умолчанию проверка защищенных соединений включена.

Вы можете включать и выключать проверку защищенных соединений, а также настраивать параметры проверки:

- Выбирать действие, выполняемое приложением при обнаружении недоверенного сертификата.
- Выбирать действие, выполняемое приложением при возникновении ошибки проверки защищенных соединений на веб-сайте.
- Включать и выключать использование интернета при проверке сертификатов.
- Просматривать и настраивать список доверенных доменов. Приложение не будет проверять защищенные соединения, установленные при посещении указанных доменов.
- Настраивать список сертификатов, которые приложение будет считать доверенными во время проверки защищенных соединений.
- Настраивать список сетевых портов, контролируемых приложением. Вы можете указывать определенные сетевые порты или диапазоны сетевых портов для проверки.

При изменении параметров проверки защищенных соединений приложение формирует событие *NetworkSettingsChanged*.

В этом разделе

Настройка проверки защищенных соединений в Web Console	388
Настройка проверки защищенных соединений в Консоли администрирования	391
Настройка проверки защищенных соединений в командной строке	394

Настройка проверки защищенных соединений в Web Console

В Web Console вы можете настраивать параметры проверки защищенных соединений в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры сети**).

Таблица 95. Параметры проверки защищенных соединений

Параметр	Описание
Проверка защищенных соединений включена / выключена	Переключатель включает или выключает проверку защищенных соединений. По умолчанию переключатель включен.
Доверенные корневые сертификаты	По ссылке Управлять доверенными корневыми сертификатами открывается окно Доверенные корневые сертификаты (см. раздел "Окно Доверенные корневые сертификаты" на стр. 390), в котором вы можете настроить список доверенных сертификатов. Доверенные сертификаты используются при проверке защищенных соединений.
Переход на домен с недоверенным сертификатом	Вы можете выбрать действие, которое приложение будет выполнять при переходе на домен с недоверенным сертификатом: • Разрешать (значение по умолчанию) – разрешать подключение к домену с недоверенным сертификатом. • Блокировать – блокировать подключение к домену с недоверенным сертификатом.
Переход на домен с ошибкой проверки защищенных соединений	Вы можете выбрать действие, которое приложение будет выполнять при переходе на домен с ошибкой проверки защищенных соединений: • Разрешать и добавлять домен в исключения (значение по умолчанию) – добавить домен, вызвавший ошибку, в список доменов с ошибками при проверке и не проверять зашифрованный сетевой трафик при посещении этого домена. • Блокировать – блокировать подключение к домену с ошибкой проверки.
Политика проверки сертификатов	Вы можете выбрать способ проверки сертификатов приложением: • Локальная проверка – приложение не использует интернет для проверки сертификата. • Полная проверка (значение по умолчанию) – приложение использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.
Доверенные домены	По ссылке Настроить доверенные домены открывается окно Доверенные домены (см. раздел "Окно Доверенные домены" на стр. 390), в котором вы можете настроить список имен доверенных доменов.
Контролировать все сетевые порты	Если выбран этот вариант, приложение проверяет все сетевые порты.
Контролировать только выбранные сетевые порты	Если выбран этот вариант, приложение проверяет только сетевые порты, указанные в окне Контролируемые порты (см. раздел "Окно Контролируемые порты" на стр. 390). Этот вариант выбран по умолчанию.
Контролируемые порты	По ссылке Настроить параметры сетевых портов открывается окно Контролируемые порты (см. раздел "Окно Контролируемые порты" на стр. 390), в котором вы можете указать, какие сетевые порты будет проверять приложение.

Окно Доверенные корневые сертификаты

Вы можете настроить список сертификатов, которые приложение Kaspersky Industrial CyberSecurity for Linux Nodes будет считать доверенными. Список доверенных сертификатов используется при проверке зашифрованных соединений.

Для каждого сертификата отображаются следующие сведения:

- субъект сертификата;
- серийный номер;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- отпечаток сертификата SHA256.

По умолчанию список сертификатов пуст.

Вы можете добавлять (см. раздел "Окно добавления доверенного сертификата" на стр. [390](#)) и удалять сертификаты.

Окно добавления доверенного сертификата

В этом окне вы можете добавить сертификат, который приложение Kaspersky Industrial CyberSecurity for Linux Nodes будет считать доверенным.

По ссылке **Добавить сертификат** открывается стандартное окно для выбора файла. Укажите путь к файлу формата DER или PEM, содержащему сертификат.

После выбора файла сертификата в окне отображается информация о сертификате и путь к файлу.

Окно Доверенные домены

Список содержит доменные имена и маски доменных имен, которые будут исключены из проверки зашифрованных соединений.

Пример: `*example.com`. Например, `*example.com/*` – это неправильное значение, так как требуется указывать адрес домена, а не веб-страницы.

По умолчанию список пуст.

Вы можете добавлять, изменять и удалять домены в списке доверенных доменов.

Окно Контролируемые порты

Таблица содержит сетевые порты, которые будет проверять приложение, если в окне **Параметры сети** (см. раздел "Настройка проверки защищенных соединений в Web Console" на стр. [388](#)) в блоке **Контролируемые порты** выбран вариант **Контролировать только выбранные сетевые порты**.

Таблица содержит два столбца:

- **Порт** – контролируемый порт.
- **Описание** – описание контролируемого порта.

По умолчанию в таблице отображается список сетевых портов, которые обычно используются для передачи почтового и сетевого трафика. Список сетевых портов входит в пакет приложения.

Настройка проверки защищенных соединений в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры проверки защищенных соединений в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры сети**).

Таблица 96. Параметры проверки защищенных соединений

Параметр	Описание
Включить проверку защищенных соединений	Флажок включает или выключает проверку защищенных соединений. По умолчанию флажок установлен.
Переход на домен с недоверенным сертификатом	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять при переходе на домен с недоверенным сертификатом: • Разрешать (значение по умолчанию) – разрешать подключение к домену с недоверенным сертификатом. • Блокировать – блокировать подключение к домену с недоверенным сертификатом.
Переход на домен с ошибкой проверки защищенных соединений	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять при переходе на домен с ошибкой проверки защищенных соединений: • Добавлять домен в исключения (значение по умолчанию) – добавить домен, вызвавший ошибку, в список доменов с ошибками при проверке и не проверять зашифрованный сетевой трафик при посещении этого домена. • Блокировать – блокировать подключение к домену с ошибкой проверки.
Политика проверки сертификатов	В раскрывающемся списке вы можете выбрать способ проверки сертификатов приложением: • Локальная проверка – приложение не использует интернет для проверки сертификата. • Полная проверка (значение по умолчанию) – приложение использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.
Доверенные домены	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Доверенные домены (см. раздел "Окно Доверенные домены" на стр. 392), в котором вы можете настроить список имен доверенных доменов.
Доверенные корневые сертификаты	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Доверенные корневые сертификаты (см. раздел "Окно Доверенные корневые сертификаты" на стр. 393), в котором вы можете настроить список доверенных сертификатов. Доверенные сертификаты используются при проверке защищенных соединений.
Параметры сетевых портов	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Контролируемые порты (см. раздел "Окно Контролируемые порты" на стр. 394).

Окно Доверенные домены

Список содержит доменные имена и маски доменных имен, которые будут исключены из проверки зашифрованных соединений.

Пример: `*example.com`. Например, `*example.com/*` – это неправильное значение, так как требуется указывать адрес домена, а не веб-страницы.

По умолчанию список пуст.

Окно Доверенные корневые сертификаты

Вы можете настроить список сертификатов, которые приложение Kaspersky Industrial CyberSecurity for Linux Nodes будет считать доверенными. Список доверенных сертификатов используется при проверке зашифрованных соединений.

Для каждого сертификата отображаются следующие сведения:

- **Субъект** – субъект сертификата;
- **Серийный номер** – серийный номер сертификата;
- **Издатель** – издатель сертификата;
- **Действует с** – дата начала срока действия сертификата;
- **Действует до** – дата окончания срока действия сертификата;
- **Отпечаток SHA256** – отпечаток сертификата SHA256.

По умолчанию список сертификатов пуст.

Окно Добавление сертификата

В этом окне вы можете добавить сертификат в список доверенных сертификатов одним из следующих способов:

- Указать путь к файлу сертификата. По кнопке **Обзор** открывается стандартное окно для выбора файла. Укажите путь к файлу формата DER или PEM, содержащему сертификат.
- Скопировать содержимое файла сертификата в поле **Ввести данные сертификата**.

Окно Контролируемые порты

Таблица 97. Параметры сетевых портов

Параметр	Описание
Контролировать все сетевые порты	Если выбран этот вариант, приложение проверяет все сетевые порты.
Контролировать только выбранные сетевые порты	Если выбран этот вариант, приложение проверяет только сетевые порты, указанные в таблице. Этот вариант выбран по умолчанию.
Параметры сетевых портов	Таблица содержит сетевые порты, которые будет проверять приложение, если выбран вариант Контролировать только указанные порты . Таблица содержит два столбца: • Порт – контролируемый порт. • Описание – описание контролируемого порта. По умолчанию в таблице отображается список сетевых портов, которые обычно используются для передачи почтового и сетевого трафика. Список сетевых портов входит в пакет приложения. Элементы в таблице можно добавлять, изменять и удалять.

Настройка проверки защищенных соединений в командной строке

В командной строке для управления параметрами проверки защищенных соединений предусмотрены специальные команды управления (см. раздел "Команды управления параметрами проверки защищенных соединений" на стр. [686](#)). С помощью команд управления параметрами проверки защищенных соединений вы можете:

- Настраивать параметры (см. раздел "Просмотр и изменение параметров проверки защищенных соединений" на стр. [395](#)) проверки защищенных соединений.
- Просматривать исключения (см. раздел "Просмотр исключений из проверки защищенных соединений" на стр. [396](#)) из проверки защищенных соединений.
- Очищать список доменов (см. раздел "Команды управления параметрами проверки защищенных соединений" на стр. [686](#)), которые приложение автоматически исключило из проверки.
- Управлять списком сертификатов (см. раздел "Управление списком доверенных сертификатов" на стр. [397](#)), которые приложение считает доверенными.

В этом разделе

Просмотр и изменение параметров проверки защищенных соединений	395
Просмотр исключений из проверки защищенных соединений	396
Управление списком доверенных сертификатов	397

Просмотр и изменение параметров проверки защищенных соединений

Вы можете просматривать и изменять параметры проверки защищенных соединений с помощью специальных команд управления (см. раздел «Команды управления параметрами проверки защищенных соединений» на стр. [686](#)):

- Вы можете выводить текущие значения параметров проверки защищенных соединений в консоль или в конфигурационный файл. Этот файл вы можете использовать для изменения параметров.
- Вы можете изменять все параметры проверки защищенных соединений, используя конфигурационный файл, который содержит параметры. Конфигурационный файл вы можете получить с помощью команды вывода параметров проверки защищенных соединений.
- Вы можете изменять отдельные параметры, используя ключи командной строки в формате `<имя параметра>=<значение параметра>`. Текущие значения параметров вы можете получить с помощью команды вывода параметров проверки защищенных соединений.

- *Чтобы вывести в консоль текущие значения параметров проверки защищенных соединений, выполните следующую команду:*

```
kics-control --get-net-settings [--json]
```

где `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

- *Чтобы вывести в файл текущие значения параметров проверки защищенных соединений, выполните следующую команду:*

```
kics-control --get-net-settings --file <путь к конфигурационному файлу> [--json]
```

где:

- `--file <путь к конфигурационному файлу>` – путь к файлу, в который будут сохранены параметры проверки защищенных соединений. Если вы укажете имя файла, не указав путь к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, файл не будет создан.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

- *Чтобы изменить значения параметров проверки защищенных соединений с помощью конфигурационного файла:*

1. Выведите общие параметры приложения в конфигурационный файл, как описано выше.
2. Измените значения нужных параметров в файле и сохраните изменения.
3. Выполните команду:

```
kics-control --set-net-settings --file <путь к конфигурационному файлу> [--json]
```

где:

- `--file` <путь к конфигурационному файлу> – полный путь к конфигурационному файлу с параметрами проверки защищенных соединений.
- `--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Значения параметров проверки защищенных соединений будут импортированы из файла в приложение.

- Чтобы изменить значения параметров проверки защищенных соединений с помощью командной строки, выполните следующую команду:

```
kics-control --set-net-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где <имя параметра>=<значение параметра> – имя и значение одного из параметров проверки защищенных соединений (см. раздел "Параметры проверки защищенных соединений" на стр. [731](#)).

Значения указанных параметров проверки защищенных соединений будут изменены.

Просмотр исключений из проверки защищенных соединений

Вы можете просматривать следующие списки исключений из проверки защищенных соединений:

- список исключений, добавленных пользователем;
- список исключений, добавленных приложением;
- список исключений, полученных из баз приложения.

- Чтобы просмотреть список исключений из проверки защищенных соединений, добавленных пользователем, выполните следующую команду:

```
kics-control -N --query user
```

- Чтобы просмотреть список исключений из проверки защищенных соединений, добавленных приложением, выполните следующую команду:

```
kics-control -N --query auto
```

- Чтобы просмотреть список исключений из проверки защищенных соединений, полученных из баз приложения, выполните следующую команду:

```
kics-control -N --query kl
```

- Чтобы очистить список доменов, которые приложение автоматически исключило из проверки, выполните следующую команду:

```
kics-control -N --clear-web-auto-excluded
```

Управление списком доверенных сертификатов

- Чтобы добавить сертификат в список доверенных сертификатов, выполните следующую команду:

```
kics-control --add-certificate <путь к сертификату>
```

где:

<путь к сертификату> – путь к файлу сертификата, который вы хотите добавить, в формате PEM или DER.

- Чтобы удалить сертификат из списка доверенных сертификатов, выполните следующую команду:

```
kics-control --remove-certificate <субъект сертификата>
```

- Чтобы просмотреть список доверенных сертификатов, выполните следующую команду:

```
kics-control --list-certificates
```

Для каждого сертификата отображается следующая информация:

- субъект сертификата;
- серийный номер;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- отпечаток сертификата SHA256.

Защита от сетевых угроз

Компонент Защита от сетевых угроз позволяет проверять входящий сетевой трафик на действия, характерные для сетевых атак.

По умолчанию Защита от сетевых угроз выключена.

Если Защита от сетевых угроз включена, приложение проверяет входящий трафик для TCP-портов, номера которых приложение Kaspersky Industrial CyberSecurity for Linux Nodes получает из актуальных баз приложения.

Для проверки сетевого трафика задача Защита от сетевых угроз принимает подключения по всем портам, номера которых получает из баз приложения. При проверке сети это может выглядеть как открытый порт на устройстве, даже если никакое приложение в системе его не прослушивает. Неиспользуемые порты рекомендуется закрывать средствами сетевого экрана.

Текущие соединения для перехватываемых TCP-портов сбрасываются при включении Защиты от сетевых угроз.

При обнаружении попытки сетевой атаки на защищаемое устройство приложение блокирует сетевую активность со стороны атакующего устройства и создает событие *Обнаружена сетевая атака*. Событие содержит информацию об атакующем устройстве.

По умолчанию сетевой трафик со стороны атакующего устройства блокируется на один час. По истечении времени блокировки приложение разблокирует устройство.

Вы можете включать и выключать Защиту от сетевых угроз, а также настраивать параметры защиты:

- Выбирать действие, которое приложение будет выполнять при обнаружении сетевой активности, характерной для сетевых атак.
- Включать и выключать блокировку сетевой активности при обнаружении попытки сетевой атаки.
- Задавать продолжительность блокировки атакующего устройства.
- Настраивать список IP-адресов, сетевая активность которых не блокируется приложением.

С помощью команд управления заблокированными устройствами (см. раздел "Управление заблокированными устройствами" на стр. [429](#)) в командной строке вы можете посмотреть список заблокированных устройств и вручную разблокировать эти устройства. В Kaspersky Security Center нет инструментов мониторинга и управления заблокированными устройствами, кроме событий *Обнаружена сетевая атака*.

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes добавляет в список таблицы mangle утилит iptables и ip6tables специальную разрешающую цепочку правил kics_bypass, которая позволяет исключать трафик из проверки приложением. Если в цепочке настроены правила исключения трафика, они влияют на работу задачи Защита от сетевых угроз. Например, для исключения исходящего http-трафика вам нужно добавить следующую команду: `iptables -t mangle -I kics_bypass -m tcp -p tcp --dport http -j ACCEPT`.

В этом разделе

Настройка защиты от сетевых угроз в Web Console	399
Настройка защиты от сетевых угроз в Консоли администрирования	400
Настройка защиты от сетевых угроз в командной строке	401

Настройка защиты от сетевых угроз в Web Console

В Web Console вы можете настраивать параметры защиты от сетевых угроз в политике (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Базовая защита** → **Защита от сетевых угроз**).

Таблица 98. Параметры компонента Защита от сетевых угроз

Параметр	Описание
Защита от сетевых угроз включена / выключена	Переключатель включает или выключает компонент Защита от сетевых угроз. По умолчанию переключатель выключен.
Действие при обнаружении угрозы	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак: • Информировать пользователя (значение по умолчанию). Приложение разрешает сетевую активность и записывает в журнал информацию об обнаруженной сетевой активности. • Блокировать сетевую активность со стороны атакующего устройства и записывать в журнал информацию об обнаруженной сетевой активности.
Блокировка атакующих устройств включена / выключена	Переключатель включает или выключает блокировку сетевой активности при обнаружении попытки сетевой атаки. По умолчанию переключатель включен.
Блокировать атакующее устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки атакующего устройства в минутах. По истечении указанного времени приложение Kaspersky Industrial CyberSecurity for Linux Nodes разрешает сетевую активность со стороны этого устройства. Доступные значения: целые числа от 1 до 32768. Значение по умолчанию: 60.
Исключения	Таблица содержит список IP-адресов, сетевые атаки с которых не будут заблокированы. По умолчанию список пуст. Вы можете добавлять, настраивать и удалять IP-адреса в таблице.

Окно IP-адрес

Вы можете добавлять и изменять IP-адреса, сетевые атаки с которых не будут заблокированы приложением Kaspersky Industrial CyberSecurity for Linux Nodes.

Таблица 99. IP-адреса

Параметр	Описание
Введите IP-адрес	Поле для ввода IP-адреса. Вы можете указывать IP-адреса в форматах IPv4 и IPv6.

Настройка защиты от сетевых угроз в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от сетевых угроз в политике (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Базовая защита** → **Защита от сетевых угроз**).

Таблица 100. Параметры компонента Защита от сетевых угроз

Параметр	Описание
Включить Защиту от сетевых угроз	Флажок включает или выключает компонент Защита от сетевых угроз. По умолчанию флажок снят.
Действие при обнаружении угрозы	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак: • Информировать пользователя (значение по умолчанию). Приложение разрешает сетевую активность и записывает в журнал информацию об обнаруженной сетевой активности. • Блокировать сетевую активность со стороны атакующего устройства и записывать в журнал информацию об обнаруженной сетевой активности.
Блокировать атакующие устройства	Флажок включает или выключает блокировку сетевой активности при обнаружении попытки сетевой атаки. По умолчанию флажок установлен.
Блокировать атакующее устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки атакующего устройства в минутах. По истечении указанного времени приложение Kaspersky Industrial CyberSecurity for Linux Nodes разрешает сетевую активность со стороны этого устройства. Доступные значения: целые числа от 1 до 32768. Значение по умолчанию: 60.
Исключения	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения (см. раздел "Окно Исключения" на стр. 400), в котором вы можете указать список IP-адресов, сетевые атаки с которых не будут заблокированы.

Окно Исключения

В этом окне вы можете добавить IP-адреса, сетевые атаки с которых не будут заблокированы.

По умолчанию список пустой.

Окно IP-адрес

Вы можете добавлять и изменять IP-адреса, сетевые атаки с которых не будут заблокированы приложением Kaspersky Industrial CyberSecurity for Linux Nodes.

Таблица 101. IP-адреса

Параметр	Описание
Введите IP-адрес	Поле для ввода IP-адреса. Вы можете указывать IP-адреса в форматах IPv4 и IPv6.

Настройка защиты от сетевых угроз в командной строке

В командной строке вы можете управлять защитой от сетевых угроз с помощью предустановленной задачи Защита от сетевых угроз (*Network_Threat_Protection*).

По умолчанию задача Защита от сетевых угроз не запущена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачу вручную.

Вы можете настраивать параметры защиты от сетевых угроз, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи Защита от сетевых угроз.

Таблица 102. Параметры задачи Защита от сетевых угроз

Параметр	Описание	Значения
ActionOnDetect	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак. При изменении значения этого параметра с Block на Notify список заблокированных устройств очищается.	Notify (значение по умолчанию) – разрешить сетевую активность, записать в журнал информацию об обнаруженной сетевой активности. Если указано это значение, значение параметра BlockAttackingHosts не учитывается. Block – заблокировать сетевую активность и записать в журнал информацию об этом.
BlockAttackingHosts	Блокировка сетевой активности со стороны атакующих устройств.	Yes (значение по умолчанию) – заблокировать сетевую активность атакующего устройства. No – не блокировать сетевую активность атакующего устройства. Если указано это значение, а для параметра ActionOnDetect указано значение Block, приложение блокирует сетевую активность со стороны атакующего устройства, но не вносит это устройство в список заблокированных устройств.

Параметр	Описание	Значения
BlockDurationMinutes	Продолжительность блокировки атакующих устройств (в минутах).	1 – 32768 Значение по умолчанию: 60.
UseExcludeIPs	Использование списка IP-адресов, сетевую активность которых не требуется блокировать при обнаружении сетевой атаки. Приложение записывает в журнал информацию о вредоносной активности со стороны этих устройств. Вы можете добавить IP-адреса в список исключений с помощью параметра <code>ExcludeIPs.item_#</code> .	Yes – использовать список исключений IP-адресов. No (значение по умолчанию) – не использовать список исключений IP-адресов.
ExcludeIPs.item_#	IP-адреса, сетевая активность которых не блокируется приложением. По умолчанию список пуст.	<code>d.d.d.d</code> – адреса IPv4, где d – десятичное число от 0 до 255. <code>d.d.d.d/p</code> – подсеть адресов IPv4, где p – число от 0 до 32. <code>x:x:x:x:x:x:x:x</code> – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. <code>x:x:x:x::0/p</code> – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию не задано.

Защита от удаленного вредоносного шифрования

Компонент Защита от шифрования позволяет защитить ваши файлы в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования.

По умолчанию Защита от удаленного вредоносного шифрования выключена.

Если защита от шифрования включена, приложение Kaspersky Industrial CyberSecurity for Linux Nodes проверяет действия удаленных устройств с файловыми ресурсами, расположенным в общих сетевых директориях защищаемого устройства, на наличие вредоносного шифрования. Если приложение расценивает действия удаленного устройства, получающего доступ к общим сетевым ресурсам, как вредоносное шифрование, приложение создает и включает правило для сетевого экрана операционной системы, которое блокирует сетевой трафик от скомпрометированного устройства. Скомпрометированное устройство добавляется в список недоверенных устройств, доступ к общим сетевым директориям для всех недоверенных устройств блокируется. Приложение создает событие *Обнаружено шифрование*, которое содержит информацию о скомпрометированном устройстве.

По умолчанию приложение блокирует доступ недоверенных устройств к сетевым файловым ресурсам на 30 минут. По истечении времени блокировки приложение удаляет скомпрометированное устройство из списка недоверенных устройств, доступ устройства к сетевым файловым ресурсам автоматически восстанавливается.

Правила сетевого экрана, созданные компонентом Защита от шифрования, нельзя удалить с помощью утилиты iptables, так как приложение восстанавливает набор правил каждую минуту.

Вы можете включать и выключать защиту от вредоносного шифрования, а также настраивать параметры защиты:

- Включать и выключать блокировку недоверенных устройств.
Если блокировка недоверенных устройств выключена, приложение все равно проверяет действия удаленных устройств с сетевыми файловыми ресурсами на наличие вредоносного шифрования, когда защита от шифрования включена. В случае обнаружения вредоносного шифрования создается событие *Обнаружено шифрование*, но скомпрометированное устройство не блокируется.
- Задавать продолжительность блокировки недоверенного устройства.
- Указывать файлы и директории, которые приложение защищает от вредоносного шифрования.
- Указывать файлы и директории, которые исключены из защиты от вредоносного шифрования.

Приложение не расценивает действия как шифрование, если активность шифрования обнаружена в директориях, исключенных из защиты от шифрования.

С помощью команд управления заблокированными устройствами (см. раздел "Управление заблокированными устройствами" на стр. [429](#)) в командной строке вы можете посмотреть список заблокированных устройств и вручную разблокировать эти устройства. В Kaspersky Security Center нет инструментов мониторинга и управления заблокированными устройствами, кроме событий *Обнаружено шифрование*.

Для корректной работы компонента Защита от шифрования требуется, чтобы в операционной системе была установлена хотя бы одна из служб: Samba или NFS. Для службы NFS требуется установленный пакет `grcbind`.

Компонент Защита от шифрования корректно работает с протоколами SMB1, SMB2, SMB3, NFS3, TCP/UDP и IP/IPv6. Работа с протоколами NFS2 и NFS4 не поддерживается. Рекомендуется настроить параметры сервера таким образом, чтобы протоколы NFS2 и NFS4 было невозможно использовать для подключения ресурсов.

Kaspersky Industrial CyberSecurity for Linux Nodes не блокирует доступ к сетевым файловым ресурсам, пока действия устройства не расцениваются как вредоносные. Таким образом, минимум один файл будет зашифрован, прежде чем приложение обнаружит вредоносную активность.

В этом разделе

Настройка защиты от шифрования в Web Console	405
Настройка защиты от шифрования в Консоли администрирования.....	414
Настройка защиты от шифрования в командной строке	423

Настройка защиты от шифрования в Web Console

В Web Console вы можете настраивать параметры защиты от шифрования в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (Параметры приложения → Продвинутая защита → Защита от шифрования).

Таблица 103. Параметры компонента Защита от шифрования

Параметр	Описание
Защита от шифрования включена / выключена	Переключатель включает или выключает защиту файлов в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования. По умолчанию переключатель выключен.
Области защиты	По ссылке Настроить область защиты открывается окно Области защиты (см. раздел "Окно Области защиты" на стр. 406).
Действие при обнаружении шифрования	Действие, которое Kaspersky Industrial CyberSecurity for Linux Nodes будет выполнять при обнаружении вредоносного шифрования: • Информировать пользователя (значение по умолчанию). Kaspersky Industrial CyberSecurity for Linux Nodes не блокирует устройство, осуществляющее шифрование, только записывает событие об обнаружении вредоносного шифрования в журнал событий. • Блокировать устройство, осуществляющее шифрование.
Блокировать недоверенное устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки недоверенного устройства в минутах. Изменение параметра не влияет на длительность блокировки ранее заблокированных скомпрометированных устройств. Длительность блокировки не является динамическим значением и рассчитывается в момент блокировки. Доступные значения: целые числа от 1 до 4294967295. Значение по умолчанию: 30.
Исключения	По ссылке Настроить области исключения открывается окно Области исключения .
Исключения по маске	По ссылке Настроить исключения по маске открывается окно Исключения по маске .

Окно Области защиты

Таблица содержит области защиты компонента Защита от шифрования. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Таблица 104. Параметры области защиты

Параметр	Описание
Название области	Название области защиты.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Industrial CyberSecurity for Linux Nodes защищает объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно добавления области защиты

В этом окне можно добавить или настроить область защиты компонента Защита от шифрования.

Таблица 105. Параметры области защиты

Параметр	Описание
Название области	Поле ввода названия области защиты. Это название будет отображаться в таблице окна Области защиты (см. раздел "Окно Области защиты" на стр. 406). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область защиты во время работы компонента. Если флажок снят, приложение не обрабатывает эту область защиты во время работы компонента. В дальнейшем вы можете включить эту область в параметры работы компонента, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • Локальная (значение по умолчанию) – локальные директории. • Общая – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • Все общие – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран элемент Общая .
Путь	Поле ввода пути к директории, которую вы хотите включить в область защиты. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Локальная . Поле не должно быть пустым. По умолчанию указан путь / (корневая директория).

Параметр	Описание
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы компонента Защита от шифрования. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 106. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

Таблица 107. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 182). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки или защиты во время своей работы. Если флажок снят, приложение включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • Локальная – локальные директории. • Смонтированная – удаленные директории, смонтированные на устройстве. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип Смонтированная.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Локальная.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке Протокол доступа выбран элемент Пользовательский.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле Путь. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Настройка защиты от шифрования в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от шифрования в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Продвинутая защита** → **Защита от шифрования**).

Таблица 108. Параметры компонента Защита от шифрования

Параметр	Описание
Включить Защиту от шифрования	Флажок включает или выключает защиту файлов в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования. По умолчанию флажок снят.
Области защиты	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки (см. раздел "Окно Области проверки" на стр. 191) и параметры защиты.
Исключения	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области исключения . В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 206). В этом окне вы можете настроить исключение объектов из проверки по маске имени.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Таблица 109. Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Industrial CyberSecurity for Linux Nodes проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне можно добавить или настроить область защиты компонента Защита от шифрования.

Таблица 110. Параметры области защиты

Параметр	Описание
Название области	Поле ввода названия области защиты. Это название будет отображаться в таблице окна Области проверки (см. раздел "Окно Области проверки" на стр. 191). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область защиты во время работы компонента. Если флажок снят, приложение не обрабатывает эту область защиты во время работы компонента. В дальнейшем вы можете включить эту область в параметры работы компонента, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • Локальная – локальные директории. • Общая – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • Все общие (значение по умолчанию) – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип Общая, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba.

Параметр	Описание
	Если в раскрывающемся списке файловых систем выбран тип Локальная, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область защиты. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, <code>/dir/*/file</code> или <code>/dir/**/file</code>. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, <code>/dir/**/file*/</code> или <code>/dir/file**/</code>. Маску ** можно использовать в имени директории только один раз. Например, <code>/dir/**/**/file</code> – это неправильная маска. Для исключения точки монтирования <code>/dir</code> требуется указывать именно <code>/dir</code> (без звездочек). Маска <code>/dir/*</code> исключает все точки монтирования на уровень ниже от <code>/dir</code>, но не саму точку монтирования <code>/dir</code>. Маска <code>/dir/**</code> исключает все точки монтирования на любом уровне вложенности под <code>/dir</code>, но не саму точку монтирования <code>/dir</code>. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы компонента Защита от шифрования. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Параметры защиты

Таблица 111. Параметры защиты

Параметр	Описание
Действие при обнаружении шифрования	Действие, которое Kaspersky Industrial CyberSecurity for Linux Nodes будет выполнять при обнаружении вредоносного шифрования: • Информировать пользователя (значение по умолчанию). Приложение не блокирует устройство, осуществляющее шифрование, только записывает событие об обнаружении вредоносного шифрования в журнал событий. • Блокировать устройство, осуществляющее шифрование.
Блокировать недоверенное устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки недоверенного устройства в минутах. По истечении указанного времени приложение удаляет недоверенные устройства из списка заблокированных. Доступ устройства к сетевым файловым ресурсам восстанавливается автоматически после его удаления из списка недоверенных устройств. Изменение параметра не влияет на длительность блокировки ранее заблокированных скомпрометированных устройств. Длительность блокировки не является динамическим значением и рассчитывается в момент блокировки. Доступные значения: целые числа от 1 до 2147483647. Значение по умолчанию: 30.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 112. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Таблица 113. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 182). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • Локальная – локальные директории. • Смонтированная – смонтированные директории. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип Смонтированная, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже.

Параметр	Описание
	Если в раскрывающемся списке файловых систем выбран тип Локальная, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • [container-id:<идентификатор>]/<путь к локальной директории> • [container-name:<название>]/<путь к локальной директории> • [image-id:<идентификатор>]/<путь к локальной директории> • [image-name:<название>]/<путь к локальной директории> Также вы можете использовать уникальные комбинации из тегов [container-id:<идентификатор>], [container-name:<название>], [image-id:<идентификатор>] и [image-name:<название>]/<путь к локальной директории>. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. В названиях и идентификаторах можно использовать маски (символы ? и *). Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке справа выбран элемент Пользовательская.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Настройка защиты от шифрования в командной строке

В командной строке вы можете управлять защитой от шифрования с помощью задачи Защита от шифрования (*Anti_Cryptor*).

По умолчанию задача Защита от шифрования не запущена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) эту задачу вручную.

Вы можете настраивать параметры защиты от шифрования, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи Защита от шифрования.

Таблица 114. Параметры задачи Защита от шифрования

Параметр	Описание	Значения
ActionOnDetect	Включение блокировки недоверенных устройств.	Block – включить блокировку недоверенных устройств. Notify (значение по умолчанию) – выключить блокировку недоверенных устройств.
BlockTime	Длительность блокировки недоверенного устройства в минутах. Изменение параметра BlockTime не влияет на длительность блокировки ранее заблокированных скомпрометированных устройств. Длительность блокировки не является динамическим значением и рассчитывается на момент блокировки.	Целое значение от 1 до 4294967295. Значение по умолчанию: 30.
UseExcludeMasks	Включение исключения из области защиты объектов, указанных параметром ExcludeMasks.item_#. Этот параметр работает, только если указано значение параметра ExcludeMasks.item_#.	Yes – исключать объекты, указанные параметром ExcludeMasks.item_#, из области защиты. No (значение по умолчанию) – не исключать объекты, указанные параметром ExcludeMasks.item_#, из области защиты.
ExcludeMasks.item_#	Исключение из области защиты объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области защиты отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр UseExcludeMasks. Если вы хотите указать несколько масок, указывайте каждую маску в новой строке с новым индексом.	Значение по умолчанию не задано.
Секция [ScanScope.item_#] содержит области, защищаемые приложением. Для задачи Защита от шифрования требуется указать хотя бы одну область защиты, можно указывать только общие директории. Вы можете указать несколько секций [ScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области защиты, содержит дополнительную информацию об области защиты.	Значение по умолчанию: All shared directories.

Параметр	Описание	Значения
UseScanArea	Включение защиты указанной области. Для выполнения задачи требуется включить защиту хотя бы одной области.	Yes (значение по умолчанию) – защищать указанную область. No – не защищать указанную область.
AreaMask.item_# _#	Ограничение области защиты. В области защиты приложение защищает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (защищать все объекты).
Path	Путь к директории с защищаемыми объектам.	<путь к локальной директории> – защищать локальную директорию, доступную через SMB/NFS. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/*file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/*/*file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. AllShared (значение по умолчанию) – защищать все ресурсы, доступные через SMB/NFS. Shared:SMB – защищать ресурсы, доступные через SMB. Shared:NFS – защищать ресурсы, доступные через NFS.

Параметр	Описание	Значения
Секция [ExcludedFromScanScope.item_#] содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#]. Объекты, удовлетворяющие правилам любой из секций [ExcludedFromScanScope.item_#], не проверяются. Формат секции [ExcludedFromScanScope.item_#] аналогичен формату секции [ScanScope.item_#]. Вы можете указать несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области исключения из защиты, содержит дополнительную информацию об области исключения.	Значение по умолчанию: <code>All objects</code> .
UseScanArea	Исключение указанной области из защиты.	<code>Yes</code> (значение по умолчанию) – исключать указанную область из защиты. <code>No</code> – не исключать указанную область из защиты.
AreaMask.item_#	Ограничение области исключения из защиты. В области исключения приложение исключает только объекты, указанные с помощью масок в формате <code>shell</code>. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: <code>*</code> (исключать все объекты).

Параметр	Описание	Значения
Path	Путь к директории с объектами, исключаемыми из защиты.	<путь к локальной директории> – исключать из защиты объекты в указанной директории. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Mounted:NFS – исключать из защиты удаленные директории, смонтированные на клиентском устройстве по протоколу NFS. Mounted:SMB – исключать из защиты удаленные директории, смонтированные на клиентском устройстве по протоколу Samba. AllRemoteMounted – исключать из защиты все удаленные директории, смонтированные на клиентском устройстве с помощью протоколов Samba и NFS.

Управление заблокированными устройствами

В ходе защиты устройства от сетевых угроз и от удаленного вредоносного шифрования приложение Kaspersky Industrial CyberSecurity for Linux Nodes может блокировать удаленные устройства, действия которых расцениваются как вредоносные:

- При обнаружении вредоносного шифрования приложение блокирует доступ удаленного устройства к общим сетевым директориям защищаемого устройства.
- При обнаружении попытки сетевой атаки на защищаемое устройство приложение блокирует сетевой трафик со стороны атакующего устройства.

Вы можете изменять продолжительность блокировки в параметрах защиты от сетевых угроз (см. раздел "Защита от сетевых угроз" на стр. [398](#)) и защиты от удаленного вредоносного шифрования (см. раздел "Защита от удаленного вредоносного шифрования" на стр. [404](#)). По истечении заданного периода времени приложение разблокирует устройство.

Если вы управляете приложением с помощью командной строки, вы можете использовать команды управления заблокированными устройствами, чтобы посмотреть список устройств, заблокированных в результате работы приложения на устройстве, и вручную разблокировать эти устройства до истечения времени блокировки. В Kaspersky Security Center нет инструментов мониторинга и управления заблокированными устройствами, кроме событий *Обнаружена сетевая атака* и *Обнаружено шифрование*.

-H –префикс, указывающий, что команда принадлежит к группе команд управления устройствами, заблокированными Защитой от шифрования (см. раздел "Защита от удаленного вредоносного шифрования" на стр. [404](#)) и Защитой от сетевых угроз (см. раздел "Защита от сетевых угроз" на стр. [398](#)).

Команда kics-control --get-blocked-hosts

Команда позволяет вывести в консоль список заблокированных устройств.

Синтаксис команды

```
kics-control [-H] --get-blocked-hosts
```

Команда kics-control --allow-hosts

Команда позволяет разблокировать заблокированные устройства.

Синтаксис команды

```
kics-control [-H] --allow-hosts <адрес>
```

Аргументы и ключи

<адрес> – IP-адрес устройства или подсети (IPv4/IPv6, включая адреса в короткой форме). Вы можете указать несколько IP-адресов устройств или подсетей, разделяя их пробелами.

► Чтобы просмотреть список заблокированных устройств, выполните следующую команду:

```
kics-control --get-blocked-hosts
```

В результате выполнения команды приложение выводит список заблокированных устройств в консоль.

- Чтобы разблокировать устройства, выполните следующую команду:

```
kics-control --allow-hosts <адрес>
```

где <адрес> – один или несколько IP-адресов устройств или подсетей (IPv4/IPv6, включая адреса в короткой форме). Вы можете указать несколько IP-адресов устройств или подсетей, разделяя их пробелами.

В результате выполнения команды приложение разблокирует указанные устройства.

Примеры:

Адреса IPv4:

```
dec - 192.168.0.1
```

```
dec - 192.168.0.0/24
```

Адреса IPv6:

```
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
```

```
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
```

```
hex - 2001:db8::ae21:ad12
```

```
hex - ::ffff:255.255.255.254
```

```
hex - ::
```

Контроль приложений

Компонент Контроль приложений позволяет управлять запуском приложений на защищаемых устройствах. Контроль приложений снижает риск заражения устройства, ограничивая доступ пользователей к приложениям.

Запуск приложений регулируется с помощью *правил контроля приложений* (см. раздел "О правилах контроля приложений" на стр. [432](#)).

Компонент Контроль приложений может применять правила одним из двух способов:

- *Список запрещенных*. Приложение Kaspersky Industrial CyberSecurity for Linux Nodes разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. По умолчанию компонент Контроль приложений использует этот способ.
- *Список разрешенных*. Приложение Kaspersky Industrial CyberSecurity for Linux Nodes запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.

Если правила контроля приложений сформированы максимально полно, Kaspersky Industrial CyberSecurity for Linux Nodes запрещает запуск всех новых, не проверенных администратором локальной сети организации приложений, но обеспечивает работоспособность операционной системы и проверенных приложений, которые нужны пользователям для выполнения должностных обязанностей.

Администратор Kaspersky Security Center или локальный пользователь с назначенной в приложении ролью *admin* (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. [77](#)) может запрещать или разрешать запуск процессов под учетной записью *root*, используя Контроль приложений.

По умолчанию Контроль приложений выключен. Вы можете включать и выключать Контроль приложений, а также настраивать параметры работы компонента:

- Выбирать способ применения правил компонента Контроль приложений: *список разрешенных* или *список запрещенных*.
- Создавать правила контроля приложений.
- Выбирать режим работы компонента Контроль приложений при обнаружении попытки запуска приложения, удовлетворяющего правилам: *блокировать* запуск приложения или *информировать* о попытке запуска приложения, удовлетворяющего правилам.
- Через Kaspersky Security Center экспортировать (см. раздел "Экспорт и импорт параметров и категорий через Kaspersky Security Center" на стр. [439](#)) с управляемого устройства параметры Контроля приложений, настроенные правила и созданные категории приложений и импортировать на управляемое устройство параметры Контроля приложений, настроенные правила и созданные категории приложений.

Вы можете получать информацию о приложениях, установленных на защищаемых устройствах с помощью задачи Инвентаризация (на стр. [450](#)).

Контроль приложений не поддерживает управление запуском приложений Snap, Flatpak и AppImage.

Контроль приложений не контролирует запуск скриптов из интерпретаторов, не поддерживаемых приложением Kaspersky Industrial CyberSecurity for Linux Nodes и запуск скриптов, передаваемых интерпретатору не через командную строку.

Kaspersky Industrial CyberSecurity for Linux Nodes поддерживает следующие интерпретаторы: python, perl, bash, ssh.

Если запуск интерпретатора разрешен правилами Контроля приложений, то Kaspersky Industrial CyberSecurity for Linux Nodes не блокирует скрипт, запущенный из этого интерпретатора. Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами Контроля приложений, то Kaspersky Industrial CyberSecurity for Linux Nodes блокирует все скрипты, указанные в командной строке интерпретатора. Исключение: cat script.py | python.

В этом разделе

О правилах контроля приложений	432
Настройка контроля приложений в Web Console	433
Настройка контроля приложений в Консоли администрирования	436
Экспорт и импорт параметров и категорий через Kaspersky Security Center	439
Настройка контроля приложений в командной строке	440

О правилах контроля приложений

Правило контроля приложений представляет собой набор параметров, которые содержат условия срабатывания правила и действия компонента Контроль приложений при срабатывании правила (разрешение или запрещение пользователям запускать приложение):

- Принадлежность приложения к категории приложений. *Категория приложений* – это группа приложений, обладающих общими признаками. Например, категория, в которую входят исполняемые файлы установленных приложений, или категория приложений, необходимых для работы, в которую входит стандартный набор приложений, используемых в организации. Вы можете использовать одну и ту же категорию только в одном правиле.

Использование KL-категорий приложения Kaspersky Security Center не поддерживается приложением Kaspersky Industrial CyberSecurity for Linux Nodes.

- Разрешение или запрещение выбранным пользователям и/или группам пользователей запускать приложения. Вы можете указать пользователя и/или группу пользователей, которым разрешен или запрещен запуск приложений из указанной категории.
- Условие срабатывания правила. Условие представляет собой соответствие "тип условия – критерий условия – значение условия". На основании условий срабатывания правила приложение Kaspersky Industrial CyberSecurity for Linux Nodes применяет или не применяет правило к приложению. В правилах используются включающие и исключающие условия:
 - *Включающие условия.* Kaspersky Industrial CyberSecurity for Linux Nodes применяет правило к приложению, если приложение соответствует хотя бы одному включающему условию.

- *Исключающие условия.* Kaspersky Industrial CyberSecurity for Linux Nodes не применяет правило к приложению, если приложение соответствует хотя бы одному исключаяющему условию или не соответствует ни одному включающему условию.

Условия срабатывания правила формируются с помощью следующих критериев:

- имя исполняемого файла приложения;
- имя директории с исполняемым файлом приложения;
- хеш исполняемого файла приложения. Допускается использование только SHA256.

Для каждого критерия, используемого в условии, вам нужно указать его значение.

Для указания имен файлов и директорий вы можете использовать маски.

Если параметры запускаемого приложения соответствуют критериям, указанным во включающем условии, правило срабатывает. В этом случае Kaspersky Industrial CyberSecurity for Linux Nodes выполняет действие, указанное в правиле. Если параметры приложения соответствуют критериям, указанным в исключаяющем условии, Kaspersky Industrial CyberSecurity for Linux Nodes не контролирует запуск приложения.

Правила контроля приложений могут иметь один из следующих *статусов работы*:

- *Включено* – правило включено, Kaspersky Industrial CyberSecurity for Linux Nodes применяет это правило для контроля приложений.
- *Выключено* – правило выключено и не используется для контроля приложений.
- *Тест* – Kaspersky Industrial CyberSecurity for Linux Nodes разрешает запуск приложений, которые удовлетворяют условиям правила, но записывает информацию о запуске этих приложений в отчет.

Статус работы правила имеет более высокий приоритет чем действие, указанное в правиле.

Настройка контроля приложений в Web Console

В Web Console вы можете настраивать параметры контроля приложений в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)). (**Параметры приложения → Контроль безопасности → Контроль приложений**)

Таблица 115. Параметры компонента Контроль приложений

Параметр	Описание
Контроль приложений включен / выключен	Переключатель включает или выключает Контроль приложений. По умолчанию переключатель выключен.
Режим работы Контроля приложений	Режим работы Контроля приложений при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам: • Блокировать. При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes блокирует запуск приложения, удовлетворяющего правилам. • Информировать (значение по умолчанию). При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes формирует событие о попытке запуска приложения, удовлетворяющего правилам.
Способ применения правил Контроля приложений	Способ применения правил компонента Контроль приложений: • Список разрешенных. При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. • Список запрещенных (значение по умолчанию). При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.
Правила Контроля приложений	По ссылке Настроить правила открывается окно Правила Контроля приложений (см. раздел "Окно Правила Контроля приложений" на стр. 434).
Применение правил	В раскрывающемся списке вы можете выбрать способ добавления правил: • Заменить правилами из политики локальные правила. При выборе этого элемента списка приложение применяет только правила, заданные в политике. • Добавить правила из политики к локальным правилам (значение по умолчанию). При выборе этого элемента списка приложение применяет правила, заданные в политике, совместно с локальными правилами, настроенными на защищаемом устройстве.

Окно Правила Контроля приложений

Таблица **Правила Контроля приложений** содержит закладки с правилами для каждого режима работы Контроля приложений: **Список запрещенных (активен)** и **Список разрешенных**. По умолчанию таблица правил контроля приложений на обеих закладках пустая.

Таблица 116. Параметры правил контроля приложений

Параметр	Описание
Категория	Название категории приложений, которая используется в работе правила.
Статус	Статус работы правила контроля приложений: • <i>Включено</i> – правило включено, Контроль приложений применяет это правило во время работы. • <i>Выключено</i> – правило выключено и не используется во время работы Контроля приложений. • <i>Тест</i> – Контроль приложений разрешает запуск приложений, которые удовлетворяют условиям правила, но записывает информацию о запуске этих приложений в отчет.

Вы можете добавлять (см. раздел "Окно Правило Контроля приложений" на стр. [435](#)), изменять и удалять правила контроля приложений.

Окно Правило Контроля приложений

В этом окне вы можете настроить параметры правила Контроля приложений.

Таблица 117. Настройка правила контроля приложений

Параметр	Описание
Описание правила	Описание правила Контроля приложений.
Статус	Вы можете выбрать статус работы правила контроля приложений: • <i>Включено</i> – правило включено, Контроль приложений применяет это правило во время работы. • <i>Выключено</i> – правило выключено и не используется во время работы Контроля приложений. • <i>Тест</i> – Контроль приложений разрешает запуск приложений, которые удовлетворяют условиям правила, но записывает информацию о запуске этих приложений в отчет.
Категория	По ссылке Выбрать категорию открывается окно Категории приложений (см. раздел "Окно Категории приложений" на стр. 436).
Пользователи и их права	Таблица содержит список имен пользователей или названий групп пользователей, на которых распространяется правило контроля приложений, и назначенные им типы доступа, и состоит из следующих столбцов: • Имя пользователя или группы – имена пользователей или названия групп пользователей, на которых распространяется правило контроля приложений. • Доступ – тип доступа (разрешение или запрет на запуск приложений). Переключатель включает или выключает тип доступа: Разрешать запуск приложений или Блокировать запуск приложений. Вы можете добавлять и изменять (см. раздел "Окно Выбор пользователя или группы" на стр. 436), а также удалять пользователей или группы пользователей.

Окно Категории приложений

В этом окне вы можете добавить новую категорию или настроить параметры категории для правила контроля приложений.

Использование KL-категорий приложения Kaspersky Security Center не поддерживается приложением Kaspersky Industrial CyberSecurity for Linux Nodes.

Таблица 118. Категории Контроля приложений

Параметр	Описание
Название категории	Строка поиска добавленных категорий приложений.
Добавить	При нажатии на кнопку запускается мастер создания категории. Следуйте указаниям мастера.
Изменить	При нажатии на кнопку открывается окно свойств категории, в котором вы можете изменить параметры категории.
Удалить	При нажатии на кнопку выбранная категория удаляется. Категорию Золотой образ (локальная) удалить нельзя.

Окно Выбор пользователя или группы

В этом окне вы можете указать локального или доменного пользователя или группу пользователей, для которых вы хотите настроить правило.

Таблица 119. Настройка правила Контроля приложений

Параметр	Описание
Вручную	Если выбран этот вариант, в поле ниже вам нужно ввести имя локального или доменного пользователя или название группы пользователей, на которых будет распространяться правило контроля приложений.
Список групп или пользователей	Если выбран этот вариант, в поле поиска вы можете ввести критерии поиска имени пользователя или названия группы пользователей, на которых будет распространяться правило контроля приложений, или выбрать название группы пользователей в списке ниже.

Настройка контроля приложений в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры контроля приложений в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Контроль безопасности** → **Контроль приложений**).

Таблица 120. Параметры компонента Контроль приложений

Параметр	Описание
Включить Контроль приложений	Флажок включает компонент Контроль приложений. По умолчанию флажок снят.
Режим работы Контроля приложений	Режим работы Контроля приложений при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам: • Блокировать. При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes блокирует запуск приложения, удовлетворяющего правилам. • Информировать (значение по умолчанию). При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes формирует событие о попытке запуска приложения, удовлетворяющего правилам.
Режим Контроля приложений	Режим компонента Контроль приложений: • Список разрешенных. При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. • Список запрещенных (значение по умолчанию). При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.
Правила Контроля приложений	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Правила Контроля приложений (см. раздел "Окно Правила Контроля приложений" на стр. 437).
Применение правил	В раскрывающемся списке вы можете выбрать способ добавления правил: • Заменить правилами из политики локальные правила. При выборе этого элемента списка приложение применяет только правила, заданные в политике. • Добавить правила из политики к локальным правилам (значение по умолчанию). При выборе этого элемента списка приложение применяет правила, заданные в политике, совместно с локальными правилами, настроенными на защищаемом устройстве.

Окно Правила Контроля приложений

Таблица **Правила Контроля приложений** содержит правила, используемые компонентом Контроль приложений. По умолчанию таблица правил контроля приложений пустая.

Таблица 121. Параметры правил контроля приложений

Параметр	Описание
Название категории	Название категории приложений, которая используется в работе правила.
Статус	Статус работы правила контроля приложений: • <i>Включено</i> – правило включено, Контроль приложений применяет это правило во время работы. • <i>Выключено</i> – правило выключено и не используется во время работы Контроля приложений. • <i>Тест</i> – Контроль приложений разрешает запуск приложений, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих приложений в отчете. Вы можете изменить статус правила в окне Добавление правила / Изменение правила (см. раздел "Окно Добавление правила" на стр. 438).

Окно Добавление правила

В этом окне вы можете настроить параметры правила контроля приложений.

Таблица 122. Добавление правила контроля приложений

Параметр	Описание
Описание	Описание правила Контроля приложений.
Статус правила	В раскрывающемся списке вы можете выбрать статус работы правила контроля приложений: • <i>Включено</i> – правило включено, Контроль приложений применяет это правило во время работы. • <i>Выключено</i> – правило выключено и не используется во время работы Контроля приложений. • <i>Тест</i> – Контроль приложений разрешает запуск приложений, которые удовлетворяют условиям правила, но записывает информацию о запуске этих приложений в отчет.
Категория	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Категории приложений (см. раздел "Окно Категории приложений" на стр. 439).
Пользователи и их права	Таблица содержит список пользователей или групп пользователей, на которых распространяется правило контроля приложений, и назначенные им типы доступа, и состоит из следующих столбцов: • Имя пользователя или группы – имена пользователей или названия групп пользователей, на которых распространяется правило контроля приложений. • Доступ – тип доступа: Разрешать запуск приложений или Блокировать запуск приложений. Вы можете добавлять и изменять (см. раздел "Окно Пользователь или группа" на стр. 439), а также удалять пользователей или группы пользователей.

Окно Категории приложений

В этом окне вы можете добавить новую категорию или настроить параметры категории для правила контроля приложений.

Использование KL-категорий приложения Kaspersky Security Center не поддерживается приложением Kaspersky Industrial CyberSecurity for Linux Nodes.

Таблица 123. Категории Контроля приложений

Параметр	Описание
Название категории	Список добавленных категорий Контроля приложений.
Добавить	При нажатии на кнопку запускается мастер создания категории. Следуйте указаниям мастера.
Изменить	При нажатии на кнопку открывается окно свойств категории, в котором вы можете изменить параметры категории.

Окно Пользователь или группа

В этом окне вы можете указать локального или доменного пользователя или группу пользователей, для которых вы хотите настроить правило.

Таблица 124. Добавление правила Контроля приложений

Параметр	Описание
Тип	Пользователь или Группа , на которых распространяется правило.
Имя пользователя или группы	Имя пользователя или название группы пользователей, на которых распространяется правило контроля приложений.
Доступ	Тип доступа: Разрешать или Блокировать запуск приложений.

Экспорт и импорт параметров и категорий через Kaspersky Security Center

В Kaspersky Security Center вы можете экспортировать в файл формата JSON параметры Контроля приложений, правила и категории приложений, настроенные на управляемом устройстве. Затем вы можете при необходимости изменить параметры Контроля приложений, правила и категории приложений в файле и импортировать на любое управляемое устройство.

Экспорт и импорт параметров, правил и категорий Контроля приложений для управляемого устройства доступен, если в политике, которая применяется на управляемом устройстве, разрешено локальное управление параметрами Контроля приложений.

Экспорт и импорт в Web Console

В Web Console вы можете экспортировать и импортировать параметры Контроля приложений в свойствах устройства (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → **Приложения** → ссылка <название приложения Kaspersky Industrial CyberSecurity for Linux Nodes> → **Параметры приложения** → **Контроль приложений**).

С помощью кнопок **Экспортировать** и **Импортировать** в блоке **Категории приложений** вы можете:

- Экспортировать в файл формата JSON список категорий приложений, настроенный на управляемом устройстве. Файл расположен в директории загрузки браузера по умолчанию.
- Импортировать на управляемое устройство список категорий приложений из файла формата JSON. В результате импорта список категорий в приложении на устройстве перезаписывается.

С помощью кнопок **Экспортировать** и **Импортировать** в блоке **Параметры Контроля приложений** вы можете:

- Экспортировать в файл формата JSON основные параметры и правила Контроля приложений, настроенные на управляемом устройстве. Файл расположен в директории загрузки браузера по умолчанию.
- Импортировать на управляемое устройство основные параметры и правила Контроля приложений из файла формата JSON. В результате импорта в приложении на устройстве применяются новые параметры и правила Контроля приложений.

Экспорт и импорт в Консоли администрирования

В Консоли администрирования вы можете экспортировать и импортировать параметры Контроля приложений в свойствах устройства (**Управляемые устройства** → **Устройства** → двойной щелчок мыши на имени устройства → **Программы** → двойной щелчок мыши на названии приложения Kaspersky Industrial CyberSecurity for Linux Nodes → **Контроль приложений**).

С помощью кнопок **Экспортировать** и **Импортировать** в блоке **Категории приложений** вы можете:

- Экспортировать в файл формата JSON список категорий приложений, настроенный на управляемом устройстве.
- Импортировать на управляемое устройство список категорий приложений из файла формата JSON. В результате импорта список категорий в приложении на устройстве перезаписывается.

С помощью кнопок **Экспортировать** и **Импортировать** в блоке **Параметры Контроля приложений** вы можете:

- Экспортировать в файл формата JSON основные параметры и правила Контроля приложений, настроенные на управляемом устройстве.
- Импортировать на управляемое устройство основные параметры и правила Контроля приложений из файла формата JSON. В результате импорта в приложении на устройстве применяются новые параметры и правила Контроля приложений.

Настройка контроля приложений в командной строке

В командной строке вы можете управлять контролем приложений с помощью предустановленной задачи **Контроль приложений** (*Application_Control*).

По умолчанию задача **Контроль приложений** не запущена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачу вручную.

Вы можете настраивать параметры (см. раздел "Параметры задачи Контроль приложений" на стр. [441](#)) контроля приложений на устройстве, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи Контроль приложений.

Если вы меняете список разрешенных приложений или запрещаете запуск всех приложений и/или приложений, влияющих на работу Kaspersky Industrial CyberSecurity for Linux Nodes, то при изменении параметров задачи с помощью конфигурационного файла (см. раздел "Изменение параметров задачи с помощью конфигурационного файла" на стр. [130](#)) или с помощью ключей командной строки (см. раздел "Изменение параметров задачи с помощью ключей командной строки" на стр. [132](#)) требуется запускать команду `kics-control --set-settings` с флагом `--accept`.

Вы также можете настраивать параметры Контроля приложений с помощью команд управления Контролем приложений:

- Создавать и изменять списки категорий (см. раздел "Создание и изменение списка категорий" на стр. [446](#)).
- Просматривать список созданных в приложении категорий (см. раздел "Просмотр списка созданных категорий" на стр. [447](#)).
- Настраивать список правил контроля приложений (см. раздел "Настройка списка правил контроля приложений" на стр. [448](#)).

В этом разделе

Параметры задачи Контроль приложений	441
Создание и изменение списка категорий	446
Просмотр списка созданных категорий	447
Настройка списка правил контроля приложений	448

Параметры задачи Контроль приложений

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Контроль приложений.

Таблица 125. Параметры задачи Контроль приложений

Параметр	Описание	Значения
AppControlMode	Способ применения правил компонента Контроль приложений (на стр. 431).	AllowList – Kaspersky Industrial CyberSecurity for Linux Nodes запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. DenyList (значение по умолчанию) – Kaspersky Industrial CyberSecurity for Linux Nodes разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.
AppControlRulesAction	Режим работы компонента Контроль приложений (на стр. 431) при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам	Block – Kaspersky Industrial CyberSecurity for Linux Nodes блокирует запуск приложения, удовлетворяющего правилам. Notify (значение по умолчанию) – Kaspersky Industrial CyberSecurity for Linux Nodes тестирует правила и формирует событие об обнаружении приложения, удовлетворяющего правилу.
Секция [Categories.item_#] содержит следующие параметры:		
Name	Название категории приложений, для которой будет применяться правило.	
UseIncludes	Использование включающих условий (см. раздел "О правилах контроля приложений" на стр. 432) для срабатывания правила.	Yes – применять правило к приложению, если приложение соответствует хотя бы одному включающему условию. No (значение по умолчанию) – не применять правило к приложению, даже если приложение соответствует включающему условию.
IncludeFileNames.item_#	Имя исполняемого файла, на которое срабатывает правило.	Для указания имени файла вы можете использовать маски.
IncludeFolders.item_#	Имя директории с исполняемым файлом приложения, на которое срабатывает правило.	Для указания имени директории вы можете использовать маски.
IncludeHashes.item_#	Хеш SHA256 исполняемого файла, на который срабатывает правило.	Допускается использование только SHA256.

Параметр	Описание	Значения
UseExcludes	Использование исключаящих условий (см. раздел "О правилах контроля приложений" на стр. 432) для срабатывания правила.	Yes – не применять правило к приложению, если приложение соответствует хотя бы одному исключаящему условию или не соответствует ни одному включающему условию. No (значение по умолчанию) – применять правило к приложению, даже если приложение соответствует исключаящему условию.
ExcludeFileNames.item_#	Имя исполняемого файла, на которое срабатывает правило.	Для указания имени файла вы можете использовать маски.
ExcludeFolders.item_#	Имя директории с исполняемым файлом приложения, на которое срабатывает правило.	Для указания имени директории вы можете использовать маски.
ExcludeHashes.item_#	Хеш SHA256 исполняемого файла, на который срабатывает правило.	Допускается использование только SHA256.
Секция [AllowListRules.item_#] содержит список правил контроля приложений для режима работы <i>Список разрешенных (AllowList)</i> . Каждая секция [AllowListRules.item_#] содержит следующие параметры:		
Description	Описание правила контроля приложений.	
AppControlRuleStatus	Статус работы правила контроля приложений (см. раздел "О правилах контроля приложений" на стр. 432).	On (значение по умолчанию) – правило включено, Kaspersky Industrial CyberSecurity for Linux Nodes применяет это правило для контроля приложений. Off – правило не используется для контроля приложений. Test – Kaspersky Industrial CyberSecurity for Linux Nodes разрешает запуск приложений, на которые распространяется действие правила, но фиксирует информацию о запуске этих приложений в отчете.
Category	Название категории приложений, для которой применяется правило. Вы можете указать в качестве категории категорию "Golden Image" (см. раздел "Параметры задачи Инвентаризация" на стр. 459).	
Секция [AllowListRules.item_#.ACL.item_#] содержит список пользователей, которым разрешен или запрещен запуск приложений.		

Параметр	Описание	Значения
Access	Тип доступа, назначаемый пользователю или группе пользователей.	Allow (значение по умолчанию) – разрешать запуск приложений. Block – запрещать запуск приложений.
Principal	Пользователь или группа пользователей, на которых распространяется правило контроля приложений.	\Everyone (значение по умолчанию) – правило применяется для всех пользователей. <имя пользователя> – имя пользователя, для которого применяется правило. &@<название группы> – название группы пользователей, для которых применяется правило.
Секция [DenyListRules.item_#] содержит список правил контроля приложений для режима работы <i>Список запрещенных (DenyList)</i> . Каждая секция [DenyListRules.item_#] содержит следующие параметры:		
Description	Описание правила контроля приложений.	
AppControlRuleStatus	Статус работы правила контроля приложений (см. раздел "О правилах контроля приложений" на стр. 432).	On (значение по умолчанию) – правило включено, Kaspersky Industrial CyberSecurity for Linux Nodes применяет это правило для контроля приложений. Off – правило не используется для контроля приложений. Test – Kaspersky Industrial CyberSecurity for Linux Nodes разрешает запуск приложений, на которые распространяется действие правила, но записывает информацию о запуске этих приложений в отчет.
Category	Название созданной категории приложений, для которой применяется правило. Вы можете указать в качестве категории список приложений "Golden Image" (см. раздел "Параметры задачи Инвентаризация" на стр. 459).	
Секция [DenyListRules.item_#.ACL.item_#] содержит список пользователей, которым разрешен или запрещен запуск приложений.		
Access	Тип доступа, назначаемый пользователю или группе пользователей.	Allow – разрешать запуск приложений. Block (значение по умолчанию) – запрещать запуск приложений.

Параметр	Описание	Значения
Principal	Пользователь или группа пользователей, на которых распространяется правило контроля приложений.	\Everyone (значение по умолчанию) – правило применяется для всех пользователей. <имя пользователя> – имя пользователя, для которого применяется правило. @<название группы> – название группы пользователей, для которых применяется правило.

Создание и изменение списка категорий

Вы можете создать новую категорию двумя способами:

- с помощью команды `kics --set-settings` и конфигурационного файла параметров задачи Контроль приложений (см. раздел "Параметры задачи Контроль приложений" на стр. [441](#)) (Application_Control);
- с помощью команды `kics --set-categories` и конфигурационного файла параметров категории.

► Чтобы создать категории приложений, выполните следующую команду:

```
kics-control --set-categories --file <путь к конфигурационному файлу>
```

где:

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу с параметрами категорий.

Файл с параметрами категорий должен иметь такую структуру:

```
[
  {
    "Exclude" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)", "(FileHash == <хеш исполняемого файла>)" ],
    "GUID" : "<уникальный идентификатор категории>",
    "Include" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)", "(FileHash == <хеш исполняемого файла>)" ],
    "Name" : "<название категории 1>"
  },
  {
    "Exclude" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)", "(FileHash == <хеш исполняемого файла>)" ],
    "GUID" : "<уникальный идентификатор категории>",
    "Include" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)", "(FileHash == <хеш исполняемого файла>)" ],
    "Name" : "<название категории 2>"
  }
]
```

Для указания имени файла в полях `Exclude` и `Include` вы можете использовать маски.

Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории.

Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/*/file*/ или /dir/file*/*.

Вы можете указать символ ? вместо любого одного символа (включая символ /) в имени файла или директории.

Параметр Name обязательный, если вы не укажете название категории, она не будет создана или будет удалена. Параметр GUID также обязательный, если вы его не укажете, отобразится сообщение об ошибке и категория не будет создана. Параметр GUID требуется указывать без дефисов.

► Чтобы изменить список созданных категорий приложений, выполните следующую команду:

```
kics-control --set-categories [--names <название категории 1> <название категории 2> ... <название категории N>] --file <путь к конфигурационному файлу>
```

где:

- <название категории 1> <название категории 2> ... <название категории N> – названия категорий, информацию о которых вы хотите изменить. Если вы хотите изменить информацию о нескольких категориях, укажите названия категорий через пробел. Если вы не укажете название категории, существующие категории будут удалены и будут созданы новые категории из указанного файла.
- --file <путь к конфигурационному файлу> – путь к конфигурационному файлу с параметрами категорий.

Просмотр списка созданных категорий

В командной строке вы можете просматривать список созданных категорий приложений с помощью команды управления контролем приложений (на стр. [694](#)).

Список созданных категорий содержит следующие категории:

- категории, созданные в Kaspersky Security Center;
- категории, добавленные в параметрах задачи Контроль приложений через командную строку;
- категория "GoldenImage", созданная с помощью задачи Инвентаризация (см. раздел "Инвентаризация" на стр. [450](#)) (в Kaspersky Security Center или через командную строку).

► Чтобы просмотреть список всех созданных категорий приложений, выполните следующую команду:

```
kics-control --get-categories [--file <путь к конфигурационному файлу>] [--json]
```

где:

- --file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу формата JSON, в который будут выведены параметры.

- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Kaspersky Industrial CyberSecurity for Linux Nodes отобразит следующую информацию о каждой категории приложений:

- уникальный идентификатор (GUID) категории;
- название категории;
- список включающих условий для срабатывания правила;
- список исключающих условий для срабатывания правила.

► Чтобы просмотреть список созданных категорий приложений, выполните следующую команду:

```
kics-control --get-categories [--names <название категории 1> <название категории 2> ... <название категории N>] [--file <путь к конфигурационному файлу>] [--json]
```

где:

- `<название категории 1> <название категории 2> ... <название категории N>` – названия категорий, информацию о которых вы хотите просмотреть. Если вы хотите просмотреть информацию о нескольких категориях, укажите названия категорий через пробел.
- `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу формата JSON, в который будут выведен список категорий.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Если в параметрах задачи Контроль приложений (см. раздел "Параметры задачи Контроль приложений" на стр. 441) в секции `[Categories.item_#]` для включающих или исключающих условий срабатывания правила вы указали символические ссылки на файл приложения или на директорию с исполняемыми файлами, то при просмотре списка категорий для этих условий будет отображаться исходный путь, на который ссылается символическая ссылка.

Настройка списка правил контроля приложений

► Чтобы просмотреть список правил контроля приложений, выполните следующую команду:

```
kics-control --get-settings 21 [--file <путь к конфигурационному файлу>] [--json]
```

где:

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут выведены параметры.

`--json` – выводить данные в формате JSON.

Kaspersky Industrial CyberSecurity for Linux Nodes отобразит следующую информацию о правилах контроля приложений:

- режим работы компонента Контроль приложений;
 - действие, которое Контроль приложений будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенному правилу;
 - описание правила контроля приложений (если есть);
 - статус работы правила контроля приложений;
 - название категории приложений, для которой применяется правило;
 - тип доступа, назначенный пользователю или группе пользователей;
 - пользователь или группа пользователей, на которых распространяется правило контроля приложений.
- *Чтобы изменить список категорий приложений и правил контроля приложений, выполните следующую команду:*

```
kics-control --set-settings 21 [--file <путь к конфигурационному файлу>]  
[--json]
```

где:

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры.

`--json` – импорт данных из файла в формате JSON.

- *Чтобы удалить список категорий приложений и правил контроля приложений, выполните следующую команду:*

```
kics-control --set-settings 21 --set-to-default
```

Инвентаризация

Задача Инвентаризация позволяет получить информацию обо всех исполняемых файлах приложений, хранящихся на клиентских устройствах. Получение информации о приложениях, установленных на устройствах, может быть полезно, например, для создания правил контроля приложений (см. раздел "О правилах контроля приложений" на стр. [432](#)).

Вы можете настраивать следующие параметры инвентаризации:

- Выбирать типы объектов, которые приложение будет обнаруживать на устройстве в ходе инвентаризации (файлы, скрипты).
- Включать и выключать добавление приложений, обнаруженных на устройстве задачей Инвентаризация, в категорию приложений "Золотой образ" ("Golden Image").
- Настраивать области инвентаризации (пути к директориям, в которых нужно искать исполняемые файлы приложений).
- Настраивать исключения из инвентаризации.

В этом разделе

Инвентаризация в Web Console	450
Инвентаризация в Консоли администрирования	454
Инвентаризация в командной строке	458

Инвентаризация в Web Console

В Web Console вы можете выполнять инвентаризацию приложений защищаемого устройства с помощью задачи *Инвентаризация*. Вы можете создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)) пользовательские задачи инвентаризации. Вы можете настраивать параметры инвентаризации, изменяя (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) параметры этих задач.

В базе данных приложения 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 устройства с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

Таблица 126. Параметры задачи Инвентаризация

Параметр	Описание
Добавлять файлы в категорию Золотой образ	Флажок включает или выключает добавление приложений, обнаруженных на устройстве задачей Инвентаризация, в категорию приложений "Золотой образ" ("Golden Image"). Если флажок установлен, то в правилах контроля приложений (см. раздел "О правилах контроля приложений" на стр. 432) вы можете использовать категорию "Золотой образ". По умолчанию флажок снят.

Параметр	Описание
Проверять все исполняемые файлы	Флажок включает или выключает проверку исполняемых файлов. По умолчанию флажок установлен.
Проверять двоичные файлы	Флажок включает или выключает проверку двоичных файлов (с расширениями elf, java и рус). По умолчанию флажок установлен.
Проверять скрипты	Флажок включает или выключает проверку скриптов. По умолчанию флажок установлен.
Области инвентаризации	Таблица, содержащая области инвентаризации, проверяемые приложением. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область инвентаризации – /usr/bin. Области инвентаризации в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки для задачи Инвентаризация.

Таблица 127. Параметры области инвентаризации

Параметр	Описание
Название области	Поле ввода названия области инвентаризации. Это название будет отображаться в таблице раздела Параметры проверки. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время выполнения задачи. Если флажок установлен, приложение обрабатывает эту область инвентаризации во время выполнения задачи. Если флажок снят, приложение не обрабатывает эту область инвентаризации во время выполнения задачи. В дальнейшем вы можете включить эту область в параметры задачи, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область инвентаризации. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле не должно быть пустым. По умолчанию указан путь / – приложение проверяет все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время выполнения задачи. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Раздел Области исключения

В разделе **Области исключения** для задачи Инвентаризация вы можете настроить области исключения из проверки.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 128. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения из проверки для задачи Инвентаризация.

Таблица 129. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 182). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время выполнения задачи. Если флажок установлен, приложение исключает эту область во время выполнения задачи. Если флажок снят, приложение включает эту область во время выполнения задачи. В дальнейшем вы можете исключить эту область из проверки, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения из инвентаризации. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, <code>/dir/*/file</code> или <code>/dir/**/file</code>. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, <code>/dir/**/file*</code> или <code>/dir/file**/</code>. Маску ** можно использовать в имени директории только один раз. Например, <code>/dir/**/**/file</code> – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Вы можете добавлять, изменять и удалять маски.

Инвентаризация в Консоли администрирования

В Консоли администрирования Kaspersky Security Center вы можете выполнять инвентаризацию приложений защищаемого устройства с помощью задачи *Инвентаризация*.

Вы можете создавать (см. раздел "Создание задач в Консоли администрирования" на стр. [116](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Консоли администрирования" на стр. [117](#)) пользовательские задачи инвентаризации. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задач в Консоли администрирования" на стр. [117](#)) параметры задач.

В базе данных приложения 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 устройства с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

Таблица 130. Параметры задачи Инвентаризация

Параметр	Описание
Добавлять файлы в категорию Золотой образ	Флажок включает или выключает добавление приложений, обнаруженных на устройстве задачей Инвентаризация, в категорию приложений "Золотой образ" ("Golden Image"). Если флажок установлен, то в правилах контроля приложений (см. раздел "О правилах контроля приложений" на стр. 432) вы можете использовать категорию "Золотой образ". По умолчанию флажок снят.
Проверять все исполняемые файлы	Флажок включает или выключает проверку исполняемых файлов. По умолчанию флажок установлен.
Проверять двоичные файлы	Флажок включает или выключает проверку двоичных файлов (с расширениями elf, java и рус). По умолчанию флажок установлен.
Проверять скрипты	Флажок включает или выключает проверку скриптов. По умолчанию флажок установлен.
Области инвентаризации	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области проверки (см. раздел "Окно Области проверки" на стр. 191).

В разделе **Области исключения** для задачи Инвентаризация вы можете также настроить области исключения из проверки.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки – /usr/bin.

Таблица 131. Параметры области проверки задачи Инвентаризация

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Industrial CyberSecurity for Linux Nodes проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки для задачи Инвентаризация.

Таблица 132. Параметры области инвентаризации

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна Области проверки (см. раздел "Окно Области проверки" на стр. 191). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время выполнения задачи. Если флажок установлен, приложение обрабатывает эту область проверки во время выполнения задачи. Если флажок снят, приложение не обрабатывает эту область проверки во время выполнения задачи. В дальнейшем вы можете включить эту область в параметры задачи, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время выполнения задачи. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Раздел Исключения

Таблица 133. Параметры исключений из проверки

Блок параметров	Описание
Области исключения	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области исключения (см. раздел "Окно Области исключения" на стр. 202). В этом окне вы можете задать список областей исключений из мониторинга.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 134. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из проверки для задачи Инвентаризация.

Таблица 135. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 202). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время выполнения задачи. Если флажок установлен, приложение исключает эту область во время выполнения задачи. Если флажок снят, приложение включает эту область во время выполнения задачи. В дальнейшем вы можете исключить эту область из проверки, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения из инвентаризации. Для указания пути вы можете использовать маски. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Вы можете добавлять, изменять и удалять маски.

Инвентаризация в командной строке

В командной строке вы можете выполнять инвентаризацию приложений защищаемого устройства следующими способами:

- С помощью предустановленной задачи Инвентаризация (см. раздел "Параметры задачи Инвентаризация" на стр. [459](#)) (*Inventory_Scan*). Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) эту задачу вручную и настраивать расписание (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)) запуска задачи. Вы можете настраивать параметры (см. раздел "Параметры задачи Инвентаризация" на стр. [459](#)) проверки, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры этой задачи.
- С помощью пользовательских задач (см. раздел "Создание задачи в командной строке" на стр. [127](#)) инвентаризации (задач типа *InventoryScan*). Вы можете запускать, останавливать, приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) пользовательские задачи вручную и настраивать расписание (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)) запуска задач.

Вы можете просматривать список приложений, обнаруженных на устройстве в результате выполнения задачи Инвентаризация, с помощью команд управления контролем приложений (см. раздел "Команды управления Контролем приложений" на стр. [694](#)).

В этом разделе

Параметры задачи Инвентаризация	459
Просмотр списка обнаруженных приложений	462

Параметры задачи Инвентаризация

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Инвентаризация.

Таблица 136. Параметры задачи Инвентаризация

Параметр	Описание	Значения
ScanScripts	Включение проверки скриптов.	Yes (значение по умолчанию) – проверять скрипты. No – не проверять скрипты.
ScanBinaries	Включение проверки бинарных файлов (elf, java и рус).	Yes (значение по умолчанию) – проверять бинарные файлы. No – не проверять бинарные файлы.
ScanAllExecutable	Включение проверки файлов с исполняемым битом.	Yes (значение по умолчанию) – проверять файлы с исполняемым битом. No – не проверять файлы с исполняемым битом.
CreateGoldenImage	Добавление приложений, обнаруженных на устройстве задачей Инвентаризация, в категорию приложений "Золотой образ" ("Golden Image"). Если значение параметра CreateGoldenImage=Yes, то в правилах контроля приложений (см. раздел "О правилах контроля приложений" на стр. 432) вы можете использовать категорию приложений "Золотой образ".	Yes – добавлять обнаруженные приложения в категорию приложений "Золотой образ". No (значение по умолчанию) – не добавлять обнаруженные приложения в категорию приложений "Золотой образ".
Секция [ScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области инвентаризации, содержит дополнительную информацию об области инвентаризации. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects.
UseScanArea	Включение проверки указанной области инвентаризации. Для выполнения задачи требуется включить проверку хотя бы одной области инвентаризации.	Yes (значение по умолчанию) – проверять указанную область инвентаризации. No – не проверять указанную область инвентаризации.
AreaMask.item_#	Ограничение области инвентаризации. В области инвентаризации приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области инвентаризации. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты).

Параметр	Описание	Значения
Path	Путь к директории с проверяемыми объектами.	<путь к локальной директории> – проверять объекты в указанной директории. Значение по умолчанию: /usr/bin
Секция [ExcludedFromScanScope.item_#] содержит следующие параметры.		
AreaDesc	Описание области исключения из инвентаризации, содержит дополнительную информацию об области инвентаризации.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из инвентаризации.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.
AreaMask.item_#	Ограничение области исключения из инвентаризации по маскам в формате shell. Если параметр не указан, приложение исключает все объекты в области инвентаризации. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (исключать все объекты).
Path	Путь к директории с исключаемыми объектами.	<путь к локальной директории> – исключать из проверки объекты в указанной директории. Для указания пути вы можете использовать маски.

Просмотр списка обнаруженных приложений

- Чтобы просмотреть список приложений, обнаруженных на устройстве, выполните следующую команду:

```
kics-control --get-app-list [--json]
```

где --json – выводить данные в формате JSON.

Kaspersky Industrial CyberSecurity for Linux Nodes отобразит следующую информацию об обнаруженных приложениях:

- **Дата и время инвентаризации.** Дата и время выполнения задачи Инвентаризация.
- **Количество приложений.** Количество приложений, обнаруженных на устройстве.
- **Список приложений, содержащий следующую информацию:**
 - **Путь.** Путь к приложению.
 - **Хеш.** Хеш-сумма приложения.
 - **Тип.** Тип приложения. Например: Script, Executable.

- **Категории.** Категории, к которым принадлежит приложение (если они были созданы ранее). Вы можете просмотреть список созданных категорий приложений с помощью команды `kics-control --get-categories` (см. раздел "Команды управления Контролем приложений" на стр. [694](#)).

При добавлении новой категории информация о ней в списке приложений автоматически не обновляется. Для обновления списка приложений требуется повторный запуск задачи Инвентаризация.

Контроль устройств

Компонент *Контроль устройств* позволяет управлять доступом пользователей к устройствам, которые установлены на клиентском устройстве или подключены к нему (например, жестким дискам, камерам или модулям Wi-Fi). Управление доступом позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных.

По умолчанию Контроль устройств выключен.

Контроль устройств управляет доступом на следующих уровнях:

- **Тип устройства** по классификации компонента Контроль устройств (например, принтеры, съемные диски, CD/DVD-приводы). Для каждого типа устройств может применяться один из следующих режимов доступа:
 - *Разрешать* – предоставлять доступ к устройствам этого типа.
 - *Блокировать* – запрещать доступ к устройствам этого типа.
 - *В зависимости от шины подключения* – разрешать или запрещать доступ к устройствам в зависимости от режима доступа для шины, по которой подключено устройство.
 - *По правилам* – разрешать или запрещать доступ к устройствам в зависимости от правил доступа к устройствам. *Правило доступа к устройству* – это набор параметров, которые определяют, какие пользователи и в какое время могут получить доступ к устройствам, установленным на клиентском устройстве или подключенным к нему.

При подключении устройства, доступ к которому запрещен, приложение запрещает указанным в правиле пользователям доступ к этому устройству и выводит уведомление. При попытке чтения и записи на этом устройстве приложение запрещает чтение/запись указанным в правиле пользователям без вывода уведомления.

Если при попытке совершить операцию с устройством, для которого установлен режим доступа *По правилам*, не нашлось правила, активного на момент доступа, то операция с устройством будет запрещена.

- **Шина подключения.** *Шина подключения* – это интерфейс, с помощью которого устройства подключаются к клиентскому устройству (например, USB, FireWire). Для шин подключения может применяться один из следующих режимов доступа:
 - *Разрешать* – предоставлять доступ к устройствам, подключенным по этой шине подключения.
 - *Блокировать* – запрещать доступ к устройствам, подключенным по этой шине подключения.

Например, может быть запрещен доступ ко всем устройствам, подключенным по шине USB.

По умолчанию для всех типов устройств выбран режим *В зависимости от шины подключения*, для шин подключения выбран режим *Разрешать*. В соответствии с этими параметрами Контроль устройств предоставляет пользователям полный доступ ко всем устройствам.

Блокировка устройств по типу устройства и по шине подключения через системный драйвер устройства не поддерживается на ядрах ОС Linux: 3.10, 5.14, 5.15, 5.17, 6.1. На этих ядрах и при режиме доступа *По правилам* блокируются только открытие файлов и чтение директорий (то есть получение имен файлов и директорий).

При первом включении компонента Контроль устройств для всех обнаруженных устройств с известным типом устройства или шины формируется событие *Доступ к устройству разрешен*, а при следующих запусках повторные события для этих устройств не формируются, если не было изменений в параметрах контроля для этих устройств.

При выключении компонента Контроль устройств приложение разблокирует доступ к заблокированным устройствам.

Вы можете включать и выключать Контроль устройств, а также настраивать параметры работы компонента:

- Выбирать режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств: блокировать или только информировать о попытке доступа к устройству.
- Выбирать режим доступа к устройствам в зависимости от их типа.
- Выбирать режим доступа для шины, по которой подключаются устройства.
- Исключать отдельные устройства из области действия Контроля устройств, добавляя их в список доверенных устройств. *Доверенные устройства* – это устройства, к которым у пользователей есть полный доступ. Вы можете добавлять устройства в список доверенных по идентификатору или маске идентификатора устройства. Например, вы можете разрешить доступ к конкретным USB-устройствам или только к USB-накопителям, при этом доступ к остальным USB-устройствам будет запрещен.

Если вы управляете приложением из командной строки, вы можете посмотреть идентификаторы подключенных устройств (см. раздел "Просмотр списка подключенных устройств в командной строке" на стр. [488](#)), выполнив на клиентском устройстве команду `kics-control --get-device-list`.

Если вы управляете приложением с помощью Kaspersky Security Center, информация об устройствах, установленных на клиентских устройствах или подключенных к ним, может передаваться на Сервер администрирования. Передача информации включена по умолчанию (см. раздел "Настройка отправки информации в хранилище Kaspersky Security Center" на стр. [583](#)).

Информация об устройствах передается, если клиентское устройство находится под управлением активной политики и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в политике Агента администрирования, по умолчанию – каждые 15 минут).

- Настраивать расписание доступа для устройств (только для жестких дисков, съемных дисков, дискет и CD/DVD-приводов).

Если в общих параметрах приложения (см. раздел "Выбор режима перехвата файловых операций" на стр. [574](#)) выключена блокировка доступа к файлам во время проверки, то заблокировать доступ к устройствам с помощью расписания доступа для устройств невозможно.

- Настраивать правила доступа к устройствам в зависимости от их типа. Вы можете разрешать или запрещать доступ для указанных пользователей в указанное время.

Контроль устройств игнорирует исключение точек монтирования (см. раздел "Настройка глобальных исключений" на стр. [566](#)). Доступ к устройству, смонтированному в исключенной точке монтирования, может быть ограничен в соответствии с настроенными параметрами Контроля устройств.

В этом разделе

Настройка контроля устройств в Web Console	466
Настройка контроля устройств в Консоли администрирования	471
Настройка Контроля устройств в командной строке	476

Настройка контроля устройств в Web Console

В Web Console вы можете настраивать параметры контроля устройств в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения → Контроль безопасности → Контроль устройств**).

Таблица 137. Параметры компонента Контроль устройств

Параметр	Описание
Контроль устройств включен / выключен	Переключатель включает или выключает компонент Контроль устройств. По умолчанию переключатель выключен.
Настроить доверенные устройства	По ссылке открывается окно Доверенные устройства . В этом окне вы можете добавлять устройства в список доверенных по идентификатору устройства (см. раздел "Окно Доверенное устройство (Идентификатор устройства)" на стр. 467) или выбрав их из списка устройств, обнаруженных на клиентских устройствах (см. раздел "Окно Доверенное устройство (Список обнаруженных устройств)" на стр. 467).
Режим работы Контроля устройств	Режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств: • Информировать (значение по умолчанию). При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes тестирует выбранный режим доступа и формирует событие об обнаружении попытки доступа к устройству. • Блокировать. При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes применяет режим доступа, заданный для устройства или шины.
Настроить параметры доступа для типов устройств	По ссылке открывается окно Типы устройств (см. раздел "Окно Типы устройств" на стр. 468). В этом окне вы можете настроить параметры доступа к устройствам в зависимости от их типа.
Настроить параметры доступа для шин подключения	По ссылке открывается окно Шины подключения (см. раздел "Окно Шины подключения" на стр. 471). В этом окне вы можете настроить параметры доступа для шин подключения.

Окно Доверенные устройства

Таблица содержит список доверенных устройств. По умолчанию таблица пустая.

Таблица 138. Параметры доверенного устройства

Параметр	Описание
Идентификатор устройства	Идентификатор доверенного устройства.
Название устройства	Название доверенного устройства.
Тип устройства	Тип доверенного устройства (например, Жесткий диск или Устройство чтения смарт-карт).
Имя клиентского устройства	Имя клиентского устройства, к которому подключено доверенное устройство.
Комментарий	Комментарий, относящийся к доверенному устройству.

Доверенные устройства в таблице можно изменять и удалять.

Вы можете добавить устройство в список доверенных устройств по идентификатору устройства (см. раздел "Окно Доверенное устройство (Идентификатор устройства)" на стр. [467](#)) или выбрав нужное устройство в списке устройств, обнаруженных на устройстве пользователя (см. раздел "Окно Доверенное устройство (Список обнаруженных устройств)" на стр. [467](#)).

Вы также можете импортировать список устройств из файла по кнопке **Импортировать** и экспортировать список добавленных устройств в файл по кнопке **Экспортировать**. При импорте вам будет предложено заменить список доверенных устройств или добавить устройства к уже существующему списку.

Окно Доверенное устройство (Идентификатор устройства)

В этом окне вы можете добавить устройство в список доверенных устройств по его идентификатору.

Таблица 139. Добавление устройства по идентификатору

Параметр	Описание
Идентификатор устройства	Поле для ввода идентификатора или маски идентификатора устройства. Вы можете указать идентификатор вручную или скопировать идентификатор нужного устройства из списка Устройства, обнаруженные на клиентских устройствах . Для указания идентификатора вы можете использовать маски * (любая последовательность символов) или ? (один любой символ). Например, вы можете указать маску USBSTOR* для разрешения доступа ко всем USB-накопителям.
Комментарий	Поле ввода комментария (необязательное). Поле доступно после ввода идентификатора устройства и нажатия на кнопку Далее .

Окно Доверенное устройство (Список обнаруженных устройств)

В этом окне вы можете добавить устройство в список доверенных, выбрав его из списка устройств, обнаруженных на управляемых клиентских устройствах.

Информация о существующих устройствах доступна, если существует активная политика и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в свойствах политики Агента администрирования, по умолчанию – каждые 15 минут). При создании новой политики в отсутствие активной политики список будет пустым.

Таблица 140. Добавление устройства из списка

Параметр	Описание
Тип устройства	В раскрывающемся списке вы можете выбрать тип устройств, которые будут отображаться в таблице Устройства, обнаруженные на клиентских устройствах .
Маска идентификатора устройства	Поле для ввода маски идентификатора устройства.
Комментарий	Поле ввода комментария (необязательное). Поле доступно после выбора устройств и нажатия на кнопку Далее .

При нажатии на кнопку **Фильтр** открывается окно, в котором вы можете настроить фильтрацию отображаемой информации об устройствах.

Окно Типы устройств

В этом окне вы можете настроить правила доступа для различных типов устройств.

Таблица 141. Правила доступа для типов устройств

Параметр	Описание
Параметры доступа к устройствам хранения данных	Таблица содержит следующие столбцы: • Тип – тип устройств (например, Жесткие диски, Принтеры). • Режим доступа – режим доступа к устройствам этого типа. Вы можете выбрать один из следующих режимов доступа: • Разрешать – предоставить доступ к устройствам этого типа. • Блокировать – запретить доступ к устройствам этого типа. Для сетевых адаптеров невозможно выбрать режим доступа Блокировать. • Зависит от шины (значение по умолчанию) – разрешить или запретить доступ к устройствам в зависимости от режима доступа для шины (см. раздел "Окно Шины подключения" на стр. 471), используемой для подключения устройства. • По правилам – разрешить или запретить доступ к устройствам в зависимости от правила доступа и расписания (см. раздел "Окно Параметры доступа к устройствам" на стр. 469). Правило доступа и расписание для него можно настроить, выбрав нужный тип устройства.
Параметры доступа к другим устройствам	Таблица содержит следующие столбцы: • Тип – тип устройства (например, Устройства ввода, Звуковые адаптеры). • Режим доступа – режим доступа к устройствам этого типа. Вы можете выбрать один из следующих режимов доступа: • Разрешать – предоставить доступ к устройствам этого типа. • Блокировать – запретить доступ к устройствам этого типа. Для сетевых адаптеров невозможно выбрать режим доступа Блокировать. • Зависит от шины (значение по умолчанию) – разрешить или запретить доступ к устройствам в зависимости от режима доступа для шины (см. раздел "Окно Шины подключения" на стр. 471), используемой для подключения устройства.

Окно Параметры доступа к устройствам

В этом окне вы можете настроить режим доступа и правила доступа для выбранного типа устройств.

Таблица 142. Параметры доступа к устройствам

Параметр	Описание
Режим доступа к устройствам	Режим доступа к устройствам выбранного типа: • Разрешать – разрешать доступ к устройствам выбранного типа. • Блокировать – запрещать доступ к устройствам выбранного типа. • Зависит от шины (значение по умолчанию) – разрешить или запретить доступ к устройствам в зависимости от правила доступа для шины (см. раздел "Окно Шины подключения" на стр. 471), используемой для подключения устройства. • По правилам – разрешить или запретить доступ к устройствам в зависимости от правила доступа и расписания.
Правила доступа к устройствам	Таблица содержит список правил доступа и состоит из следующих столбцов: • Расписание доступа – названия существующих расписаний доступа. • Пользователи и/или группы пользователей – имена пользователей или названия групп пользователей, на которых будет распространяться правило доступа. • Доступ – режим доступа для расписания: • Разрешать (предоставить доступ к устройствам выбранного типа). • Блокировать (запретить доступ к устройствам выбранного типа). • Статус – статус работы правила доступа: • Включено – правило включено, Контроль устройств применяет это правило во время работы. • Выключено – правило выключено и не используется во время работы Контроля устройств. По умолчанию таблица содержит расписание доступа Расписание по умолчанию, которое обеспечивает полный доступ к устройствам для всех пользователей (выбран вариант Все в списке пользователей и групп) в любое время, если для этого типа устройства разрешен доступ по шине подключения (см. раздел "Окно Шины подключения" на стр. 476). Вы можете добавлять, изменять (см. раздел "Окно Правило доступа к устройствам" на стр. 469), а также удалять правила доступа.

Окно Правило доступа к устройствам

В этом окне вы можете настроить правило доступа к устройствам.

Таблица 143. Правило доступа к устройствам

Параметр	Описание
Параметры правила доступа к устройствам	Режим доступа к устройствам выбранного типа: • Разрешать (значение по умолчанию) – разрешать доступ к устройствам выбранного типа. • Блокировать – запрещать доступ к устройствам выбранного типа.
Пользователи и/или группы пользователей	Имя пользователя или название группы пользователей, на которых будет распространяться правило доступа. По умолчанию указано Все (все пользователи). Вы можете добавлять, изменять (см. раздел "Окно Выбор пользователя или группы" на стр. 470), а также удалять пользователей и группы пользователей.
Статус	Статус работы правила доступа: • Включено – правило включено, Контроль устройств применяет это правило во время работы. • Выключено – правило выключено и не используется во время работы Контроля устройств.
Расписание доступа к устройствам	Расписание доступа указанных пользователей к устройствам. По умолчанию указано Расписание по умолчанию. Вы можете указать (см. раздел "Окно Расписания" на стр. 470) другое расписание.

Окно Выбор пользователя или группы

В этом окне вы можете указать локального или доменного пользователя или группу пользователей, для которых вы хотите настроить правило доступа.

Таблица 144. Настройка правила доступа

Параметр	Описание
Вручную	Если выбран этот вариант, в поле ниже вам нужно ввести имя локального или доменного пользователя или название группы пользователей, на которых будет распространяться правило доступа к устройствам.
Список групп или пользователей	Если выбран этот вариант, в поле поиска вы можете ввести критерии поиска имени пользователя или названия группы пользователей, на которых будет распространяться правило доступа к устройствам, или выбрать название группы пользователей в списке ниже.

Окно Расписания

В этом окне вы можете указать расписание для выбранного правила доступа к устройствам.

Вы можете добавлять, изменять (см. раздел "Окно Расписание доступа" на стр. [471](#)), а также удалять расписания доступа.

Расписание по умолчанию удалить невозможно.

Окно Расписание доступа

В этом окне вы можете настроить расписание доступа к устройствам. Расписания можно настраивать только для жестких дисков, съемных дисков, дискет и CD/DVD-приводов.

Если в разделе **Общие параметры** → **Параметры приложения** флажок **Блокировать доступ к файлам во время проверки** снят, то заблокировать доступ к устройствам с помощью расписания доступа невозможно.

Таблица 145. Расписание доступа к устройствам

Параметр	Описание
Название	Поле для ввода названия расписания доступа. Название расписания должно быть уникальным.
Интервалы времени	Таблица, в которой вы можете выбрать интервалы времени для расписания (дни и часы). Интервалы, выделенные зеленым, включены в расписание. Чтобы исключить интервал из расписания, выберите соответствующие ячейки. Исключенные из расписания интервалы выделены серым цветом. По умолчанию в расписание включены все интервалы (24/7).

Окно Шины подключения

В этом окне вы можете настроить режим доступа для шин подключения.

Таблица 146. Режим доступа для шин подключения

Параметр	Описание
Шина подключения	Шина подключения, по которой устройства подключаются к клиентскому устройству: • FireWire • USB
Режим доступа	Переключатель определяет режим доступа к устройствам, использующим эту шину для подключения: • Разрешать (значение по умолчанию) – предоставлять доступ к устройствам, подключенным по этой шине подключения. • Блокировать – запрещать доступ к устройствам, подключенным по этой шине подключения.

Настройка контроля устройств в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры контроля устройств в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Контроль безопасности** → **Контроль устройств**).

Таблица 147. Параметры компонента Контроль устройств

Параметр	Описание
Включить Контроль устройств	Флажок включает или выключает компонент Контроль устройств. По умолчанию флажок снят.
Доверенные устройства	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Доверенные устройства (см. раздел "Окно Доверенные устройства" на стр. 472). В этом окне вы можете добавить устройство в список доверенных устройств по его идентификатору (см. раздел "Окно Доверенное устройство" на стр. 473) или выбрав его в списке устройств, обнаруженных на клиентских устройствах (см. раздел "Окно Устройства на клиентских устройствах" на стр. 473).
Режим работы Контроля устройств	Режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств: • Информировать (значение по умолчанию). При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes тестирует выбранный режим доступа и формирует событие об обнаружении попытки доступа к устройству. • Блокировать. При выборе этого варианта приложение Kaspersky Industrial CyberSecurity for Linux Nodes применяет режим доступа, заданный для устройства или шины.
Параметры Контроля устройств	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить режим доступа к устройствам в зависимости от их типа (см. раздел "Окно Тип устройства" на стр. 474) и режим доступа для шин подключения (см. раздел "Окно Шины подключения" на стр. 476).

Окно Доверенные устройства

Таблица содержит список доверенных устройств. По умолчанию таблица пустая.

Таблица 148. Параметры доверенного устройства

Параметр	Описание
Идентификатор устройства	Идентификатор доверенного устройства.
Имя устройства	Имя доверенного устройства.
Тип устройства	Тип доверенного устройства (например, Жесткий диск или Устройство чтения смарт-карт).
Имя клиентского устройства	Имя клиентского устройства, к которому подключено доверенное устройство.
Комментарий	Комментарий, относящийся к доверенному устройству.

Доверенные устройства в таблице можно изменять и удалять.

Вы можете добавить устройство в список доверенных устройств по идентификатору или маске (см. раздел "Окно Доверенное устройство" на стр. [473](#)) или выбрав нужное устройство в списке устройств, обнаруженных на устройстве пользователя (см. раздел "Окно Устройства на клиентских устройствах" на стр. [473](#)).

Вы также можете импортировать список устройств из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных устройств в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**. При импорте вам будет предложено заменить список доверенных устройств или добавить устройства к уже существующему списку.

Окно Доверенное устройство

В этом окне вы можете добавить устройство в список доверенных устройств по его идентификатору.

Таблица 149. Добавление устройства по идентификатору

Параметр	Описание
Идентификатор устройства	Поле для ввода идентификатора или маски идентификатора устройства, которое вы хотите добавить в список доверенных устройств. Для указания идентификатора вы можете использовать маски * (любая последовательность символов) или ? (один любой символ). Например, вы можете указать маску USBSTOR* для разрешения доступа ко всем USB-накопителям.
Найти на устройствах	По нажатию на кнопку отображаются устройства, найденные по указанному идентификатору или маске на подключенных клиентских устройствах. Кнопка доступна, если поле Идентификатор устройства не пустое.
Найденные устройства	Таблица содержит следующие столбцы: • Тип устройства – тип найденного устройства (например, Жесткий диск или Устройство чтения смарт-карт). • Идентификатор устройства – идентификатор найденного устройства. • Имя устройства – имя найденного устройства. • Имя клиентского устройства – имя клиентского устройства, к которому подключено найденное устройство.
Комментарий	Поле ввода комментария к устройству, которое вы хотите добавить в список доверенных устройств (необязательное).

Окно Устройства на клиентских устройствах

В этом окне вы можете добавить устройство в список доверенных, выбрав его из списка устройств, обнаруженных на клиентских устройствах.

Информация о существующих устройствах доступна, если существует активная политика и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в политике Агента администрирования, по умолчанию – каждые 15 минут). При создании новой политики в отсутствие активной политики список будет пустым.

Таблица 150. Добавление устройства из списка

Параметр	Описание
Имя клиентского устройства	Поле ввода имени или маски имени управляемого устройства, для которого вы хотите найти подключенные устройства. По умолчанию указана маска * – все управляемые устройства.
Тип устройства	В раскрывающемся списке вы можете выбрать тип подключенного устройства для поиска (например, Жесткие диски или Устройства чтения смарт-карт). По умолчанию выбран элемент Все устройства .
Идентификатор устройства	Поле для ввода идентификатора или маски идентификатора устройства, которое вы хотите найти. По умолчанию указана маска * – все устройства.
Поиск на устройствах	По нажатию на кнопку приложение выполняет поиск устройства с указанными параметрами. Результаты поиска отображаются в таблице ниже.

Окно Тип устройства

В этом окне вы можете настроить режим доступа для различных типов устройств.

Таблица 151. Режим доступа для типов устройств

Параметр	Описание
Тип устройства	Тип устройства (например, Жесткие диски, Принтеры).
Режим доступа	Режим доступа к устройству. При нажатии на правую кнопку мыши открывается контекстное меню, в котором вы можете выбрать один из следующих элементов: • Разрешать – разрешать доступ к устройствам выбранного типа. • Блокировать – запрещать доступ к устройствам выбранного типа. • Зависит от шины (значение по умолчанию) – разрешить или запретить доступ к устройствам в зависимости от режима доступа для шины подключения (см. раздел "Окно Шины подключения" на стр. 471). • По правилам – разрешить или запретить доступ к устройствам в зависимости от правила доступа (см. раздел "Окно Настройка правила доступа к устройствам" на стр. 474) и расписания.

Вы можете настроить правила доступа и расписания доступа в окне **Настройка правила доступа к устройствам** (см. раздел "Окно Настройка правила доступа к устройствам" на стр. [474](#)), которое открывается двойным щелчком мыши по названию типа устройства.

Окно Настройка правила доступа к устройствам

В этом окне вы можете настроить правила доступа и расписания для выбранного типа устройств.

Окно открывается по двойному щелчку на названии типа устройства в окне **Тип устройства** (см. раздел "Окно Тип устройства" на стр. [474](#)).

Таблица 152. Правила доступа и расписания для устройств

Параметр	Описание
Пользователи и/или группы пользователей	Список пользователей и групп, для которых можно настроить расписание доступа. По умолчанию таблица содержит элемент Все (все пользователи). Вы можете добавлять, изменять и удалять пользователей и группы пользователей.
Правила для выделенной группы пользователей по расписаниям доступа	Таблица содержит расписания доступа для пользователей и групп и состоит из следующих столбцов: • Расписание доступа – названия существующих расписаний доступа. Флажок рядом с расписанием показывает, используется ли это расписание в работе компонента. • Доступ – тип доступа для расписания: Разрешать (предоставить доступ к устройствам выбранного типа) или Блокировать (запретить доступ к устройствам выбранного типа). Расписания можно настраивать только для жестких дисков, съемных дисков, дискет и CD/DVD-приводов. По умолчанию таблица содержит расписание доступа По умолчанию, которое обеспечивает полный доступ к устройствам для всех пользователей (выбран элемент Все в списке Пользователи и/или группы пользователей) в любое время, если для этого типа устройства разрешен доступ по шине подключения (см. раздел "Окно Шины подключения" на стр. 476). Вы можете добавлять, изменять и удалять расписания доступа для выбранных пользователей. Расписание По умолчанию невозможно изменить или удалить.

Окно Пользователь или группа

В этом окне вы можете указать пользователя или группу пользователей, на которых распространяется правило доступа к устройствам.

Таблица 153. Настройка правила доступа к устройствам

Параметр	Описание
Тип	Пользователь или Группа , на которых распространяется правило.
Имя пользователя или группы	Имя пользователя или название группы пользователей, на которых распространяется правило.

Окно Расписание доступа

В этом окне вы можете настроить расписание доступа к устройствам.

Таблица 154. Расписание доступа к устройствам

Параметр	Описание
Название	Поле для ввода названия расписания доступа.
Интервалы времени	Таблица, в которой вы можете выбрать интервалы времени для расписания (дни и часы). Интервалы, выделенные зеленым, включены в расписание. Чтобы исключить интервал из расписания, выберите соответствующие ячейки. Исключенные из расписания интервалы выделены серым цветом. По умолчанию в расписание включены все интервалы (24/7).

Окно Шины подключения

В этом окне вы можете настроить режим доступа для шин подключения.

Таблица 155. Режим доступа для шин подключения

Параметр	Описание
Шина подключения	Шина подключения, по которой устройства подключаются к клиентскому устройству: • FireWire • USB
Режим доступа	Режим доступа для шины подключения. При нажатии на правую кнопку мыши открывается контекстное меню, в котором вы можете выбрать один из следующих элементов: • Разрешать (значение по умолчанию) – предоставлять доступ к устройствам, подключенным по этой шине подключения. • Блокировать – запрещать доступ к устройствам, подключенным по этой шине подключения.

Настройка Контроля устройств в командной строке

В командной строке вы можете управлять контролем устройств с помощью предустановленной задачи Контроль устройств (*Device_Control*).

Задача Контроль устройств по умолчанию не запущена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачу вручную.

Вы можете настраивать параметры (см. раздел "Параметры задачи Контроль устройств" на стр. [477](#)) контроля устройств, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи Контроль устройств.

Вы также можете просматривать список подключенных устройств (см. раздел "Просмотр списка подключенных устройств в командной строке" на стр. [488](#)) с помощью команд управления Контролем устройств.

В этом разделе

Параметры задачи Контроль устройств	477
Просмотр списка подключенных устройств в командной строке	488

Параметры задачи Контроль устройств

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Контроль устройств.

Таблица 156. Параметры задачи Контроль устройств

Параметр	Описание	Значения
OperationMode	Режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств.	Block – приложение применяет режим доступа, заданный для устройства или шины. Notify (значение по умолчанию) – приложение тестирует выбранный режим доступа и формирует событие об обнаружении попытки доступа к устройству.
Секция [DeviceClass] содержит режимы доступа к устройствам в зависимости от их типа.		
HardDrive	Режим доступа к жестким дискам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к жестким дискам. DependsOnBus (значение по умолчанию) – доступ к жесткому диску зависит от режима доступа для шины подключения, по которой подключен диск. Block – пользователям запрещен доступ ко всем жестким дискам (за исключением системных жестких дисков, которые Контроль устройств не блокирует). ByRule – доступ к жестким дискам зависит от правил доступа.
RemovableDrive	Режим доступа к съемным дискам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к съемным дискам. DependsOnBus (значение по умолчанию) – доступ к съемному диску зависит от режима доступа для шины подключения, по которой подключен диск. Block – пользователям запрещен доступ к съемным дискам. ByRule – доступ к съемным дискам зависит от правил доступа.
FloppyDrive	Режим доступа к дискетам, подключенным к клиентскому устройству. Приложение не блокирует дискеты, подключенные к клиентскому устройству с помощью шины ISA.	Allow – пользователям разрешен доступ к дискетам. DependsOnBus (значение по умолчанию) – доступ к дискете зависит от режима доступа для шины подключения, по которой подключена дискета. Block – пользователям запрещен доступ к дискетам. ByRule – доступ к дискетам зависит от правил доступа.

Параметр	Описание	Значения
OpticalDrive	Режим доступа к CD/DVD-приводам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к CD/DVD-приводам. DependsOnBus (значение по умолчанию) – доступ к CD/DVD-приводу зависит от режима доступа для шины подключения, по которой подключен CD/DVD-привод. Block – пользователям запрещен доступ к CD/DVD-приводам. ByRule – доступ к CD/DVD-приводам зависит от правил доступа.
SerialPortDevice	Режим доступа к устройствам, подключенным к клиентскому устройству через последовательный порт. Приложение не блокирует устройства, подключенные к клиентскому устройству через последовательный порт с помощью шины ISA.	Allow – пользователям разрешен доступ к устройствам, подключенным через последовательный порт. DependsOnBus (значение по умолчанию) – доступ к устройству, подключенному через последовательный порт, зависит от режима доступа для шины подключения. Block – пользователям запрещен доступ к устройствам, подключенным через последовательный порт.
ParallelPortDevice	Режим доступа к устройствам, подключенным к клиентскому устройству через параллельный порт.	Allow – пользователям разрешен доступ к устройствам, подключенным через параллельный порт. DependsOnBus (значение по умолчанию) – доступ к устройству, подключенному через параллельный порт, зависит от режима доступа для шины подключения. Block – пользователям запрещен доступ к устройствам, подключенным через параллельный порт.
Printer	Режим доступа к принтерам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к принтерам. DependsOnBus (значение по умолчанию) – доступ к принтеру зависит от режима доступа для шины подключения, по которой подключен принтер. Block – пользователям запрещен доступ к принтерам.

Параметр	Описание	Значения
Modem	Режим доступа к модемам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к модемам. DependsOnBus (значение по умолчанию) – доступ к модему зависит от режима доступа для шины подключения, по которой подключен модем. Block – пользователям запрещен доступ к модемам.
TapeDrive	Режим доступа к стримерам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к стримерам. DependsOnBus (значение по умолчанию) – доступ к стримеру зависит от режима доступа для шины подключения, по которой подключен стример. Block – пользователям запрещен доступ к стримерам.
MultifuncDevice	Режим доступа к multifunctional устройствам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к multifunctional устройствам. DependsOnBus (значение по умолчанию) – доступ к multifunctional устройству зависит от режима доступа для шины подключения, по которой подключено устройство. Block – пользователям запрещен доступ к multifunctional устройствам.
SmartCardReader	Режим доступа к устройствам чтения смарт-карт, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к устройствам чтения смарт-карт. DependsOnBus (значение по умолчанию) – доступ к устройству чтения смарт-карт зависит от режима доступа для шины подключения, по которой подключено устройство. Block – пользователям запрещен доступ к устройствам чтения смарт-карт.
WiFiAdapter	Режим доступа к Wi-Fi-адаптерам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к Wi-Fi-адаптерам. DependsOnBus (значение по умолчанию) – доступ к Wi-Fi-адаптеру зависит от режима доступа для шины подключения. Block – пользователям запрещен доступ к Wi-Fi-адаптерам.

Параметр	Описание	Значения
NetworkAdapter	Режим доступа к внешним сетевым адаптерам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к внешним сетевым адаптерам. DependsOnBus (значение по умолчанию) – доступ к внешнему сетевому адаптеру зависит от режима доступа для шины подключения, по которой подключен адаптер. Контроль устройств не позволяет запрещать доступ к внешним сетевым адаптерам, чтобы избежать отключения клиентского устройства от сети.
PortableDevice	Режим доступа к портативным устройствам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к портативным устройствам. DependsOnBus (значение по умолчанию) – доступ к портативному устройству зависит от режима доступа для шины подключения, по которой подключено устройство. Block – пользователям запрещен доступ к портативным устройствам.
BluetoothDevice	Режим доступа к Bluetooth-устройствам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к Bluetooth-устройствам. DependsOnBus (значение по умолчанию) – доступ к Bluetooth-устройству зависит от режима доступа для шины подключения, по которой подключено устройство. Block – пользователям запрещен доступ к Bluetooth-устройствам.
ImagingDevice	Режим доступа к устройствам обработки изображений, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к устройствам обработки изображений. DependsOnBus (значение по умолчанию) – доступ к устройству обработки изображений зависит от режима доступа для шины подключения, по которой подключено устройство. Block – пользователям запрещен доступ к устройствам обработки изображений.
SoundAdapter	Режим доступа к звуковым адаптерам, подключенным к клиентскому устройству.	Allow – пользователям разрешен доступ к звуковым адаптерам. DependsOnBus (значение по умолчанию) – доступ к звуковому адаптеру зависит от режима доступа для шины подключения, по которой подключено устройство. Block – пользователям запрещен доступ к звуковым адаптерам.

Параметр	Описание	Значения
InputDevice	Режим доступа к устройствам ввода, подключенным к клиентскому устройству (клавиатура, мышь, тачпад и другие).	Allow – пользователям разрешен доступ к устройствам ввода. DependsOnBus (значение по умолчанию) – доступ к устройству ввода зависит от режима доступа для шины подключения, по которой подключено устройство. Block – пользователям запрещен доступ к устройствам ввода.
Секция [DeviceBus] содержит режимы доступа для шин подключения.		
USB	Режим доступа для устройств, подключенных к клиентскому устройству через USB-интерфейс.	Allow (значение по умолчанию) – пользователям разрешен доступ к USB-устройствам. Block – пользователям запрещен доступ к USB-устройствам.
FireWire	Режим доступа для устройств, подключенных к клиентскому устройству через интерфейс FireWire.	Allow (значение по умолчанию) – пользователям разрешен доступ к устройствам, подключенным через интерфейс FireWire. Block – пользователям запрещен доступ к устройствам, подключенным через интерфейс FireWire.
Секция [TrustedDevices.item_#] содержит доверенные устройства (см. раздел "Контроль устройств" на стр. 464).		
DeviceId	Идентификатор или маска идентификатора доверенного устройства.	Вы можете использовать маски * (любая последовательность символов) или ? (один любой символ), чтобы указать идентификатор устройства. Примеры: ► Чтобы запретить доступ ко всем USB-устройствам, кроме указанного, укажите следующие параметры: В секции [DeviceBus] параметр USB=Block В секции [TrustedDevices.item_#] параметр DeviceId=<идентификатор устройства> ► Чтобы запретить доступ ко всем USB-устройствам, но разрешить доступ ко всем USB-накопителям, укажите следующие параметры: В секции [DeviceBus] параметр USB=Block В секции [TrustedDevices.item_#] параметр DeviceId=USBSTOR*

Параметр	Описание	Значения
Comment	Комментарий к указанному доверенному устройству.	—
Секция [Schedules.item_#] содержит расписание доступа для устройств. Вы можете настраивать расписание только для жестких дисков, съемных дисков, дискет и CD/DVD-приводов.		
ScheduleName	Название расписания. Название расписания должно быть уникальным.	Значение по умолчанию: <code>Default</code> . Расписание <code>Default</code> обеспечивает полный доступ к устройствам для всех пользователей в любое время, если для соответствующего типа устройства разрешен доступ по шине подключения. Расписание <code>Default</code> удалить нельзя.

Параметр	Описание	Значения
DaysHours	Интервалы времени для расписания.	All (значение по умолчанию) – расписание действует 24/7 (без ограничений по времени). <день недели> – дни недели. Вы можете использовать как полные названия дней недели, так и аббревиатуры (например, для понедельника можно указать Mo, Mon или Monday). Для дней недели можно указывать либо интервалы, либо конкретные дни. Неделя начинается с воскресенья. <час> – часы [0:24]. Для часов вы можете указывать только интервалы. Примеры: Расписание schedule_1, действующее с воскресенья по субботу с 0 до 11, с 12 до 15 и с 16 до 24: <pre>[Schedules.item_0001] ScheduleName=schedule_1 DaysHours=Su-Sa:0..11,12..15,16..24</pre> Расписание schedule_2, действующее по четвергам с 12 до 14 и по пятницам с 2 до 15 и с 16 до 24: <pre>[Schedules.item_0002] ScheduleName=schedule_2 DaysHours=Th:12..14;Fr:2..15,16..24</pre> Расписание schedule_3, действующее 24 часа 7 дней в неделю: <pre>[Schedules.item_0003] ScheduleName=schedule_3 DaysHours=All</pre>

Секция [HardDrivePrincipals.item_#] содержит правила доступа к жестким дискам.

Для жестких дисков должно быть включено хотя бы одно расписание. Вы можете назначить несколько правил доступа к жесткому диску. Также для пользователя или группы пользователей можно указать несколько расписаний. Если возникает конфликт правила доступа для пользователя или группы, предоставляются минимальные права доступа.

Параметр	Описание	Значения
Principal	Пользователь или группа пользователей, к которым применяется правило доступа.	\Everyone (значение по умолчанию) – правило доступа применяется для всех пользователей. <имя пользователя> – имя пользователя, для которого применяется правило доступа. @<название группы> – название группы пользователей, для которых применяется правило доступа.
[HardDrivePrincipals.item_#.AccessRules.item_#]	Параметры правил доступа.	—
UseRule	Показывает, включено или выключено правило.	Yes (значение по умолчанию) – правило доступа включено. No – правило доступа выключено.
ScheduleName	Расписание, указанное в секции [Schedules.item_#].	Значение по умолчанию: Default.
Access	Тип доступа.	Allow (значение по умолчанию) – доступ к жестким дискам разрешен. Block – доступ к жестким дискам запрещен.
Секция [RemovableDrivePrincipals.item_#] содержит правила доступа к съемным дискам. Для съемных дисков должно быть включено хотя бы одно расписание. Вы можете назначить несколько правил доступа к съемному диску. Также для пользователя или группы пользователей можно указать несколько расписаний. Если возникает конфликт правила доступа для пользователя или группы, предоставляются минимальные права доступа.		
Principal	Пользователь или группа пользователей, к которым применяется правило доступа.	\Everyone (значение по умолчанию) – правило доступа применяется для всех пользователей. <имя пользователя> – имя пользователя, для которого применяется правило доступа. @<название группы> – название группы пользователей, для которых применяется правило доступа.
[RemovableDrivePrincipals.item_#.AccessRules.item_#]	Параметры правил доступа.	—
UseRule	Показывает, включено или выключено правило.	Yes (значение по умолчанию) – правило доступа включено. No – правило доступа выключено.
ScheduleName	Расписание, указанное в секции [Schedules.item_#].	Значение по умолчанию: Default.

Параметр	Описание	Значения
Access	Тип доступа.	Allow (значение по умолчанию) – доступ к съемным дискам разрешен. Block – доступ к съемным дискам запрещен.
Секция [FloppyDrivePrincipals.item_#] содержит правила доступа к дискетам. Для дискет должно быть включено хотя бы одно расписание. Вы можете назначить несколько правил доступа к дискете. Также для пользователя или группы пользователей можно указать несколько расписаний. Если возникает конфликт правила доступа для пользователя или группы, предоставляются минимальные права доступа.		
Principal	Пользователь или группа пользователей, к которым применяется правило доступа.	\Everyone (значение по умолчанию) – правило доступа применяется для всех пользователей. <имя пользователя> – имя пользователя, для которого применяется правило доступа. @<название группы> – название группы пользователей, для которых применяется правило доступа.
[FloppyDrivePrincipals.item_#.AccessRules.item_#]	Параметры правил доступа.	—
UseRule	Показывает, включено или выключено правило.	Yes (значение по умолчанию) – правило доступа включено. No – правило доступа выключено.
ScheduleName	Расписание, указанное в секции [Schedules.item_#].	Значение по умолчанию: Default.
Access	Тип доступа.	Allow (значение по умолчанию) – доступ к дискетам разрешен. Block – доступ к дискетам запрещен.
Секция [OpticalDrivePrincipals.item_#] содержит правила доступа к CD/DVD-приводам. Для CD/DVD-приводов должно быть включено хотя бы одно расписание. Вы можете назначить несколько правил доступа к CD/DVD-приводу. Также для пользователя или группы пользователей можно указать несколько расписаний. Если возникает конфликт правила доступа для пользователя или группы, предоставляются минимальные права доступа.		
Principal	Пользователь или группа пользователей, к которым применяется правило доступа.	\Everyone (значение по умолчанию) – правило доступа применяется для всех пользователей. <имя пользователя> – имя пользователя, для которого применяется правило доступа. @<название группы> – название группы пользователей, для которых применяется правило доступа.
[OpticalDrivePrincipals.item_#.AccessRules.item_#]	Параметры правил доступа.	—

Параметр	Описание	Значения
UseRule	Показывает, включено или выключено правило.	Yes (значение по умолчанию) – правило доступа включено. No – правило доступа выключено.
ScheduleName	Расписание, указанное в секции [Schedules.item_#].	Значение по умолчанию: Default.
Access	Тип доступа.	Allow (значение по умолчанию) – доступ к CD/DVD-приводам разрешен. Block – доступ к CD/DVD-приводам запрещен.

Просмотр списка подключенных устройств в командной строке

Только пользователи с ролями **admin** и **audit** могут просматривать список подключенных устройств.

► Чтобы просмотреть список подключенных устройств, выполните следующую команду:

```
kics-control [-D] --get-device-list
```

Kaspersky Industrial CyberSecurity for Linux Nodes отобразит следующую информацию о подключенных устройствах:

- **Тип устройства.** Тип подключенного устройства. Например, `OpticalDrive` или `HardDrive`.
- **Идентификатор.** Идентификатор подключенного устройства.
- **Название.** Название подключенного устройства.
- **Путь.** Путь к устройству в виртуальной операционной системе `sysfs`.
- **Системный диск.** Параметр показывает, является ли подключенное устройство системным диском (да или нет).
- **Шина.** Шина подключения. Возможные значения: `UnknownBus`, `USB`, `FireWire`.
- **Драйвер.** Название используемого драйвера, читаемое виртуальной операционной системой `sysfs`.

Веб-Контроль

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, приложение Kaspersky Industrial CyberSecurity for Linux Nodes блокирует доступ или показывает сообщение-предупреждение о том, что веб-сайт не рекомендован для посещения.

Kaspersky Industrial CyberSecurity for Linux Nodes контролирует только HTTP- и HTTPS-трафик.

Веб-Контроль позволяет настраивать доступ к веб-сайтам следующими способами:

- По категориям содержания.
Категоризацию содержания веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз приложения). Вы можете ограничить доступ пользователей, например, к категории содержания "Социальные сети" или другим категориям (<https://support.kaspersky.com/Legal/WebCategories/ru-RU/206917.htm>).
- По категориям типов данных. Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Приложение определяет тип данных по формату файла, а не по расширению.

Приложение не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, приложение определит тип данных "Архивы", а не "Графические файлы".

- По веб-адресу. Вы можете указать веб-адрес или маску веб-адреса (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. [514](#)).

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к категории типов данных "Файлы офисных приложений" только для категории содержания "Веб-почта".

По умолчанию для всех веб-ресурсов выбрано *правило по умолчанию Разрешать*. В соответствии с этим правилом Веб-Контроль разрешает пользователям доступ к веб-ресурсам, если не заданы другие *правила доступа к веб-ресурсам* (см. раздел "О правилах доступа к веб-ресурсам" на стр. [490](#)).

Вы можете изменить для Веб-Контроля правило по умолчанию, согласно которому приложение будет регулировать доступ к веб-ресурсам, которые не попадают под действие других правил, и задать *правило по умолчанию Блокировать*. В соответствии с этим правилом Веб-Контроль запрещает пользователям доступ к веб-ресурсам, если не заданы другие *правила доступа к веб-ресурсам* (см. раздел "О правилах доступа к веб-ресурсам" на стр. [490](#)).

В этом разделе

О правилах доступа к веб-ресурсам	490
Настройка Веб-Контроля в Web Console	491
Настройка Веб-Контроля в Консоли администрирования	498
Настройка шаблонов сообщений Веб-Контроля.....	506
Настройка Веб-Контроля в командной строке	508
Правила формирования масок адресов веб-ресурсов	514

О правилах доступа к веб-ресурсам

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое приложение выполняет при посещении пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют задать веб-ресурсы, доступ к которым контролирует компонент Веб-Контроль.

Доступны следующие фильтры:

- **Фильтр по категориям содержания.** Веб-Контроль может распределять веб-ресурсы по категориям содержания (<https://support.kaspersky.com/Legal/WebCategories/ru-RU/206917.htm>). Вы можете контролировать доступ пользователей к веб-ресурсам, имеющим определенное этими категориями содержание. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории содержания, приложение выполняет действие, указанное в правиле.
- **Фильтр по категориям типов данных.** Веб-Контроль может распределять веб-ресурсы по категориям типов данных. Вы можете контролировать доступ пользователей к размещенным на веб-ресурсах данным, относящимся к определенным типам данных. При посещении пользователем веб-ресурсов, которые относятся к выбранной категории типов данных, приложение 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 категориям содержания и/или по категориям типов данных, и фильтр по адресам веб-ресурсов, и заданные адреса веб-ресурсов и/или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типов данных, приложение контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и/или категорий типов 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. Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.
- **Расписание работы правила.** Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда приложение контролирует доступ к веб-ресурсам, указанным в правиле. Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Для каждого правила вы можете задать действие, которое Веб-Контроль выполняет при посещении пользователем веб-ресурса, удовлетворяющего параметрам правила:

- **Разрешать.** Веб-Контроль разрешает доступ пользователя к веб-ресурсу.
- **Блокировать.** Веб-Контроль запрещает доступ пользователя к веб-ресурсу и выводит сообщение о запрете доступа. По ссылкам из сообщения о блокировке пользователь может отправить сообщение-жалобу администратору локальной сети организации об ошибочной блокировке и получить доступ к запрошенному веб-ресурсу.
- **Информировать.** Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может отправить сообщение-жалобу администратору локальной сети организации об ошибочном предупреждении. При этом доступ пользователя к веб-ресурсу не блокируется.

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 этому веб-сайту по правилу с высшим приоритетом. Например, приложение 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 содержания "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.

Если не создано ни одного запрещающего правила, расшифровка HTTPS-трафика не выполняется.

Настройка Веб-Контроля в Web Console

В Web Console вы можете настраивать параметры Веб-Контроля в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения → Контроль безопасности → Веб-Контроль**).

Таблица 157. Параметры компонента Веб-Контроль

Параметр	Описание
Веб-Контроль включен / выключен	Переключатель включает или выключает компонент Веб-Контроль. По умолчанию переключатель выключен.
Список правил	Таблица содержит список правил доступа к веб-ресурсам. В процессе работы Веб-Контроль применяет правила в том порядке, в котором они указаны в таблице. Таблица содержит следующие столбцы: • Название правила. Название правила доступа к веб-ресурсам. • Статус. Статус работы правила доступа к веб-ресурсам: • <i>Включено</i> – правило включено, Веб-Контроль применяет это правило во время работы. • <i>Выключено</i> – правило выключено и не используется во время работы Веб-Контроля. Вы можете включить или выключить переключатель в таблице, а также установить или снять флажок Использовать это правило в окне Правило Веб-Контроля (см. раздел "Окно Правило Веб-Контроля" на стр. 494). • Действие. Действие, которое приложение будет выполнять при обнаружении попытки доступа к веб-ресурсам, удовлетворяющим правилу. Элементы в таблице можно добавлять, изменять (см. раздел "Окно Правило Веб-Контроля" на стр. 494), удалять, перемещать вверх и вниз. Вы также можете импортировать список правил из файла по кнопке Импортировать и экспортировать список добавленных правил в файл по кнопке Экспортировать. При импорте вам будет предложено заменить список правил или добавить правила к уже существующему списку.
Правило по умолчанию	Вы можете выбрать правило по умолчанию, согласно которому приложение будет регулировать доступ к веб-ресурсам, которые не попадают под действие других правил: • Разрешать все, что не указано в списке правил (значение по умолчанию) – разрешать доступ к веб-ресурсам. • Блокировать все, что не указано в списке правил – блокировать доступ к веб-ресурсам.
Шаблоны	Предупреждение. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекommenдованному веб-ресурсу. Сообщение о блокировке. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу. Сообщение администратору. Поле ввода содержит шаблон сообщения-жалобы для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ приложение Kaspersky Industrial CyberSecurity for Linux Nodes отправляет в Kaspersky Security Center событие <i>Сообщение администратору о запрете доступа к веб-странице</i>. Описание события содержит сообщение администратору с подставленными переменными. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

Параметр	Описание

В этом разделе

Окно Правило Веб-Контроля	494
Окно Группы адресов	497
Окно Группа.....	497
Окно Выбор пользователя или группы	497
Окно Расписания	498
Окно Расписание доступа	498

Окно Правило Веб-Контроля

В этом окне вы можете настроить параметры правила доступа к веб-ресурсам.

Таблица 158. Добавление правила доступа к веб-ресурсам

Параметр	Описание
Название правила	Поле ввода названия правила доступа к веб-ресурсам.
Статус	Вы можете выбрать статус работы правила доступа к веб-ресурсам: <i>Включено</i> – правило включено, Веб-Контроль применяет это правило во время работы. <i>Выключено</i> – правило выключено и не используется во время работы Веб-Контроля.
Действие	Вы можете выбрать действие, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсу, удовлетворяющему правилу: Разрешать (значение по умолчанию) – разрешать доступ к веб-ресурсу. Блокировать – блокировать доступ к веб-ресурсу и выводить сообщение о запрете доступа. Информировать – выводить предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
Фильтровать по категориям содержания	Флажок включает или выключает использование фильтра по категориям содержания. Если флажок установлен, доступна ссылка Категории содержания , по нажатию на которую открывается окно, в котором вы можете выбрать нужные категории содержания. По умолчанию флажок снят.
Фильтровать по категориям типов данных	Флажок включает или выключает использование фильтра по категориям содержания. Если флажок установлен, доступна ссылка Категории типов данных , по нажатию на которую открывается окно, в котором вы можете выбрать нужные категории типов данных. По умолчанию флажок снят.
Адреса	Вы можете выбрать использование фильтра адресов веб-ресурса: Применять ко всем адресам (значение по умолчанию). При выборе этого варианта фильтр адресов веб-ресурсов не используется, правило Веб-Контроля применяется ко всем адресам веб-ресурсов. Применять к указанным адресам и/или группам. При выборе этого варианта становятся доступны таблица адресов веб-ресурсов, на которые распространяется правило, и кнопки Добавить адрес, по нажатию на которую открывается окно, в котором вы можете добавить нужный адрес веб-ресурса, и Добавить группу, по нажатию на которую открывается окно Группы адресов (см. раздел "Окно Группы адресов" на стр. 497), в котором вы можете добавить группы адресов веб-ресурсов.
Пользователи	Вы можете выбрать использование фильтра пользователей, на которых распространяется правило доступа к веб-ресурсам: Применять ко всем пользователям (значение по умолчанию). При выборе этого варианта фильтр пользователей не используется, правило Веб-Контроля применяется ко всем пользователям. Применять к указанным пользователям и/или группам. При выборе этого варианта становятся доступны таблица пользователей и групп пользователей, на которые распространяется правило, и кнопка Добавить, по нажатию на которую открывается окно Выбор пользователя или группы, в котором вы можете добавить нужных пользователей и/или группы пользователей.

Параметр	Описание
Расписание работы правила	Расписание работы правила Веб-Контроля. По умолчанию указано расписание Всегда . По ссылке Всегда открывается окно Расписания , в котором вы можете настроить другое расписание работы правила.

Окно Группы адресов

Таблица содержит группы адресов веб-ресурсов, доступ пользователей к которым контролирует компонент Веб-Контроль. По умолчанию таблица пустая.

Таблица 159. Настройка правила доступа к веб-ресурсам

Параметр	Описание
Название группы	Название группы адресов веб-ресурсов, на которые распространяется правило.
Количество адресов в группе	Количество адресов в группе адресов.

Элементы в таблице можно добавлять, изменять и удалять.

Если вы хотите добавить новую группу адресов в список групп в этом окне, откройте окно **Группа** (см. раздел "Окно Группа" на стр. [497](#)), нажав на кнопку **Добавить**, расположенную над таблицей.

Если вы хотите добавить группу адресов в список групп в окне **Правило Веб-Контроля** (см. раздел "Окно Правило Веб-Контроля" на стр. [494](#)), установите флажок около названия группы в таблице и нажмите на кнопку **Добавить группы в правило**, расположенную под таблицей.

Окно Группа

В этом окне вы можете добавить группу адресов веб-ресурсов.

Таблица 160. Настройка правила доступа к веб-ресурсам

Параметр	Описание
Название группы	Название новой группы адресов веб-ресурсов.
Адреса	Таблица адресов, входящих в группу адресов веб-ресурсов.

Элементы в таблице можно добавлять, изменять, и удалять.

Окно Выбор пользователя или группы

В этом окне вы можете указать локального или доменного пользователя или группу пользователей, для которых вы хотите настроить правило доступа к веб-ресурсам.

Таблица 161. Настройка правила доступа к веб-ресурсам

Параметр	Описание
Вручную	Если выбран этот вариант, в поле ниже вам нужно ввести имя локального или доменного пользователя или название группы пользователей, на которых будет распространяться правило доступа к веб-ресурсам.
Список групп или пользователей	Если выбран этот вариант, в поле поиска вы можете ввести критерии поиска имени пользователя или названия группы пользователей, на которых будет распространяться правило доступа к веб-ресурсам, или выбрать название группы пользователей в списке ниже.

Окно Расписания

В этом окне вы можете указать расписание для выбранного правила доступа к устройствам.

Вы можете добавлять, изменять (см. раздел "Окно Расписание доступа" на стр. [498](#)), а также удалять расписания доступа. Расписание по умолчанию **Всегда** невозможно удалить или изменить.

Окно Расписание доступа

В этом окне вы можете настроить расписание доступа к веб-ресурсам.

Таблица 162. Расписание доступа к веб-ресурсам

Параметр	Описание
Название	Поле для ввода названия расписания доступа. Название расписания должно быть уникальным.
Интервалы времени	Таблица, в которой вы можете выбрать интервалы времени для расписания (дни и часы). Интервалы, выделенные зеленым, включены в расписание. Чтобы исключить интервал из расписания, выберите соответствующие ячейки. Исключенные из расписания интервалы выделены серым цветом. По умолчанию в расписание включены все интервалы (24/7).

Настройка Веб-Контроля в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры Веб-Контроля в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Контроль безопасности** → **Веб-Контроль**).

Таблица 163. Параметры компонента Веб-Контроль

Параметр	Описание
Включить Веб-Контроль	Флажок включает компонент Веб-Контроль. По умолчанию флажок снят.
Параметры Веб-Контроля	Таблица содержит список правил доступа к веб-ресурсам. В процессе работы Веб-Контроль применяет правила в том порядке, в котором они указаны в таблице. Таблица содержит следующие столбцы: • Статус. Статус работы правила доступа к веб-ресурсам: • <i>Включено</i> – правило включено, Веб-Контроль применяет это правило во время работы. • <i>Выключено</i> – правило выключено и не используется во время работы Веб-Контроля. Вы можете установить или снять флажок в таблице, а также установить или снять флажок Использовать это правило в окне Правило Веб-Контроля (см. раздел "Окно Правило Веб-Контроля" на стр. 501). • Действие. Действие, которое приложение будет выполнять при обнаружении попытки доступа к веб-ресурсам, удовлетворяющим правилу. • Название. Название правила доступа к веб-ресурсам. Элементы в таблице можно добавлять (см. раздел "Окно Правило Веб-Контроля" на стр. 501), изменять (см. раздел "Окно Правило Веб-Контроля" на стр. 501), удалять, перемещать вверх и вниз. Вы также можете импортировать список правил из файла по кнопке Дополнительно → Импортировать и экспортировать список добавленных правил в файл по кнопке Дополнительно → Экспортировать выбранное или Дополнительно → Экспортировать все. При импорте вам будет предложено заменить список правил или добавить правила к уже существующему списку.
Правило по умолчанию	В раскрывающемся списке вы можете выбрать правило по умолчанию, согласно которому приложение будет регулировать доступ к веб-ресурсам, которые не попадают под действие других правил: • Разрешать (значение по умолчанию) – разрешать доступ к веб-ресурсам. • Блокировать – блокировать доступ к веб-ресурсам.
Шаблоны сообщений	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Шаблоны сообщений (см. раздел "Настройка шаблонов сообщений Веб-Контроля" на стр. 506).

Параметр	Описание

В этом разделе

Окно Правило Веб-Контроля	501
Окно Выбор категории содержания	504
Окно Выбор категории типов данных	504
Окно Выбор адресов	504
Окно Выбор групп адресов	505
Окно Добавление группы адресов	505
Окно Выбор пользователей	505
Окно Пользователь или группа	505
Окно Расписание доступа	505

Окно Правило Веб-Контроля

В этом окне вы можете настроить параметры правила доступа к веб-ресурсам.

Таблица 164. Добавление правила Веб-Контроля

Параметр	Описание
Название правила	Поле ввода названия правила доступа к веб-ресурсам.
Использовать правило	Флажок включает или выключает использование этого правила во время работы приложения. Если флажок установлен, правило включено, Веб-Контроль применяет это правило во время работы. Если флажок снят, правило выключено и не используется во время работы Веб-Контроля. В дальнейшем вы можете включить использование этого правила Веб-Контролем, установив флажок. По умолчанию флажок установлен.
Фильтровать содержимое	В раскрывающемся списке вы можете выбрать фильтр содержимого веб-ресурса: • Не фильтровать (значение по умолчанию). При выборе этого элемента списка фильтр содержимого веб-ресурсов не используется. • По категориям содержания. При выборе этого элемента списка становится доступна кнопка Выбрать, по нажатию на которую открывается окно Выбор категории содержания (см. раздел "Окно Выбор категории содержания" на стр. 504). • По категориям типов данных. При выборе этого элемента списка становится доступна кнопка Выбрать, по нажатию на которую открывается окно Выбор категории типов данных (см. раздел "Окно Выбор категории типов данных" на стр. 504). • По категориям содержания и типов данных. При выборе этого элемента списка становятся доступны кнопки Выбрать, по нажатию на которые открываются окна, в которых вы можете выбрать нужные категории.
Фильтровать адрес	В раскрывающемся списке вы можете выбрать фильтр адреса веб-ресурса: • Любой адрес (значение по умолчанию). При выборе этого элемента списка фильтр адресов веб-ресурсов не используется, правило Веб-Контроля применяется ко всем адресам веб-ресурсов. • Указанные адреса. При выборе этого элемента списка становится доступна кнопка Выбрать адреса, по нажатию на которую открывается окно Выбор адресов (см. раздел "Окно Выбор адресов" на стр. 504), в котором вы можете выбрать нужные адреса веб-ресурсов.
Применять к пользователям	В раскрывающемся списке вы можете выбрать пользователей, на которых распространяется правило доступа к веб-ресурсам: • Ко всем пользователям (значение по умолчанию). При выборе этого элемента списка фильтр пользователей не используется, правило Веб-Контроля применяется ко всем пользователям. • К выбранным пользователям. При выборе этого элемента списка становится доступна кнопка Выбрать пользователей, по нажатию на которую открывается окно Выбор пользователей (см. раздел "Окно Выбор пользователей" на стр. 505).

Параметр	Описание
Расписание работы правила	В раскрывающемся списке вы можете настроить расписание работы правила доступа к веб-ресурсу: • Всегда (значение по умолчанию). При выборе этого элемента списка настраиваемое правило доступа к веб-ресурсу применяется без ограничений по времени, то есть в любое время. • <Название расписания>. При выборе этого элемента списка становятся доступны кнопки Удалить и Изменить, по нажатию на которые вы можете удалить или настроить это расписание. • Добавить новое расписание. При выборе этого элемента списка открывается окно Расписание доступа (см. раздел "Окно Расписание доступа" на стр. 475), в котором вы можете настроить новое расписание работы правила доступа к веб-ресурсу.
Действие правила	В раскрывающемся списке вы можете выбрать действие, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсу, удовлетворяющему правилу: • Разрешать (значение по умолчанию) – разрешать доступ к веб-ресурсу. • Блокировать – блокировать доступ к веб-ресурсу и выводить сообщение о запрете доступа. • Информировать – выводить предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

Окно Выбор категории содержания

В этом окне вы можете выбрать категории содержания, доступ к которым вы хотите контролировать.

Для этого установите флажки около нужных категорий. По умолчанию все флажки сняты.

При установке флажков около всех вложенных категорий содержания флажок около основной категории содержания, содержащей вложенные, автоматически не устанавливается.

Окно Выбор категории типов данных

В этом окне вы можете выбрать категории типов, доступ к которым вы хотите контролировать.

Для этого установите флажки около нужных категорий.

По умолчанию все флажки сняты.

Окно Выбор адресов

В этом окне вы можете указать адреса веб-ресурсов, доступ пользователей к которым вы хотите контролировать. Вы можете указать несколько адресов, в этом случае указывайте каждый адрес в новой строке для удобства их копирования. Для указания адресов вы можете использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. 514).

Если вы хотите указать группу адресов, откройте окно **Выбор групп адресов** (см. раздел "Окно Выбор групп адресов" на стр. [505](#)), нажав на кнопку **Добавить группу адресов**.

Окно Выбор групп адресов

Таблица содержит группы адресов веб-ресурсов, доступ пользователей к которым контролирует компонент Веб-Контроль. По умолчанию таблица пустая.

Если вы хотите добавить группу адресов в список групп в окне **Выбор адресов** (см. раздел "Окно Выбор адресов" на стр. [504](#)), установите флажок около названия группы в таблице и нажмите на кнопку **Добавить**, расположенную под таблицей.

Если вы хотите добавить новую группу адресов в список групп в этом окне, откройте окно **Добавление группы адресов** (см. раздел "Окно Добавление группы адресов" на стр. [505](#)), нажав на кнопку **Добавить**, расположенную над таблицей.

Окно Добавление группы адресов

В этом окне вы можете указать группы адресов веб-ресурсов, доступ пользователей к которым вы хотите контролировать. Вы можете указать несколько адресов в группе адресов, в этом случае указывайте каждый адрес в новой строке для удобства их копирования. Для указания адресов вы можете использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. [514](#)).

Окно Выбор пользователей

Таблица содержит имена и группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом. По умолчанию таблица пустая.

Если вы хотите добавить нового пользователя и/или группу пользователей в список пользователей в этом окне, нажав на кнопку **Добавить**, расположенную над таблицей, откройте окно **Пользователь или группа** (см. раздел "Окно Пользователь или группа" на стр. [505](#)).

Окно Пользователь или группа

В этом окне вы можете указать пользователя или группу пользователей, на которых распространяется правило доступа к веб-ресурсам.

Таблица 165. Настройка правила доступа к веб-ресурсам

Параметр	Описание
Тип	Пользователь или Группа, на которых распространяется правило.
Имя пользователя или группы	Имя пользователя или название группы пользователей, на которых распространяется правило.

Окно Расписание доступа

В этом окне вы можете настроить расписание доступа к веб-ресурсам.

Таблица 166. Расписание доступа к веб-ресурсам

Параметр	Описание
Название	Поле для ввода названия расписания доступа.
Интервалы времени	Таблица, в которой вы можете выбрать интервалы времени для расписания (дни и часы). Интервалы, выделенные зеленым, включены в расписание. Чтобы исключить интервал из расписания, выберите соответствующие ячейки. Исключенные из расписания интервалы выделены серым цветом. По умолчанию в расписание включены все интервалы (24/7).

Настройка шаблонов сообщений Веб-Контроля

В зависимости от действия, заданного в свойствах правил Веб-Контроля, при попытке пользователей получить доступ к веб-ресурсам приложение 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. Приложение выводит сообщение-предупреждение, если в параметрах правила, описывающего этот веб-ресурс, выбрано действие **Информировать**.
Если, по мнению пользователя, предупреждение ошибочно, по ссылке из предупреждения пользователь может отправить уже сформированное сообщение-жалобу администратору локальной сети организации.
- Сообщение о блокировке веб-ресурса. Приложение выводит сообщение о блокировке веб-ресурса, если в параметрах правила, которое описывает этот веб-ресурс, выбрано действие **Блокировать**.
Если, по мнению пользователя, блокировка доступа к веб-ресурсу была ошибочна, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить уже сформированное сообщение-жалобу администратору локальной сети организации.

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и сообщения-жалобы для отправки администратору локальной сети организации предусмотрены шаблоны. Вы можете изменять их содержание.

► Чтобы изменить шаблон сообщения в Web Console:

- В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.
Откроется список политик.
- Выберите группу администрирования, содержащую устройства, на которых применяется политика. Для этого нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите группу администрирования в открывшемся окне.
В списке отобразятся политики, настроенные для выбранной группы администрирования.
- Нажмите на название нужной политики в списке.
Откроется окно свойств политики.
- В окне свойств политики выберите **Параметры приложения** → **Контроль безопасности** → **Веб-Контроль**.

5. В блоке **Шаблоны** настройте шаблоны сообщений Веб-Контроля на следующих закладках:

- **Предупреждение.** Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекommenованному веб-ресурсу.
- **Сообщение о блокировке.** Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.
- **Сообщение администратору.** Поле ввода содержит шаблон сообщения-жалобы для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ приложение Kaspersky Industrial CyberSecurity for Linux Nodes отправляет в Kaspersky Security Center событие *Сообщение администратору о запрете доступа к веб-странице*. Описание события содержит сообщение администратору с подставленными переменными. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

На закладках **Предупреждение** и **Сообщение о блокировке** вы можете добавлять переменные и ссылки в тексты сообщений для пользователя, используя кнопки **Добавить переменную** и **Добавить ссылку**. Вы можете восстановить текст шаблона сообщения, нажав на кнопку **По умолчанию**.

6. Нажмите на кнопку **ОК**.

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

► Чтобы изменить шаблон сообщения в Консоли администрирования:

1. В дереве Консоли администрирования в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.
2. В рабочей области выберите закладку **Политики**.
3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

Вы также можете открыть окно свойств политики с помощью пункта **Свойства** контекстного меню политики или по ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

4. В окне политики выберите **Контроль безопасности** → **Веб-Контроль**.
5. В блоке **Шаблоны сообщений** нажмите на кнопку **Настроить**.
6. В открывшемся окне **Шаблоны сообщений** настройте шаблоны сообщений Веб-Контроля на следующих закладках:

- **Предупреждение.** Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекommenованному веб-ресурсу.
- **Сообщение о блокировке.** Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.
- **Жалоба администратору.** Поле ввода содержит шаблон сообщения-жалобы для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ приложение Kaspersky Industrial CyberSecurity for Linux Nodes отправляет в Kaspersky Security Center событие *Сообщение администратору о запрете доступа к веб-странице*. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной

выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

На закладках **Предупреждение** и **Сообщение о блокировке** вы можете добавлять переменные и ссылки в тексты сообщений для пользователя, используя кнопки **Переменная** и **Вставить ссылку**. Вы можете восстановить текст шаблона сообщения, нажав на кнопку **По умолчанию**.

7. Нажмите на кнопку **ОК**.
8. Нажмите на кнопку **Применить**.

Настройка Веб-Контроля в командной строке

В командной строке вы можете управлять Веб-Контролем с помощью предустановленной задачи Веб-Контроль (*Web_Control*).

Задача Веб-Контроль по умолчанию остановлена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачу вручную.

Вы можете настраивать параметры (см. раздел "Параметры задачи Веб-Контроль" на стр. [508](#)) Веб-Контроля, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи Веб-Контроль.

Вы также можете просматривать и настраивать параметры Веб-Контроля (см. раздел "Просмотр и изменение параметров Веб-Контроля" на стр. [513](#)) с помощью команд управления Веб-Контролем.

В этом разделе

Параметры задачи Веб-Контроль	508
Просмотр и изменение параметров Веб-Контроля	513

Параметры задачи Веб-Контроль

В таблице ниже описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Веб-Контроль.

Таблица 167. Параметры задачи Веб-Контроль

Параметр	Описание	Значения
WebControlDefaultAction	Правило по умолчанию, то есть действие, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсам, которые не попадают под действие других правил.	Allow (значение по умолчанию) – разрешать доступ к веб-ресурсам. Block – запрещать доступ к веб-ресурсам.
ComplaintRecipient	Адрес электронной почты администратора для отправки ему сообщения об ошибочной блокировке веб-ресурса.	
Секция [Rules.item_#] содержит следующие параметры:		
Name	Название правила доступа к веб-ресурсам (см. раздел "О правилах доступа к веб-ресурсам" на стр. 490).	
WebControlAction	Действие правила, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсу, удовлетворяющему правилу.	Allow (значение по умолчанию) – разрешать доступ к веб-ресурсу. Block – запрещать доступ к веб-ресурсу. Notify – выводить предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
Enabled	Статус работы правила доступа к веб-ресурсам.	Yes – правило включено, Веб-Контроль применяет это правило во время работы. No (значение по умолчанию) – правило выключено и не используется во время работы Веб-Контроля.
ScheduleId	Идентификатор расписания, который используется в секции [Schedules.item_#].	
UseUrls	Использование в правиле фильтра адресов веб-ресурса.	Yes – использовать в правиле фильтр адресов веб-ресурсов. No (значение по умолчанию) – не использовать фильтр адресов веб-ресурсов, применять правило ко всем адресам веб-ресурсов.
Urls.item_#	Адрес веб-ресурса, доступ к которому регулирует правило.	Для указания адреса веб-ресурса вы можете использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. 514).

Параметр	Описание	Значения
UseCategories	Использование в правиле фильтров по категориям содержания и по категориям типов данных.	None (значение по умолчанию) – не использовать фильтр содержимого веб-ресурсов. ContentOnly – использовать в правиле фильтр по категориям содержания. FormatOnly – использовать в правиле фильтр категориям типов данных. ContentAndFormat – использовать в правиле фильтр по категориям содержания и категориям типов данных.
[Rules.item_#.ContentCategories.item_#]	Секция для указания категории содержания.	–
ContentCategory	Категория содержания.	AdultContent, AlcoholTobaccoNarcotics, Violence, Profanity, Weapons, ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepstakes, InternetCommunicationMedia, CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileSharing, AudioAndVideo, BankSites, Blogs, DatingSites, LegislationRF, LegislationGlobal, SexuallyExplicit, Sexuality, GenerativeAITools
[Rules.item_#.FormatCategories.item_#]	Секция для указания категории типов данных.	–

Параметр	Описание	Значения
<code>FormatCategories.item_#.FormatCategory</code>	Категория типов данных.	<code>Video</code> – Видео <code>Audio</code> – Звуковые данные <code>OfficeDocument</code> – Файлы офисных приложений <code>Executable</code> – Исполняемые файлы <code>Archives</code> – Архивы <code>Images</code> – Графические файлы <code>Scripts</code> – Скрипты
<code>UsePrincipals</code>	Использование фильтра пользователей, на которых распространяется правило доступа к веб-ресурсам.	<code>Yes</code> – использовать в правиле фильтр пользователей. <code>No</code> (значение по умолчанию) – не использовать фильтр пользователей, применять правило ко всем пользователям.
<code>[Rules.item_#.Principals.item_#]</code>	Секция для указания пользователей, на которых распространяется правило доступа к веб-ресурсам.	
<code>Name</code>	Пользователь или группа пользователей, на которых распространяется правило доступа к веб-ресурсам.	<code><имя пользователя></code> – имя пользователя, для которого применяется правило. <code>@<название группы></code> – название группы пользователей, для которых применяется правило. Значение по умолчанию: правило доступа к веб-ресурсам применяется для всех пользователей.
Секция [UrlCategories.item_#] содержит следующие параметры:		
<code>Name</code>	Название группы адресов веб-ресурсов, доступ к которым регулирует правило.	
<code>Urls.item_#</code>	Адрес веб-ресурса, входящего в группу.	Для указания адреса веб-ресурса вы можете использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. 514).
Секция [Schedules.item_#] содержит расписание работы правила.		
<code>Id</code>	Идентификатор расписания, который используется в секции <code>[Rules.item_#]</code> .	1 – 999999 0 – идентификатор расписания <code>Default</code> (по умолчанию), которое обеспечивает работу правила без ограничений по времени, то есть в любое время.

Параметр	Описание	Значения
Name	Название расписания.	
DaysHours	Интервалы времени для расписания.	<день недели> – дни недели. Вы можете использовать как полные названия дней недели, так и аббревиатуры (например, для понедельника можно указать Mo, Mon или Monday). Для дней недели можно указывать либо интервалы, либо конкретные дни. Неделя начинается с воскресенья. <час> – часы [0:24]. Для часов вы можете указывать только интервалы.

Просмотр и изменение параметров Веб-Контроля

- Чтобы просмотреть параметры Веб-Контроля, выполните следующую команду:

```
kics-control --get-settings 26 [--file <путь к конфигурационному файлу>]
[--json]
```

где:

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу, в который будут выведены параметры.

--json – выводить данные в формате JSON.

- Чтобы изменить параметры Веб-Контроля, выполните следующую команду:

```
kics-control --set-settings 26 [--file <путь к конфигурационному файлу>]
[--json]
```

где:

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу, из которого будут импортированы параметры.

--json – импорт данных из файла в формате JSON.

- Чтобы удалить настроенные параметры и восстановить значения параметров Веб-Контроля до правила по умолчанию (см. раздел "Веб-Контроль" на стр. [489](#)), выполните следующую команду:

```
kics-control --set-settings 26 --set-to-default
```

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 (см. раздел "О правилах доступа к веб-ресурсам" на стр. 490) 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`.

2. Последовательность символов ***.** позволяет выбрать все домены адреса – *маска домена*. Маска домена ***.** трактуется как любое имя домена, имя поддомена или пустая строка.

Пример: под действие маски ***.example.com** попадают следующие адреса:

- `http://pictures.example.com` – маска домена ***.** применена для **pictures..**
- `http://user.pictures.example.com` – маска домена ***.** применена для **pictures.** и **user..**
- `http://example.com` – маска домена ***.** трактуется как пустая строка.

3. Последовательность символов **www.** в начале маски адреса трактуется как последовательность ***..**

Пример: маска адреса `www.example.com` трактуется как ***.example.com**. Под действие маски попадают адреса `www2.example.com` и `www.pictures.example.com`.

4. Если маска адреса начинается не с символа *****, то содержание маски адреса эквивалентно тому же содержанию с префиксом ***..**
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 168. 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 2.
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 3, 2, 1.
7	www.example.com	https://www.example.com	Да	См. правила 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Да	См. правила 3, 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.

Контроль целостности системы

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes позволяет контролировать целостность операционной системы защищаемого устройства в режиме реального времени и по требованию.

- Компонент *Контроль целостности системы* позволяет в реальном времени отслеживать изменения в файлах и директориях (см. раздел "Контроль целостности системы в реальном времени" на стр. [516](#)), которые вы включили в область мониторинга в параметрах компонента. Вы можете отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве.
- С помощью задач *Проверка целостности системы* вы можете проверять наличие изменений в файлах и директориях (см. раздел "Проверка целостности системы" на стр. [528](#)), которые вы включили в область мониторинга, путем сравнения текущего состояния контролируемого объекта с ранее зафиксированным состоянием.

Обнаружив изменения файлов и директорий из области мониторинга, приложение Kaspersky Industrial CyberSecurity for Linux Nodes формирует события об изменениях в списках контроля доступа к объектам. Компонент Контроль целостности системы не передает данные о том, какие именно изменения внесены. Задача *Проверка целостности системы* передает данные об измененных атрибутах и перемещенных файлах и директориях.

В этом разделе

Контроль целостности системы в реальном времени.....	516
Проверка целостности системы	528

Контроль целостности системы в реальном времени

Компонент Контроль целостности системы позволяет определять каждое изменение объекта, включенного в область мониторинга, путем перехвата файловых операций в режиме реального времени.

Во время работы компонента Контроль целостности системы приложение контролирует изменение следующих параметров файлов:

- содержимое (write (), truncate (), etc.);
- метаданные (правообладание (chmod/chown));
- отметки времени (utimensat);
- расширенные атрибуты (setxattr) и другие.

Контрольная сумма файла не рассчитывается.

Технологические ограничения операционной системы Linux не позволяют приложению определять, какой пользователь или процесс внес изменение в файл.

По умолчанию Контроль целостности системы выключен. Вы можете включать и выключать Контроль

целостности системы, а также настраивать параметры работы компонента:

- Настраивать области мониторинга для контроля целостности системы. Приложение отслеживает операции с файлами в областях мониторинга, указанных в параметрах компонента Контроль целостности системы. Для работы компонента требуется указать хотя бы одну область мониторинга. По умолчанию задана область мониторинга *Внутренние объекты "Лаборатории Касперского"* (/opt/kaspersky/kics/).

Вы можете указать несколько областей мониторинга. Вы можете изменять области мониторинга в режиме реального времени.

Приложение не отслеживает изменения файлов (атрибутов и содержимого) с жесткими ссылками, которые расположены вне области мониторинга.

- Настраивать исключение объектов из мониторинга по маске имени.
- Настраивать области исключения для контроля целостности системы. Исключения задаются для каждой отдельной области мониторинга и работают только для указанной области. Вы можете указать несколько областей исключения из мониторинга.

Исключение имеет более высокий приоритет, чем область мониторинга, исключенный объект не проверяется, даже если находится в области мониторинга. Если область мониторинга задана на более низком уровне, чем директория, указанная в исключении, то приложение не отслеживает эту область мониторинга во время контроля целостности системы.

При добавлении директории в область мониторинга или в область исключения приложение не проверяет, существует ли такая директория.

В этом разделе

Настройка контроля целостности системы в Web Console.....	517
Настройка контроля целостности системы в Консоли администрирования	522
Настройка контроля целостности системы в командной строке	525

Настройка контроля целостности системы в Web Console

В Web Console вы можете настраивать параметры контроля целостности системы в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения → Контроль безопасности → Контроль целостности системы**).

Таблица 169. Параметры компонента Контроль целостности системы

Параметр	Описание
Контроль целостности системы включен / выключен	Переключатель включает или выключает компонент Контроль целостности системы. По умолчанию переключатель выключен.
Области мониторинга	По ссылке Настроить области мониторинга открывается окно Области мониторинга (см. раздел "Окно Области мониторинга" на стр. 518).
Области исключения	По ссылке Настроить области исключения из мониторинга открывается окно Области исключения (см. раздел "Окно Области исключения" на стр. 519).
Исключения по маске	По ссылке Настроить исключения по маске открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 521).

Окно Области мониторинга

Таблица содержит области мониторинга компонента Контроль целостности системы. Приложение контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kics/).

Таблица 170. Параметры области мониторинга Контроля целостности системы

Параметр	Описание
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Industrial CyberSecurity for Linux Nodes проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно добавления области мониторинга

В этом окне вы можете добавить или настроить область мониторинга для компонента Контроля целостности системы.

Таблица 171. Параметры области мониторинга

Параметр	Описание
Название области	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна Области мониторинга (см. раздел "Окно Области мониторинга" на стр. 518). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение контролирует эту область мониторинга во время работы. Если флажок снят, приложение не контролирует эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Для указания пути вы можете использовать маски. Поле не должно быть пустым. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, <code>/dir/*/file</code> или <code>/dir/**/file</code>. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, <code>/dir/**/file*/</code> или <code>/dir/file**/</code>. Маску ** можно использовать в имени директории только один раз. Например, <code>/dir/**/**/file</code> – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение проверяет все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Области исключения

Таблица содержит области исключения из мониторинга для компонента Контроль целостности системы. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 172. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли приложение эту область из мониторинга при работе компонента.

Элементы в таблице можно добавлять, изменять и удалять.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения из мониторинга для компонента Контроль целостности системы.

Таблица 173. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 519). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы приложения. Если флажок установлен, приложение исключает эту область из мониторинга во время работы компонента. Если флажок снят, приложение контролирует эту область во время работы компонента. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски. Поле не должно быть пустым. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение исключает из мониторинга. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Приложение не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Настройка контроля целостности системы в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры контроля целостности системы в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Контроль безопасности** → **Контроль целостности системы**).

Таблица 174. Параметры компонента Контроль целостности системы

Параметр	Описание
Включить Контроль целостности системы	Флажок включает или выключает Контроль целостности системы. По умолчанию флажок снят.
Области мониторинга	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области проверки (см. раздел "Окно Области мониторинга" на стр. 518).
Исключения из мониторинга	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области исключения (см. раздел "Окно Области исключения" на стр. 519).
Исключения по маске	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 521).

Окно Области проверки

Таблица содержит области мониторинга для компонента Контроль целостности системы. Приложение контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kics/).

Таблица 175. Параметры области мониторинга

Параметр	Описание
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Industrial CyberSecurity for Linux Nodes проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить области мониторинга для компонента Контроль целостности системы.

Таблица 176. Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна Области проверки (см. раздел "Окно Области мониторинга" на стр. 518). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение контролирует эту область мониторинга во время работы приложения. Если флажок снят, приложение не контролирует эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Поле не должно быть пустым. По умолчанию указан путь /opt/kaspersky/kics.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Области исключения

Таблица содержит области исключения из мониторинга для компонента Контроль целостности системы. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 177. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли приложение эту область из мониторинга при работе компонента.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Название области исключения>

В этом окне вы можете добавить или настроить область исключения из мониторинга для компонента Контроль целостности системы.

Таблица 178. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 519). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы приложения. Если флажок установлен, приложение исключает эту область из мониторинга во время работы компонента. Если флажок снят, приложение контролирует эту область во время работы компонента. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Поле не должно быть пустым. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение исключает из мониторинга. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Приложение не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задать маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Настройка контроля целостности системы в командной строке

В командной строке вы можете управлять контролем целостности системы в реальном времени с помощью предустановленной задачи Контроль целостности системы (*System_Integrity_Monitoring*). Тип задачи – *OAFIM*.

Задача Контроль целостности системы по умолчанию не запущена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачу вручную.

Вы можете настраивать параметры контроля целостности системы на устройстве, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи Контроль целостности системы.

Таблица 179. Параметры задачи Контроль целостности системы при доступе

Параметр	Описание	Значения
UseExcludeMasks	Включение исключения из области мониторинга объектов, указанными параметром <code>ExcludeThreats.item_#</code>. Этот параметр работает, только если указано значение параметра <code>ExcludeMasks.item_#</code>.	Yes – исключать объекты, указанные параметром <code>ExcludeMasks.item_#</code>, из области мониторинга. No (значение по умолчанию) – не исключать объекты, указанные параметром <code>ExcludeMasks.item_#</code>, из области мониторинга.
ExcludeMasks.item_#	Исключение из мониторинга объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр <code>UseExcludeMasks</code>. Вы можете указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом.	Значение по умолчанию не задано.
Секция [ScanScope.item_#] содержит области мониторинга для задачи Контроль целостности системы. Для задачи должна быть указана минимум одна область мониторинга. Вы можете указать несколько секций [ScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области мониторинга, содержит дополнительную информацию об области мониторинга.	Значение по умолчанию не задано.
UseScanArea	Включение мониторинга указанной области.	Yes (значение по умолчанию) – контролировать указанную область. No – не контролировать указанную область.
Path	Путь к директории для мониторинга.	Для указания пути вы можете использовать маски. Значение по умолчанию: <code>/opt/kaspersky/kics/</code>

Параметр	Описание	Значения
AreaMask.item_#	Ограничение области мониторинга. В области мониторинга приложение проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (контролировать все объекты).
Секция [ExcludedFromScanScope.item_#] содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#]. Вы можете указать несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области исключения из мониторинга, содержит дополнительную информацию об области исключения из мониторинга.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из мониторинга.	Yes (значение по умолчанию) – исключать указанную область из мониторинга. No – не исключать указанную область из мониторинга.
Path	Путь к директории с объектами, исключаемыми из мониторинга.	Для указания пути вы можете использовать маски. Значение по умолчанию не задано.
AreaMask.item_#	Ограничение области исключения из мониторинга. В области исключения из мониторинга приложение исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (исключать из мониторинга все объекты).

Проверка целостности системы

Во время выполнения задачи *Проверка целостности системы* изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием. Сравнение может выполняться по следующим критериям:

- хеш файла;
- время изменения файла;
- размер файла.

Исходное состояние контролируемых объектов фиксируется в качестве *снимка состояния системы*. Снимок состояния системы содержит пути к контролируемым объектам и их метаданные.

Снимок состояния системы может содержать персональные данные.

Снимок состояния системы создается во время первого выполнения задачи проверки целостности системы на устройстве. Если вы создали несколько задач проверки целостности системы, для каждой задачи создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы содержит информацию об объектах, которые относятся к области мониторинга, настроенной для задачи. Если снимок состояния системы не соответствует области мониторинга, приложение Kaspersky Industrial CyberSecurity for Linux Nodes формирует событие о нарушении целостности системы.

Снимок состояния системы обновляется при изменении параметров задачи, например, при добавлении новой области мониторинга.

Приложение создает хранилище для снимков состояния системы на защищаемом устройстве. По умолчанию снимки состояния системы хранятся в базе данных `/var/opt/kaspersky/kics/private/fim.db`. Для доступа к базе данных, в которой хранятся снимки состояния системы, требуются root-права.

Вы можете удалить снимок состояния системы, удалив соответствующую задачу проверки целостности системы.

Вы можете запускать проверку целостности системы по требованию и настраивать параметры проверки:

- Включать и выключать обновление снимка состояния системы каждый раз после завершения задачи проверки целостности системы.
- Выбирать критерии, по которым выполняется сравнение текущего состояния контролируемого файла с исходным состоянием: использовать хеш и время изменения файла или только размер файла.
- Настраивать области мониторинга для проверки целостности системы.
- Настраивать области исключения из проверки целостности системы. Вы можете указывать пути к исключаемым файлам и директориям и исключать отдельные объекты по маске имени.

В этом разделе

Проверка целостности системы в Web Console	529
Проверка целостности системы в Консоли администрирования	534
Проверка целостности системы в командной строке	539

Проверка целостности системы в Web Console

В Web Console вы можете выполнять проверку целостности системы с помощью задачи *Проверка целостности системы*.

Вы можете создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)) пользовательские задачи проверки целостности системы. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) параметры задач.

Таблица 180. Параметры задачи Проверка целостности системы

Параметр	Описание
Обновлять снимок состояния системы при каждом запуске задачи	Флажок включает или выключает обновление снимка состояния системы при каждом запуске задачи <i>Проверка целостности системы</i> . По умолчанию флажок снят.
Использовать хеш SHA256 для проверки	Флажок включает или выключает использование хеша файла в качестве критерия для сравнения текущего состояния файла с исходным состоянием. Если флажок снят, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром). По умолчанию флажок снят.
Проверять директории в областях мониторинга	Флажок включает или выключает проверку директорий во время выполнения проверки целостности системы. По умолчанию флажок снят.
Отслеживать время последнего доступа к файлу	Флажок включает или выключает отслеживание времени доступа к файлу во время выполнения проверки целостности системы. По умолчанию флажок снят.
Области мониторинга	Таблица, содержащая области мониторинга, проверяемые задачей. По умолчанию таблица содержит область мониторинга Внутренние объекты "Лаборатории Касперского" (/opt/kaspersky/kics/). Области мониторинга в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область мониторинга для задачи Проверка целостности системы.

Таблица 181. Параметры области мониторинга

Параметр	Описание
Название области	Поле ввода названия области мониторинга. Это название будет отображаться в таблице раздела Параметры проверки. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение контролирует эту область мониторинга во время работы приложения. Если флажок снят, приложение не контролирует эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, <code>/dir/*/file</code> или <code>/dir/**/file</code>. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, <code>/dir/**/file*/</code> или <code>/dir/file**/</code>. Маску ** можно использовать в имени директории только один раз. Например, <code>/dir/**/**/file</code> – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле не должно быть пустым. По умолчанию указан путь / – приложение проверяет все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Раздел Области исключения

В разделе **Области исключения** для задачи Проверка целостности системы вы можете настроить области исключения (см. раздел "Окно Области исключения" на стр. [532](#)) из проверки и исключения по маске (см. раздел "Окно Исключения по маске" на стр. [521](#)).

Окно Области исключения

Таблица содержит области исключения из мониторинга для задачи Проверка целостности системы. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 182. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли приложение эту область из мониторинга при работе задачи.

Элементы в таблице можно добавлять, изменять и удалять.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения из мониторинга для задачи Проверка целостности системы.

Таблица 183. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 532). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы приложения. Если флажок установлен, приложение исключает эту область из мониторинга во время работы задачи. Если флажок снят, приложение контролирует эту область во время работы задачи. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле не должно быть пустым. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение исключает из мониторинга. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Приложение не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задать маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_???.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Проверка целостности системы в Консоли администрирования

В Консоли администрирования вы можете выполнять проверку целостности системы с помощью задачи *Проверка целостности системы*.

Вы можете создавать (см. раздел "Создание задач в Консоли администрирования" на стр. [116](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Консоли администрирования" на стр. [117](#)) пользовательские задачи проверки целостности системы. Вы можете настраивать параметры проверки, изменяя (см. раздел "Изменение параметров задач в Консоли администрирования" на стр. [117](#)) параметры задач.

В разделе **Параметры** в свойствах задачи Проверка целостности системы вы можете настроить параметры, приведенные в таблице ниже.

Таблица 184. Параметры задачи Проверка целостности системы

Параметр	Описание
Обновлять снимок состояния системы при каждом запуске задачи	Флажок включает или выключает обновление снимка состояния системы при каждом запуске задачи Проверка целостности системы. По умолчанию флажок снят.
Использовать хеш (SHA256) для проверки	Флажок включает или выключает использование хеша файла в качестве критерия для сравнения текущего состояния файла с исходным состоянием. Если флажок снят, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром). По умолчанию флажок снят.
Проверять директории в областях мониторинга	Флажок включает или выключает проверку директорий в указанных областях мониторинга во время выполнения проверки целостности системы. По умолчанию флажок снят.
Отслеживать время последнего доступа к файлу	Флажок включает или выключает отслеживание времени доступа к файлу во время выполнения проверки целостности системы. По умолчанию флажок снят.
Области мониторинга	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области проверки (см. раздел "Окно Области проверки" на стр. 522).

В разделе **Области исключения** (см. раздел "Раздел Области исключения" на стр. [537](#)) в свойствах задачи Проверка целостности системы вы можете настроить области исключения из мониторинга (см. раздел "Окно Области исключения" на стр. [519](#)) и исключения по маске (см. раздел "Окно Исключения по маске" на стр. [521](#)).

Окно Области проверки

Таблица содержит области мониторинга для задачи Проверка целостности системы. Приложение контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kics/).

Таблица 185. Параметры области мониторинга

Параметр	Описание
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Industrial CyberSecurity for Linux Nodes проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить области мониторинга для задачи Проверка целостности системы.

Таблица 186. Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна Области проверки (см. раздел "Окно Области мониторинга" на стр. 518). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение контролирует эту область мониторинга во время работы приложения. Если флажок снят, приложение не контролирует эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, <code>/dir/*/file</code> или <code>/dir/**/file</code>. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, <code>/dir/**/file*/</code> или <code>/dir/file**/</code>. Маску ** можно использовать в имени директории только один раз. Например, <code>/dir/**/**/file</code> – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле не должно быть пустым. По умолчанию указан путь <code>/opt/kaspersky/kics</code>.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Раздел Области исключения

Таблица 187. Параметры исключений из проверки

Блок параметров	Описание
Исключения из мониторинга	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Области исключения (см. раздел "Окно Области исключения" на стр. 519). В этом окне вы можете задать список областей исключений из мониторинга.
Исключения по маске	Блок параметров содержит кнопку Настроить , по нажатию на которую открывается окно Исключения по маске (см. раздел "Окно Исключения по маске" на стр. 521). В этом окне вы можете настроить исключение объектов из мониторинга по маске имени.

Окно Области исключения

Таблица содержит области исключения из проверки для задачи Проверка целостности системы. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям.

По умолчанию таблица пуста.

Таблица 188. Параметры области исключения задачи Проверка целостности системы

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, исключает ли приложение эту область из проверки при работе задачи.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из мониторинга для задачи Проверка целостности системы.

Таблица 189. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения (см. раздел "Окно Области исключения" на стр. 537). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы приложения. Если флажок установлен, приложение исключает эту область из мониторинга во время работы задачи. Если флажок снят, приложение контролирует эту область во время работы задачи. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле не должно быть пустым. По умолчанию указан путь / – приложение исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение исключает из мониторинга. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Приложение не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Industrial CyberSecurity for Linux Nodes исключает из проверки.

Примеры:

Маска *.txt – все текстовые файлы.

Маска *_my_file_?.html – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием _my_file_, за которым следуют любые два символа (например, 2020_my_file_09.html).

Проверка целостности системы в командной строке

В командной строке вы можете выполнять проверку целостности системы на устройстве с помощью пользовательских задач (см. раздел "Создание задачи в командной строке" на стр. [127](#)) *Проверка целостности системы* (задач типа *ODFIM*).

Вы можете запускать, останавливать, приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) пользовательские задачи вручную и настраивать расписание (см. раздел "Настройка расписания задачи в командной строке" на стр. [135](#)) запуска задачи. Вы можете настраивать параметры проверки целостности системы, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры этих задач.

Таблица 190. Параметры задачи Проверка целостности системы

Параметр	Описание	Значения
RebuildBaseline	Включение обновления снимка состояния системы после завершения задачи <i>Проверка целостности системы</i> .	Yes – обновлять снимок состояния системы каждый раз после завершения задачи <i>Проверка целостности системы</i> . No (значение по умолчанию) – не обновлять снимок состояния системы каждый раз после завершения задачи <i>Проверка целостности системы</i> .
CheckFileHash	Использовать хеш файла (SHA256) в качестве критерия, по которому выполняется сравнение текущего состояния контролируемого файла с исходным состоянием.	Yes – проверять хеш. No (значение по умолчанию) – выключить проверку хеша. Если проверка выключена, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром).
TrackDirectoryChanges	Включение мониторинга директорий.	Yes – контролировать директории во время выполнения проверки целостности системы. No (значение по умолчанию) – не контролировать директории.
TrackLastAccessTime	Включение проверки времени последнего доступа к файлу. В операционных системах Linux это параметр <code>noatime</code> .	Yes – проверять время последнего доступа к файлу. No (значение по умолчанию) – не проверять время последнего доступа к файлу.
UseExcludeMasks	Включение исключения из области мониторинга объектов, указанными параметром <code>ExcludeMasks.item_#</code> . Этот параметр работает, только если указано значение параметра <code>ExcludeMasks.item_#</code> .	Yes – исключать объекты, указанные параметром <code>ExcludeMasks.item_#</code> , из области мониторинга. No (значение по умолчанию) – не исключать объекты, указанные параметром <code>ExcludeMasks.item_#</code> , из области мониторинга.

Параметр	Описание	Значения
<code>ExcludeMasks.item_#</code>	Исключение из мониторинга объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр <code>UseExcludeMasks</code>. Вы можете указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом.	Значение по умолчанию не задано.
Секция [ScanScope.item_#] содержит области мониторинга для задачи <i>Проверка целостности системы</i>. Для задачи должна быть указана минимум одна область мониторинга. Вы можете указать несколько секций [ScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
<code>AreaDesc</code>	Описание области мониторинга, содержит дополнительную информацию об области мониторинга.	Значение по умолчанию не задано.
<code>UseScanArea</code>	Включение мониторинга указанной области.	Yes (значение по умолчанию) – контролировать указанную область. No – не контролировать указанную область.
<code>Path</code>	Путь к директории для мониторинга.	Для указания пути вы можете использовать маски. Значение по умолчанию: <code>/opt/kaspersky/kics/</code>
<code>AreaMask.item_#</code>	Ограничение области мониторинга. В области мониторинга приложение проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов <code>AreaMask.item_#</code> в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (контролировать все объекты).
Секция [ExcludedFromScanScope.item_#] содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#]. Вы можете указать несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		

Параметр	Описание	Значения
AreaDesc	Описание области исключения из мониторинга, содержит дополнительную информацию об области исключения из мониторинга.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из мониторинга.	Yes (значение по умолчанию) – исключать указанную область из мониторинга. No – не исключать указанную область из мониторинга.
Path	Путь к директории с объектами, исключаемыми из мониторинга.	Для указания пути вы можете использовать маски. Значение по умолчанию не задано.
AreaMask.item_#	Ограничение области исключения из мониторинга. В области исключения из мониторинга приложение исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (исключать из мониторинга все объекты).

Анализ поведения

Компонент Анализ поведения позволяет контролировать вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности Kaspersky Industrial CyberSecurity for Linux Nodes может завершать процесс приложения, осуществляющего вредоносную активность.

По умолчанию Анализ поведения выключен.

Вы можете включать и выключать Анализ поведения, а также настраивать параметры работы компонента:

- Выбирать действие, которое Kaspersky Industrial CyberSecurity for Linux Nodes будет выполнять при обнаружении вредоносной активности в операционной системе: информировать пользователя или блокировать приложение, осуществляющее вредоносную активность.
- Исключать активность процессов из проверки.

Если включена интеграция приложения Kaspersky Industrial CyberSecurity for Linux Nodes с решением Kaspersky Managed Detection and Response, исключения по процессам не применяются при анализе поведения приложений в операционной системе.

По умолчанию на операционной системе СинтезМ-Клиент конфигурация службы auditd заблокирована против изменений, то есть находится в режиме работы `enabled` 2. Для корректной работы компонента Анализ поведения при интеграции Kaspersky Industrial CyberSecurity for Linux Nodes с решением Kaspersky Managed Detection and Response требуется изменить режим работы auditd в конфигурационных файлах на режим без блокировки конфигурации `enabled` 1 и перезагрузить операционную систему.

В этом разделе

Настройка анализа поведения в Web Console.....	544
Настройка анализа поведения в Консоли администрирования	546
Настройка анализа поведения в командной строке	548

Настройка анализа поведения в Web Console

В Web Console вы можете настраивать параметры анализа поведения приложений в политике (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (Параметры приложения → Продвинутая защита → Анализ поведения).

Таблица 191. Параметры компонента Анализ поведения

Параметр	Описание
Анализ поведения включен / выключен	Переключатель включает или выключает компонент Анализ поведения. По умолчанию переключатель выключен.
Действие при обнаружении вредоносной активности	Действие, которое Kaspersky Industrial CyberSecurity for Linux Nodes будет выполнять при обнаружении вредоносной активности в операционной системе: • Информировать пользователя (значение по умолчанию). Kaspersky Industrial CyberSecurity for Linux Nodes не завершает процесс, осуществляющий вредоносную активность, только записывает событие об обнаружении вредоносной активности в журнал событий. • Блокировать приложение, осуществляющее вредоносную активность. Kaspersky Industrial CyberSecurity for Linux Nodes завершает процесс, осуществляющий вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности.
Исключения по процессам	По ссылке Настроить исключения по процессам открывается окно Исключения по процессам (см. раздел "Окно Исключения по процессам" на стр. 545). В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса и файлов, изменяемых указанным процессом. По умолчанию таблица пуста.

Если включена интеграция приложения Kaspersky Industrial CyberSecurity for Linux Nodes с решением Kaspersky Managed Detection and Response, исключения по процессам не применяются.

Таблица 192. Параметры области исключения по процессам

Параметр	Описание
Исключать / Не исключать из проверки доверенные процессы	Переключатель включает или выключает использование настроенных исключений по процессам в работе компонента Анализ поведения. По умолчанию переключатель выключен.
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять (см. раздел "Окно добавления области исключения по процессам" на стр. [546](#)) и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Экспортировать**. При импорте вам будет предложено заменить список исключений или добавить исключения к уже существующему списку.

Окно добавления области исключения по процессам

В этом окне вы можете добавить или настроить область исключения по процессам.

Таблица 193. Параметры области исключения

Параметр	Описание
Название области исключения по процессам	Поле ввода названия области исключения по процессам. Это название будет отображаться в таблице окна Исключения по процессам (см. раздел "Окно Исключения по процессам" на стр. 545). Поле ввода не должно быть пустым.
Использовать это исключение	Флажок включает или выключает исключение этой области во время работы приложения. По умолчанию флажок установлен.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле ввода не должно быть пустым.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром Путь к исключаемому процессу. По умолчанию флажок снят.

Настройка анализа поведения в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры анализа поведения приложений в политике (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Продвинутая защита** → **Анализ поведения**).

Таблица 194. Параметры компонента Анализ поведения

Параметр	Описание
Включить Анализ поведения	Флажок включает или выключает компонент Анализ поведения. По умолчанию флажок снят.
Действие при обнаружении вредоносной активности	Действие, которое Kaspersky Industrial CyberSecurity for Linux Nodes будет выполнять при обнаружении вредоносной активности в операционной системе: • Блокировать приложение, осуществляющее вредоносную активность. Kaspersky Industrial CyberSecurity for Linux Nodes завершает процесс, осуществляющий вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности. • Информировать пользователя (значение по умолчанию). Kaspersky Industrial CyberSecurity for Linux Nodes не завершает процесс, осуществляющий вредоносную активность, только записывает событие об обнаружении вредоносной активности в журнал событий.
Использовать исключения по процессам	Флажок включает или выключает использование исключений по процессам в работе компонента Анализ поведения. По умолчанию флажок снят. По кнопке Настроить открывается окно Исключения по процессам (см. раздел "Окно Исключения по процессам" на стр. 547). В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса из проверки. По умолчанию таблица пуста.

Если включена интеграция приложения Kaspersky Industrial CyberSecurity for Linux Nodes с решением Kaspersky Managed Detection and Response, исключения по процессам не применяются.

Таблица 195. Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять (см. раздел "Окно Доверенный процесс" на стр. 548) и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**. При импорте вам будет предложено заменить список исключений или добавить исключения к уже существующему списку.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Таблица 196. Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Исключения по процессам (см. раздел "Окно Исключения по процессам" на стр. 547).
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, <code>/dir/*/file</code> или <code>/dir/*/*/file</code>. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, <code>/dir/**/file*</code> или <code>/dir/file**/</code>. Маску ** можно использовать в имени директории только один раз. Например, <code>/dir/***/file</code> – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле ввода не должно быть пустым.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром Путь к исключаемому процессу. По умолчанию флажок снят.
Использовать эту область	Флажок включает или выключает исключение этой области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область во время работы. Если флажок снят, приложение включает эту область во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.

Настройка анализа поведения в командной строке

В командной строке вы можете управлять анализом поведения приложений в операционной системе с помощью предустановленной задачи Анализ поведения (*Behavior_Detection*).

Задача Анализ поведения по умолчанию не запущена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачу вручную.

Вы можете настраивать параметры анализа поведения, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи Анализ поведения.

Таблица 197. Параметры задачи Анализ поведения

Параметр	Описание	Значения
TaskMode	Действие, выполняемое приложением при обнаружении вредоносной активности в операционной системе.	Block – завершать процесс приложения, осуществляющего вредоносную активность. Notify (значение по умолчанию) – не завершать процесс, осуществляющий вредоносную активность, только регистрировать обнаружение вредоносной активности в журнале событий.
UseTrustedPrograms	Исключение процессов из проверки.	Yes – исключать из проверки активность указанных процессов. No (значение по умолчанию) – проверять все процессы.
Секция [TrustedPrograms.item_#] содержит процессы, которые исключаются из проверки. Приложение Kaspersky Industrial CyberSecurity for Linux Nodes не контролирует активность указанных процессов.		
ProgramPath	Путь к исключаемому процессу.	<полный путь к процессу> – исключать из проверки процесс в указанной локальной директории. Для указания пути вы можете использовать маски.
ApplyToDescendants	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром ProgramPath.	Yes – исключать из проверки указанный процесс и все его дочерние процессы. No (значение по умолчанию) – исключать из проверки только указанный процесс, не исключать из проверки дочерние процессы.
ProgramDesc	Описание исключаемого процесса.	
UseTrustedProgram	Включение исключения указанного процесса из проверки.	Yes (значение по умолчанию) – включить исключение активности указанного процесса из проверки. No – не включать исключение активности указанного процесса из проверки.

Использование Kaspersky Security Network

Для повышения эффективности защиты устройств и данных пользователей приложение Kaspersky Industrial CyberSecurity for Linux Nodes может использовать облачную базу знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения – Kaspersky Security Network (KSN). Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции на различные угрозы, высокую производительность компонентов защиты и снижение количества ложных срабатываний.

Использование Kaspersky Security Network является добровольным. Вы можете включить или выключить использование KSN в любой момент.

Инфраструктурные решения Kaspersky Security Network

Kaspersky Industrial CyberSecurity for Linux Nodes поддерживает следующие инфраструктурные решения для работы с репутационными базами «Лаборатории Касперского»:

- *Kaspersky Security Network (KSN)* – это решение, которое позволяет получать информацию от "Лаборатории Касперского", а также отправлять в "Лабораторию Касперского" данные об объектах, обнаруженных на устройствах пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.
- *Kaspersky Private Security Network (KPSN)* – это решение, которое позволяет пользователям устройств с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих устройств. KPSN разработан для корпоративных клиентов, не имеющих возможности использовать Kaspersky Security Network, например, по следующим причинам:
 - отсутствие подключения локальных рабочих мест к интернету;
 - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

В сертифицированной версии приложения допускается только использование KPSN. Использование KSN не допускается, так как приводит к выходу приложения из сертифицированного состояния. Рекомендуется использовать KPSN или отказаться от использования KSN.

После активации приложения по новой лицензии для использования KPSN требуется предоставить поставщику услуг информацию о новом лицензионном ключе. В противном случае обмен информацией с KPSN будет невозможен из-за ошибки аутентификации.

Варианты использования Kaspersky Security Network

Существует два варианта использования KSN:

- **Расширенный режим KSN** – вы можете получать информацию из базы знаний "Лаборатории Касперского", при этом приложение Kaspersky Industrial CyberSecurity for Linux Nodes автоматически

отправляет в Kaspersky Security Network статистическую информацию, полученную в результате своей работы. Также приложение может отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или части файлов), которые злоумышленники могут использовать для нанесения вреда устройству или данным.

- **Стандартный режим KSN** – вы можете получать информацию из базы знаний "Лаборатории Касперского", при этом приложение Kaspersky Industrial CyberSecurity for Linux Nodes не отправляет анонимную статистику и данные о типах и источниках угроз.

Вы можете в любой момент выбрать другой вариант использования Kaspersky Security Network.

Сбор, обработка и хранение персональных данных пользователя не производится. 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 с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Облачный режим работы Kaspersky Industrial CyberSecurity for Linux Nodes

Облачный режим – это режим работы приложения Kaspersky Industrial CyberSecurity for Linux Nodes, при котором используется облегченная версия баз вредоносного ПО. Это позволяет снизить нагрузку на оперативную память устройства. Работу приложения с облегченными базами вредоносного ПО обеспечивает Kaspersky Security Network.

Kaspersky Industrial CyberSecurity for Linux Nodes переходит к использованию облегченной версии баз вредоносного ПО после включения облачного режима и выполнения очередного обновления баз и модулей приложения. Если облачный режим выключается, Kaspersky Industrial CyberSecurity for Linux Nodes загружает полную версию баз приложения с серверов "Лаборатории Касперского" в ходе очередного обновления баз и модулей приложения.

Включение облачного режима приводит к выходу приложения из сертифицированного состояния.

Если вы не используете KSN или облачный режим выключен, Kaspersky Industrial CyberSecurity for Linux Nodes использует полную версию баз приложения.

Использование службы прокси-сервера KSN

Устройства пользователей, работающие под управлением Сервера администрирования, могут взаимодействовать с KSN напрямую или при помощи службы прокси-сервера KSN.

Прокси-сервер KSN предоставляет следующие возможности:

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

Параметры прокси-сервера KSN вы можете настроить в свойствах Сервера администрирования. Подробнее о прокси-сервере KSN см. в справке Kaspersky Security Center.

В этом разделе

Настройка использования Kaspersky Security Network в Web Console	552
Настройка использования Kaspersky Security Network в Консоли администрирования	554
Настройка использования Kaspersky Security Network в командной строке	556
Проверка подключения к Kaspersky Security Network с помощью командной строки	557

Настройка использования Kaspersky Security Network в Web Console

В сертифицированной версии приложения допускается только использование KPSN. Использование KSN не допускается, так как приводит к выходу приложения из сертифицированного состояния. Рекомендуется использовать KPSN или отказаться от использования KSN.

В Web Console вы можете настраивать использование Kaspersky Security Network в работе приложения Kaspersky Industrial CyberSecurity for Linux Nodes в политике (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Продвинутая защита** → **Kaspersky Security Network**).

Текст Положения о Kaspersky Security Network вы можете прочитать в окне **Положение о Kaspersky Security Network**, которое можно открыть по ссылке **Положение о Kaspersky Security Network**.

Информация о доступности KSN отображается в Kaspersky Security Center с помощью статуса клиентского устройства (**ОК**, **Критический**, **Предупреждение**) в списке управляемых устройств на закладке **Устройства**.

Таблица 198. Параметры использования Kaspersky Security Network

Параметр	Описание
Не использовать KSN	Выбирая этот вариант, вы отказываетесь от использования Kaspersky Security Network.
Расширенный режим KSN	Выбирая этот вариант, вы принимаете условия использования Kaspersky Security Network. Вы сможете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Кроме того, для улучшения работы Kaspersky Security Network в "Лабораторию Касперского" будет отправляться анонимная статистика и данные о типах и источниках различных угроз.
Стандартный режим KSN	Выбирая этот вариант, вы принимаете условия использования Kaspersky Security Network. Вы сможете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения.

Параметр	Описание
Включить облачный режим	Флажок включает или выключает режим работы, при котором приложение Kaspersky Industrial CyberSecurity for Linux Nodes использует облегченную версию баз вредоносного ПО. Флажок доступен, если включено использование KSN. Включение облачного режима приводит к выходу приложения из сертифицированного состояния. Режим включается или выключается после следующего обновления баз приложения.
Использовать серверы KSN, если прокси-сервер KSN недоступен	Флажок включает или выключает возможность взаимодействовать с серверами KSN напрямую, когда служба прокси-сервера KSN недоступна. По умолчанию флажок установлен.
Положение о Kaspersky Security Network	По ссылке открывается окно Положение о Kaspersky Security Network, в котором вы можете прочитать текст Положения о Kaspersky Security Network.

Положение о Kaspersky Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Security Network и принять его условия.

Таблица 199. Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите использовать Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Security Network.
Я не принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите использовать Kaspersky Security Network.

Положение о Kaspersky Private Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Private Security Network и принять его условия.

Таблица 200. Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите использовать Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Private Security Network.
Я не принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите использовать Kaspersky Security Network.

Настройка использования Kaspersky Security Network в Консоли администрирования

В сертифицированной версии приложения допускается только использование KPSN. Использование KSN не допускается, так как приводит к выходу приложения из сертифицированного состояния. Рекомендуется использовать KPSN или отказаться от использования KSN.

В Консоли администрирования вы можете настраивать использование Kaspersky Security Network в работе приложения Kaspersky Industrial CyberSecurity for Linux Nodes в политике (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Продвинутая защита** → **Kaspersky Security Network**).

Текст Положения о Kaspersky Security Network вы можете прочитать в окне **Положение о Kaspersky Security Network**, которое можно открыть по ссылке **Положение о Kaspersky Security Network**.

Информация о доступности KSN отображается в Kaspersky Security Center с помощью статуса клиентского устройства (*ОК, Критический, Предупреждение*) в списке управляемых устройств на закладке **Устройства**.

Таблица 201. Параметры использования Kaspersky Security Network

Параметр	Описание
Положение о Kaspersky Security Network	По ссылке открывается окно Положение о Kaspersky Security Network . В этом окне вы можете просмотреть текст Положения о Kaspersky Security Network.
Kaspersky Security Network (KSN)	В блоке отображается информация о режиме использования KSN или о том, что KSN не используется в работе Kaspersky Industrial CyberSecurity for Linux Nodes. По кнопке Изменить открывается окно, в котором вы можете настроить использование Kaspersky Security Network (см. раздел "Параметры Kaspersky Security Network" на стр. 555).
Включить облачный режим	Флажок включает или выключает режим работы, при котором приложение Kaspersky Industrial CyberSecurity for Linux Nodes использует облегченную версию баз вредоносного ПО. Флажок доступен, если включено использование KSN. Включение облачного режима приводит к выходу приложения из сертифицированного состояния. Режим включается или выключается после следующего обновления баз приложения.
Использовать серверы KSN, если прокси-сервер KSN недоступен	Флажок включает или выключает возможность взаимодействовать с серверами KSN напрямую, когда служба прокси-сервера KSN недоступна. По умолчанию флажок установлен.

Параметры Kaspersky Security Network

В этом окне вы можете настроить параметры использования Kaspersky Security Network.

Таблица 202. Параметры Kaspersky Security Network

Параметр	Описание
Подробнее...	По ссылке открывается веб-сайт "Лаборатории Касперского".
Не использовать Kaspersky Security Network	Выбирая этот вариант, вы отказываетесь от использования Kaspersky Security Network.
Стандартный режим KSN	Выбирая этот вариант, вы принимаете условия использования Kaspersky Security Network. Вы можете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения.
Расширенный режим KSN	Выбирая этот вариант, вы принимаете условия использования Kaspersky Security Network. Вы можете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Кроме того, для улучшения работы Kaspersky Security Network в "Лабораторию Касперского" будет отправляться анонимная статистика и данные о типах и источниках различных угроз.
Положение о Kaspersky Security Network	По ссылке открывается окно Положение о Kaspersky Security Network (на стр. 555), в котором вы можете прочитать текст Положения о Kaspersky Security Network.

Положение о Kaspersky Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Security Network и принять его условия.

Таблица 203. Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите использовать Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Security Network. Вариант доступен, если в окне Параметры Kaspersky Security Network (на стр. 555) вы выбрали вариант Стандартный режим KSN или Расширенный режим KSN .
Я не принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите использовать Kaspersky Security Network. Вариант доступен, если в окне Параметры Kaspersky Security Network (на стр. 555) вы выбрали вариант Стандартный режим KSN или Расширенный режим KSN .

Положение о Kaspersky Private Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Private Security Network и принять его условия.

Таблица 204. Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите использовать Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Private Security Network.
Я не принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите использовать Kaspersky Security Network.

Настройка использования Kaspersky Security Network в командной строке

В сертифицированной версии приложения допускается только использование KPSN. Использование KSN не допускается, так как приводит к выходу приложения из сертифицированного состояния. Рекомендуется использовать KPSN или отказаться от использования KSN.

В командной строке вы можете включать и выключать использование Kaspersky Security Network с помощью параметра `UseKSN` из общих параметров приложения.

Вы можете изменять значение параметра (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) `UseKSN` с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

- Чтобы включить использование Kaspersky Security Network с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

где:

- `<Extended/Basic>` – режим использования Kaspersky Security Network.
- `--accept-ksn` – ключ, означающий, что вы соглашаетесь с условиями, изложенными в Положении о Kaspersky Security Network. Вы подтверждаете, что полностью прочитали, понимаете и принимаете условия Положения о Kaspersky Security Network.

Файл `ksn_license.<ID языка>` с текстом Положения о Kaspersky Security Network находится в директории `/opt/kaspersky/kics/doc/`.

- Чтобы выключить использование Kaspersky Security Network с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-app-settings UseKSN=No
```

- Чтобы включить или выключить использование Kaspersky Security Network с помощью конфигурационного файла, выполните следующую команду:

```
kics-control --set-app-settings --file <имя конфигурационного файла> [--json] [--accept-ksn]
```

где:

- `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу с общими параметрами приложения, в котором настроено нужное значение параметра `UseKSN`.
- `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.
- `--accept-ksn` – ключ, означающий, что вы соглашаетесь с условиями, изложенными в Положении о Kaspersky Security Network. Ключ требуется указать, если вы включаете использование Kaspersky Security Network.

Если приложение Kaspersky Industrial CyberSecurity for Linux Nodes, установленное на клиентском устройстве, работает под управлением политики, которая была назначена в Kaspersky Security Center, значение параметра `UseKSN` можно изменить только в Kaspersky Security Center. Когда приложение Kaspersky Industrial CyberSecurity for Linux Nodes, установленное на клиентском устройстве, прекращает работать под управлением политики, параметру присваивается значение `UseKSN=No`.

Проверка подключения к Kaspersky Security Network с помощью командной строки

- Чтобы проверить подключение к Kaspersky Security Network, выполните следующую команду:

```
kics-control --app-info
```

В строке **Использование Kaspersky Security Network** отображается статус подключения к Kaspersky Security Network:

- Если отображается статус **Расширенный режим KSN**, приложение Kaspersky Industrial CyberSecurity for Linux Nodes использует Kaspersky Security Network, можно получать информацию из базы знаний, отправляется анонимная статистика и информация о типах и источниках угроз.
- Если отображается статус **Стандартный режим KSN**, приложение Kaspersky Industrial CyberSecurity for Linux Nodes использует Kaspersky Security Network, можно получать информацию из базы знаний, но анонимная статистика и информация о типах и источниках угроз не отправляется.
- Если отображается статус **Выключен**, приложение Kaspersky Industrial CyberSecurity for Linux Nodes не использует Kaspersky Security Network.

В строке **Инфраструктура Kaspersky Security Network** отображается информация об инфраструктурном решении, которое используется для работы с репутационными базами "Лаборатории Касперского":

[Kaspersky Security Network](#) или [Kaspersky Private Security Network](#).

В сертифицированной версии приложения допускается только использование KPSN. Использование KSN не допускается, так как приводит к выходу приложения из сертифицированного состояния. Рекомендуется использовать KPSN или отказаться от использования KSN.

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Устройство пользователя не подключено к интернету.
- Использование Kaspersky Security Network не включено.
- Приложение не активировано, или срок действия лицензии истек.
- Выявлены проблемы, связанные с лицензионным ключом. Например, ключ находится в списке запрещенных ключей.

Дополнительные параметры работы приложения

Вы можете настраивать следующие дополнительные параметры работы приложения:

- Использование прокси-сервера (см. раздел "Настройка прокси-сервера" на стр. [560](#)) в работе приложения.
- Глобальные исключения (см. раздел "Настройка глобальных исключений" на стр. [566](#)) – исключение точек монтирования из перехвата файловых операций для компонентов Защита от файловых угроз, Защита от шифрования, Мониторинг контейнеров и задач Поиск вредоносного ПО, Проверка важных областей, Проверка контейнеров и Проверка съемных дисков.
- Исключение памяти процессов (см. раздел "Исключение памяти процессов из проверки" на стр. [572](#)) из проверки.
- Режим перехвата файловых операций (см. раздел "Выбор режима перехвата файловых операций" на стр. [574](#)).
- Обнаружение легальных приложений (см. раздел "Настройка обнаружения приложений, которые злоумышленники могут использовать для нанесения вреда" на стр. [575](#)), которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
- Отслеживание стабильности работы приложения (см. раздел "Включение мониторинга стабильности работы приложения" на стр. [576](#)).
- Параметры запуска приложения (см. раздел "Настройка параметров запуска приложения" на стр. [577](#)).
- Ограничение на использование памяти и ресурсов процессора (на стр. [578](#)) для задач проверки.
- Ограничение на использование резидентной памяти (см. раздел "Ограничение на использование резидентной памяти приложением" на стр. [580](#)) приложением.
- Ограничение на количество задач выборочной проверки (на стр. [583](#)), которые может одновременно запустить непривилегированный пользователь.
- Параметры отправки информации в хранилище Kaspersky Security Center (см. раздел "Настройка отправки информации в хранилище Kaspersky Security Center" на стр. [583](#)).
- Разрешения на управление задачами (см. раздел "Настройка разрешений на управление задачами" на стр. [584](#)).

В этом разделе

Настройка прокси-сервера	560
Настройка глобальных исключений	566
Исключение памяти процессов из проверки	572
Выбор режима перехвата файловых операций	574
Настройка обнаружения приложений, которые злоумышленники могут использовать для нанесения вреда	575
Включение мониторинга стабильности работы приложения	576
Настройка параметров запуска приложения	577
Ограничение на использование памяти и ресурсов процессора	578
Ограничение на использование резидентной памяти приложением	580
Ограничение на количество задач выборочной проверки	583
Настройка отправки информации в хранилище Kaspersky Security Center	583
Настройка разрешений на управление задачами	584

Настройка прокси-сервера

Вы можете настроить параметры прокси-сервера, если доступ пользователей с клиентских устройств в интернет осуществляется через прокси-сервер. Приложение Kaspersky Industrial CyberSecurity for Linux Nodes может использовать прокси-сервер для подключения к серверам "Лаборатории Касперского", например, при обновлении баз и модулей приложения или при взаимодействии с Kaspersky Security Network и с Kaspersky Industrial CyberSecurity for Networks.

По умолчанию использование прокси-сервера выключено.

В этом разделе

Настройка параметров прокси-сервера в Web Console	560
Настройка параметров прокси-сервера в Консоли администрирования	563
Настройка параметров прокси-сервера в командной строке	566

Настройка параметров прокси-сервера в Web Console

В Web Console вы можете настраивать использование прокси-сервера в политике (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры прокси-сервера**).

Таблица 205. Параметры прокси-сервера

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, прокси-сервер не используется в работе приложения.
Использовать указанные параметры прокси-сервера	Если выбран этот вариант, приложение использует указанные параметры прокси-сервера, например, для интеграции с Kaspersky Industrial CyberSecurity for Networks.
Адрес	Поле для ввода IP-адреса или доменного имени прокси-сервера. Поле доступно, если выбран вариант Использовать указанные параметры прокси-сервера .
Порт	Поле для ввода порта прокси-сервера. Значение по умолчанию: 3128. Поле доступно, если выбран вариант Использовать указанные параметры прокси-сервера .
Использовать аутентификацию на прокси-сервере	Включает или выключает аутентификацию с помощью имени пользователя и пароля при доступе к прокси-серверу. Флажок доступен, если выбран вариант Использовать указанные параметры прокси-сервера. По умолчанию флажок снят. Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.
Имя пользователя	Поле ввода имени пользователя для его аутентификации на прокси-сервере. Поле ввода доступно, если установлен флажок Использовать аутентификацию на прокси-сервере.
Изменить	Позволяет указать пароль пользователя для авторизации на прокси-сервере. Поле Пароль недоступно для редактирования. По умолчанию пароль пустой. Чтобы указать пароль, нажмите на кнопку Изменить, в открывшемся окне введите пароль и нажмите на кнопку ОК. Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев. При нажатии на кнопку Показать в окне ввода пароля пароль отображается в открытом виде. Кнопка доступна, если установлен флажок Использовать аутентификацию на прокси-сервере.

Параметр	Описание
Использовать Kaspersky Security Center в качестве прокси-сервера для активации приложения	Флажок включает или выключает использование Kaspersky Security Center в качестве прокси-сервера при активации приложения. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes использует Kaspersky Security Center в качестве прокси-сервера при активации приложения. По умолчанию флажок снят.

Настройка параметров прокси-сервера в Консоли администрирования

В Консоли администрирования вы можете настраивать использование прокси-сервера в политике (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры прокси-сервера**).

Таблица 206. Параметры прокси-сервера

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, прокси-сервер не используется в работе приложения.
Использовать указанные параметры прокси-сервера	Если выбран этот вариант, приложение использует указанные параметры прокси-сервера, например, для интеграции с Kaspersky Industrial CyberSecurity for Networks.
Адрес и порт	Поля для ввода IP-адреса или доменного имени прокси-сервера и порта прокси-сервера. Порт по умолчанию: 3128. Поля доступны, если выбран вариант Использовать указанные параметры прокси-сервера .
Использовать аутентификацию на прокси-сервере	Флажок включает или выключает аутентификацию с помощью имени пользователя и пароля при доступе к прокси-серверу. Флажок доступен, если выбран вариант Использовать указанные параметры прокси-сервера . По умолчанию флажок снят. Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.
Имя пользователя	Поле ввода имени пользователя для его аутентификации на прокси-сервере. Поле ввода доступно, если установлен флажок Использовать аутентификацию на прокси-сервере .
Пароль	Поле для ввода пароля пользователя для авторизации на прокси-сервере. Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев. При нажатии на кнопку Показать пароль пользователя отображается в поле Пароль в открытом виде. По умолчанию пароль пользователя скрыт и отображается в виде точек. Поле ввода и кнопка доступны, если установлен флажок Использовать аутентификацию на прокси-сервере .
Использовать Kaspersky Security Center в качестве прокси-сервера для активации приложения	Флажок включает или выключает использование Kaspersky Security Center в качестве прокси-сервера при активации приложения. Если флажок установлен, Kaspersky Industrial CyberSecurity for Linux Nodes использует Kaspersky Security Center в качестве прокси-сервера при активации приложения. По умолчанию флажок снят.

Настройка параметров прокси-сервера в командной строке

В командной строке вы можете включать и выключать использование прокси-сервера компонентами приложения с помощью параметров `UseProxy` и `ProxyServer` из общих параметров приложения.

Вы можете изменять значение параметров (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `UseProxy` может принимать следующие значения:

- `Yes` – включить использование прокси-сервера.
- `No` – выключить использование прокси-сервера.

Параметр `ProxyServer` позволяет задавать параметры прокси-сервера в формате `[<пользователь>[:<пароль>]@]<адрес прокси-сервера>[:<порт>]`, где:

- `<пользователь>` – имя пользователя для аутентификации на прокси-сервере.
- `<пароль>` – пароль пользователя для авторизации на прокси-сервере.
- `<адрес прокси-сервера>` – IP-адрес или доменное имя прокси-сервера.
- `<порт>` – порт прокси-сервера.

Если для подключения к прокси-серверу не требуется аутентификация, параметр `ProxyServer` указывать не нужно.

Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.

Настройка глобальных исключений

Вы можете настраивать исключение точек монтирования из перехвата файловых операций для компонентов Защита от файловых угроз (на стр. [172](#)) и Защита от шифрования (см. раздел "Защита от удаленного вредоносного шифрования" на стр. [404](#)), а также из проверки задачами Поиск вредоносного ПО, Проверка важных областей и Проверка контейнеров. Исключение точек монтирования позволяет исключать из перехвата файловых операций локальные или удаленные директории, смонтированные на устройстве. Кроме того, глобальные исключения влияют на работу компонента Мониторинг контейнеров (на стр. [322](#)) и задачи Проверка съемных дисков (на стр. [314](#)).

В этом разделе

Настройка глобальных исключений в Web Console	567
Настройка глобальных исключений в Консоли администрирования	570
Настройка глобальных исключений в командной строке	571

Настройка глобальных исключений в Web Console

В Web Console вы можете настраивать глобальные исключения в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (Параметры приложения → Общие параметры → Глобальные исключения).

Таблица в разделе **Глобальные исключения** содержит точки монтирования, которые будут исключены из перехвата файловых операций. По умолчанию таблица пустая. Элементы в таблице можно добавлять, изменять (см. раздел "Окно добавления исключения точки монтирования" на стр. [568](#)) и удалять.

В столбце **Путь** отображается путь к исключенным точкам монтирования.

Окно добавления исключения точки монтирования

Таблица 207. Параметры точки монтирования

Параметр	Описание
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • Локальная – локальные точки монтирования. • Смонтированная – удаленные директории, смонтированные на устройстве по протоколу Samba или NFS. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательский – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип Смонтированная.
Путь	Поле ввода пути к точке монтирования, которую вы хотите добавить в исключения из перехвата файловых операций. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Локальная.

Параметр	Описание
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из перехвата файловых операций. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке Протокол доступа выбран элемент Пользовательский.

Настройка глобальных исключений в Консоли администрирования

В Консоли администрирования вы можете настраивать глобальные исключения в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Глобальные исключения**).

Блок параметров **Исключенные точки монтирования** содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключенные точки монтирования**.

Список в окне содержит пути к исключенным точкам монтирования. По умолчанию список пуст.

Элементы в списке можно добавлять, изменять (см. раздел "Окно Путь к точке монтирования" на стр. [571](#)), и удалять.

Окно Путь к точке монтирования

Таблица 208. Параметры точки монтирования

Параметр	Описание
Файловая система, протокол доступа и путь	Блок параметров позволяет задать расположение точки монтирования. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • Локальная – локальные точки монтирования. • Смонтированная – удаленные директории, смонтированные на устройстве по протоколу Samba или NFS. • Все удаленные смонтированные – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип Смонтированная , то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • NFS – удаленные директории, смонтированные на устройстве по протоколу NFS. • Samba – удаленные директории, смонтированные на устройстве по протоколу Samba. • Пользовательская – все ресурсы файловой системы устройства, указанной в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип Локальная , то в поле ввода вы можете указать путь к точке монтирования, которую вы хотите добавить в исключения из перехвата файловых операций. Для указания пути вы можете использовать маски.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из перехвата файловых операций. Поле доступно, если в раскрывающемся списке файловых систем выбран тип Смонтированная и в раскрывающемся списке справа выбран элемент Пользовательская .

Настройка глобальных исключений в командной строке

В командной строке вы можете настраивать исключения точек монтирования с помощью параметра `ExcludedMountPoint.item_#` общих параметров приложения. Вы можете изменять значение параметра (см. раздел "Изменение общих параметров приложения" на стр. 139) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `ExcludedMountPoint.item_#` может принимать следующие значения:

- `AllRemoteMounted` – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протоколов SMB и NFS.
- `Mounted:NFS` – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протокола NFS.

- `Mounted:SMB` – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протокола SMB.
- `Mounted:<тип файловой системы>` – исключать из перехвата файловых операций все смонтированные директории с указанным типом файловой системы.
- `/mnt` – исключать из перехвата объекты, находящиеся в точке монтирования `/mnt` (включая вложенные директории), используемой в качестве временной точки монтирования съемных дисков.
- `<путь, содержащий маску /mnt/user* или /mnt/**/user_share>` – исключать из перехвата объекты, находящиеся в точках монтирования, имена которых содержат указанную маску.

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/**/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек).

Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Вы можете указать несколько точек монтирования, которые вы хотите исключить из проверки.

Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды `mount`.

Исключение памяти процессов из проверки

Вы можете настраивать исключения из проверки памяти процессов. Приложение не будет проверять память указанных процессов.

Настройка исключений в Web Console

В Web Console вы можете настраивать исключения памяти процессов из проверки в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры приложения**).

По ссылке **Настроить исключение памяти процессов из проверки** в блоке **Исключение памяти процессов из проверки** открывается окно **Исключение памяти процессов из проверки**, в котором вы можете сформировать список исключений.

Список в окне **Исключение памяти процессов из проверки** содержит пути к процессам, которые приложение исключает из проверки памяти процессов. Для указания пути вы можете использовать маски.

По умолчанию список пуст. Элементы в списке можно добавлять, изменять и удалять.

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/**/*.file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек).

Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Настройка исключений в Консоли администрирования

В Консоли администрирования вы можете настраивать исключения памяти процессов из проверки в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Исключение памяти процессов**).

По кнопке **Настроить** в блоке **Исключение памяти процессов из проверки** открывается окно, в котором вы можете сформировать список исключений.

Список в окне **Исключение памяти процессов из проверки** содержит пути к процессам, которые приложение исключает из проверки памяти процессов. Для указания пути вы можете использовать маски. По умолчанию список пуст. Элементы в списке можно добавлять, изменять и удалять.

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/**/*.file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек).

Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Настройка исключений в командной строке

В командной строке вы можете настраивать исключение памяти процессов из проверки с помощью параметра `MemScanExcludedProgramPath.item_#` в общих параметрах приложения.

Вы можете изменять значение параметра (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `MemScanExcludedProgramPath.item_#` содержит полный путь к процессу в локальной директории. Для указания пути вы можете использовать маски.

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/**/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Вы можете указать несколько процессов, память которых требуется исключить из проверки.

Выбор режима перехвата файловых операций

Режим перехвата файловых операций влияет на работу компонентов Защита от файловых угроз (на стр. [172](#)) и Контроль устройств (на стр. [464](#)).

- Приложение может блокировать на время проверки доступ к файлам, которые проверяет компонент Защита от файловых угроз. Если доступ блокируется, то любое обращение к проверяемому файлу ожидает результатов проверки. Если в результате проверки в файле не обнаружены угрозы, приложение разрешает доступ к файлу. При обнаружении зараженных объектов приложение выполняет действия, указанные в параметрах **Первое действие** (`FirstAction`) и **Второе действие** (`SecondAction`) компонента Защита от файловых угроз.

По умолчанию блокировка доступа к файлам, которые проверяет компонент Защита от файловых угроз, выключена. Проверка выполняется в асинхронном режиме.

- Приложение может блокировать доступ к файлам на устройстве на время, пока компонент Контроль устройств определяет возможность предоставления доступа к устройству. Если доступ блокируется, то любое обращение к файлам на контролируемом устройстве ожидает результатов проверки. Приложение разрешает доступ к файлам, если в результате проверки Контроль устройств разрешает доступ к устройству с файлами.

По умолчанию блокировка доступа к файлам на устройстве, которое контролирует компонент Контроль устройств, выключена. Контроль устройств определяет возможность предоставления доступа к устройству в асинхронном режиме.

Настройка в Web Console

В Web Console вы можете настраивать режим перехвата файловых операций в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Режим перехвата файловых операций**).

Флажок **Блокировать доступ к файлам во время проверки** включает или выключает блокировку доступа к файлам на время проверки компонентами Защита от файловых угроз и Контроль устройств.

По умолчанию флажок снят. На время проверки обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.

Если флажок установлен, на время проверки обращение к любому файлу блокируется.

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать режим перехвата файлов в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры приложения**, блок **Режим перехвата файловых операций**).

Флажок **Блокировать доступ к файлам во время проверки** включает или выключает блокировку доступа к файлам на время проверки компонентами Защита от файловых угроз и Контроль устройств.

По умолчанию флажок снят. На время проверки обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.

Если флажок установлен, на время проверки обращение к любому файлу блокируется.

Настройка в командной строке

В командной строке вы можете настраивать режим перехвата файловых операций с помощью параметра `FileBlockDuringScan` в общих параметрах приложения.

Вы можете изменять значение параметра (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `FileBlockDuringScan` может принимать следующие значения:

- **Yes** – блокировать доступ к файлам на время проверки компонентами Защита от файловых угроз и Контроль устройств.
- **No** (значение по умолчанию) – не блокировать доступ к файлам на время проверки. Обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.

Настройка обнаружения приложений, которые могут использовать злоумышленники для нанесения вреда

Вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.

Настройка в Web Console

В Web Console вы можете включать и выключать обнаружение легальных приложений, которые могут использовать злоумышленники для нанесения вреда устройствам или данным, в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Параметры проверки**).

Флажок **Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным** включает или выключает обнаружение легальных приложений, через которые злоумышленники могут навредить устройству или данным пользователя.

По умолчанию флажок снят.

Настройка в Консоли администрирования

В Консоли администрирования вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным, в свойствах

политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры приложения**, блок **Параметры проверки**).

Флажок **Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным** включает или выключает обнаружение легальных приложений, через которые злоумышленники могут навредить устройству или данным пользователя.

По умолчанию флажок снят.

Настройка в командной строке

В командной строке вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным, с помощью параметра `DetectOtherObjects` в общих параметрах приложения.

Вы можете изменять значение параметра (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `DetectOtherObjects` может принимать следующие значения:

- **Yes** – включить обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
- **No** – не включать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.

Включение мониторинга стабильности работы приложения

Вы можете включать и выключать мониторинг стабильности работы приложения Kaspersky Industrial CyberSecurity for Linux Nodes, который позволяет отслеживать количество нештатных остановок приложения и уведомлять администратора о нестабильной работе приложения.

Настройка в Web Console

В Web Console вы можете включать и выключать мониторинг стабильности работы приложения в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Дополнительные параметры приложения**).

Флажок **Включить мониторинг стабильности работы приложения** включает или выключает отслеживание состояния работы приложения Kaspersky Industrial CyberSecurity for Linux Nodes. По умолчанию флажок снят.

Для применения параметра требуется перезапустить приложение.

Если приложение работает нестабильно, в свойствах устройства с установленным приложением отображается сообщение: *<Количество> нештатных остановок приложения начиная с <дата и время>.*

Настройка в Консоли администрирования

В Консоли администрирования вы можете включать и выключать мониторинг стабильности работы приложения в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры приложения**, блок **Дополнительные параметры приложения**).

Флажок **Включить мониторинг стабильности работы приложения** включает или выключает отслеживание состояния работы приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

По умолчанию флажок снят.

Для применения параметра требуется перезапустить приложение.

Если приложение работает нестабильно, в свойствах устройства с установленным приложением отображается сообщение: *<Количество> нештатных остановок приложения начиная с <дата и время>.*

Настройка в командной строке

В командной строке вы можете настроить мониторинг стабильности работы приложения с помощью параметров `TrackProductCrashes`, `ProductHealthLogFile`, `WarnThreshold`, `WarnAfter_#_crash` и `WarnRemovingThreshold` в конфигурационном файле `kics.ini` (см. раздел "Предустановленные конфигурационные файлы" на стр. [702](#)).

Параметр `TrackProductCrashes` позволяет включить или выключить мониторинг стабильности работы приложения. Параметр может принимать следующие значения:

- `Yes/true` – включить мониторинг стабильности работы приложения.
- `No/false` – не включать мониторинг стабильности работы приложения.

Параметр `ProductHealthLogFile` позволяет задать путь к файлу, с помощью которого осуществляется мониторинг стабильности приложения. Значение по умолчанию:
`/var/opt/kaspersky/kics/private/kics_health.log`.

Параметр `WarnThreshold` позволяет задать интервал времени (в секундах), за который приложение должно посчитать количество нештатных остановок, прежде чем вывести уведомление о нестабильной работе. Значение по умолчанию: 3600 секунд.

Параметр `WarnRemovingThreshold` позволяет задать интервал времени (в секундах), по истечении которого статус о нестабильной работе приложения будет снят. Значение по умолчанию: 86400 секунд.

Параметр `WarnAfter_#_crash` позволяет задать количество нештатных остановок приложения, необходимых для отображения уведомления о нестабильной работе приложения. Параметр может принимать значения от 0 до 10. Значение по умолчанию: 10. Если указано значение 0, уведомление о нестабильной работе приложения не отображается.

Настройка параметров запуска приложения

Вы можете настраивать параметры запуска приложения.

Настройка ограничения в Web Console

В Web Console вы можете настраивать параметры запуска приложения в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (Параметры приложения → Общие параметры → Параметры приложения, блок Параметры запуска приложения).

Таблица 209. Параметры запуска приложения

Параметр	Описание
Максимальное количество неудачных последовательных попыток запуска приложения	Поле ввода максимального количества неудачных последовательных попыток запуска приложения. Значение по умолчанию: 5.
Максимальное время ожидания запуска приложения (мин.)	Поле ввода максимального времени ожидания запуска приложения (в минутах), после которого процесс kics будет перезапущен. Значение по умолчанию: 3.

Настройка ограничения в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры запуска приложения в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры приложения**, блок **Параметры запуска приложения**).

В блоке **Параметры запуска приложения** по нажатию на кнопку **Настроить** открывается окно **Параметры запуска приложения**, в котором вы можете настроить параметры запуска приложения (см. таблицу ниже).

Таблица 210. Параметры запуска приложения

Параметр	Описание
Максимальное количество неудачных последовательных попыток запуска приложения	Поле ввода максимального количества неудачных последовательных попыток запуска приложения. Значение по умолчанию: 5.
Максимальное время ожидания запуска приложения (мин.)	Поле ввода максимального времени ожидания запуска приложения (в минутах), после которого процесс kics будет перезапущен. Значение по умолчанию: 3.

Настройка ограничения в командной строке

В командной строке вы можете настраивать параметры запуска приложения с помощью параметров `MaxRestartCount` и `StartupTimeout` в конфигурационном файле `kics.ini` (см. раздел "Предустановленные конфигурационные файлы" на стр. [702](#)).

Параметр `MaxRestartCount` позволяет задать максимальное количество неудачных последовательных попыток запуска приложения. Параметр может принимать значения от 1 до 10. Значение по умолчанию: 5.

Параметр `StartupTimeout` позволяет задать максимальное время ожидания запуска приложения в минутах, после которого процесс `kics` будет перезапущен. Параметр может принимать значения от 1 до 60. Значение по умолчанию: 3.

Ограничение на использование памяти и ресурсов процессора

Вы можете настраивать ограничение на использование ресурсов процессора для задач проверки. По умолчанию ограничение не установлено. Также вы можете настраивать ограничение на использование памяти для задач проверки. По умолчанию установлено ограничение 8192 мегабайт.

Настройка ограничения в Web Console

В Web Console вы можете включать и выключать ограничение на использование ресурсов процессора и настраивать ограничение на использование памяти для задач проверки в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Производительность**).

Таблица 211. Параметры

Параметр	Описание
Ограничение на использование памяти для задач проверки (МБ)	Поле ввода ограничения на использование памяти для задач проверки (в мегабайтах). Значение по умолчанию: 8192.
Ограничить потребление ресурсов процессора для задач проверки	Флажок включает или выключает ограничение на использование ресурсов процессора для задач Поиск вредоносного ПО, Проверка важных областей, Инвентаризация и Проверка контейнеров. Если флажок установлен, максимальная нагрузка на все ядра процессора при работе этих задач не превышает значения, указанного в поле Максимальное значение (%) . По умолчанию флажок снят.

Настройка ограничения в Консоли администрирования

В Консоли администрирования вы можете включать и выключать ограничение на использование ресурсов процессора и настраивать ограничение на использование памяти для задач проверки в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры приложения**, блок **Производительность**).

В блоке **Производительность** по нажатию на кнопку **Настроить** открывается окно **Потребление ресурсов процессора и памяти**, в котором вы можете настроить ограничения (см. таблицу ниже).

Таблица 212. Параметры

Параметр	Описание
Ограничить потребление ресурсов процессора для задач проверки (%)	Флажок включает или выключает ограничение на использование ресурсов процессора для задач Поиск вредоносного ПО, Проверка важных областей, Инвентаризация и Проверка контейнеров. Если флажок установлен, максимальная нагрузка на все ядра процессора при работе этих задач не превышает значения в процентах, указанного в поле справа. По умолчанию флажок снят.
Ограничение на использование памяти для задач проверки (МБ)	Поле ввода ограничения на использование памяти для задач проверки (в мегабайтах). Значение по умолчанию: 8192.

Настройка ограничения в командной строке

В командной строке вы можете настраивать ограничение на использование ресурсов процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan* с помощью параметров `UseOnDemandCPULimit` и `OnDemandCPULimit` в общих параметрах приложения.

Вы можете изменять значение параметров (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `UseOnDemandCPULimit` может принимать следующие значения:

- `Yes` – включить ограничение потребления ресурсов процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan*.
- `No` – выключить ограничение потребления ресурсов процессора для задач.

Параметр `OnDemandCPULimit` позволяет задать максимальное значение нагрузки на все ядра процессора (в процентах) при работе задач типа *ODS*, *ContainerScan* и *InventoryScan*. Параметр может принимать значения от 10 до 100. Значение по умолчанию 100.

В командной строке вы можете настраивать ограничение на использование памяти для задач типа *ODS*, *ContainerScan* и *InventoryScan* с помощью параметра `ScanMemoryLimit` в конфигурационном файле `kics.ini` (см. раздел "Предустановленные конфигурационные файлы" на стр. [702](#)). Значение по умолчанию: 8192.

Ограничение на использование резидентной памяти приложением

Вы можете настраивать ограничение на использование резидентной памяти приложением. По умолчанию установлено автоматическое ограничение.

Настройка ограничения в Web Console

В Web Console вы можете настраивать ограничение на использование резидентной памяти приложением в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Дополнительные параметры приложения**).

В блоке **Дополнительные параметры приложения** по ссылке **Настроить использование памяти** открывается окно, в котором вы можете настроить ограничение на использование резидентной памяти (см. таблицу ниже).

Таблица 213. Параметры

Параметр	Описание
Использование резидентной памяти приложением	В раскрывающемся списке вы можете выбрать способ ограничения на использование резидентной памяти: • Не ограничено. При выборе этого элемента списка использование резидентной памяти не ограничивается. • Ограничено значением в процентах от общего объема. При выборе этого элемента списка становится доступно поле Ограничение на использование памяти (%), в котором вы можете указать нужное значение в процентах. • Ограничено значением в мегабайтах. При выборе этого элемента списка становится доступно поле Ограничение на использование памяти (МБ), в котором вы можете указать нужное значение в мегабайтах. • Ограничено наименьшим из указанных значений (% , МБ). При выборе этого элемента списка становятся доступны поля Ограничение на использование памяти (%) и Ограничение на использование памяти (МБ), в которых вы можете указать нужные значения. • Ограничено наибольшим из указанных значений (% , МБ). При выборе этого элемента списка становятся доступны поля Ограничение на использование памяти (%) и Ограничение на использование памяти (МБ), в которых вы можете указать нужные значения. • Ограничивается автоматически (рекомендуется). При выборе этого элемента списка использование резидентной памяти ограничивается автоматически (значение по умолчанию).
Ограничение на использование памяти (%)	Поле ввода ограничения на использование памяти (в процентах). Значение по умолчанию: 50.
Ограничение на использование памяти (МБ)	Поле ввода ограничения на использование памяти (в мегабайтах). Значение по умолчанию: 2000.

Настройка ограничения в Консоли администрирования

В Консоли администрирования вы можете настраивать ограничение на использование резидентной памяти приложением в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры приложения**).

В блоке **Дополнительные параметры приложения** по нажатию на кнопку **Настроить** открывается окно **Дополнительные параметры**, в котором вы можете настроить ограничение на использование резидентной памяти (см. таблицу ниже).

Таблица 214. Параметры

Параметр	Описание
Использование памяти приложением	В раскрывающемся списке вы можете выбрать способ ограничения на использование резидентной памяти: • Не ограничено. При выборе этого элемента списка использование резидентной памяти не ограничивается. • Ограничивается автоматически (рекомендуется). При выборе этого элемента списка использование резидентной памяти ограничивается автоматически (значение по умолчанию). • Ограничено значением в процентах от общего объема. При выборе этого элемента списка становится доступно поле Ограничение на использование памяти (%), в котором вы можете указать нужное значение в процентах. • Ограничено значением в мегабайтах. При выборе этого элемента списка становится доступно поле Ограничение на использование памяти (МБ), в котором вы можете указать нужное значение в мегабайтах. • Ограничено наименьшим из указанных значений (% , МБ). При выборе этого элемента списка становятся доступны поля Ограничение на использование памяти (%) и Ограничение на использование памяти (МБ), в которых вы можете указать нужные значения. • Ограничено наибольшим из указанных значений (% , МБ). При выборе этого элемента списка становятся доступны поля Ограничение на использование памяти (%) и Ограничение на использование памяти (МБ), в которых вы можете указать нужные значения.
Ограничение на использование памяти (%)	Поле ввода ограничения на использование памяти (в процентах). Значение по умолчанию: 50.
Ограничение на использование памяти (МБ)	Поле ввода ограничения на использование памяти (в мегабайтах). Значение по умолчанию: 2000.

Настройка ограничения в командной строке

В командной строке вы можете настраивать ограничение на использование резидентной памяти приложением с помощью параметра `MaxMemory` в конфигурационном файле `kics.ini` (см. раздел "Предустановленные конфигурационные файлы" на стр. [702](#)).

Параметр `MaxMemory` может принимать следующие значения:

- `off` – использование резидентной памяти не ограничено.
- `<значение>%` – значение от 1 до 100 в процентах от объема памяти.
- `<значение>MB` – значение в мегабайтах.
- `lowest/<значение>%/<значение>MB` – наименьшее значение между значением в процентах и значением в мегабайтах.
- `highest/<значение>%/<значение>MB` – наибольшее значение между значением в процентах и значением в мегабайтах.

- `auto` (значение по умолчанию) – до 50% доступной памяти, но не менее 2 ГБ и не более 16 ГБ.

Ограничение на количество задач выборочной проверки

Вы можете настраивать ограничение на количество задач выборочной проверки (см. раздел "Выборочная проверка файлов и директорий" на стр. [265](#)), которые может одновременно запустить на устройстве непривилегированный пользователь. Количество задач, которые может запустить пользователь с root-правами, не ограничивается.

Вы можете включать и выключать ограничение на количество одновременно запущенных задач выборочной проверки в командной строке с помощью параметра `LimitNumberOfScanFileTasks` из общих параметров приложения.

Вы можете изменять значение параметра (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `LimitNumberOfScanFileTasks` может принимать значения от 0 до 4294967295. Значение по умолчанию: 0.

Если задано значение 0, непривилегированный пользователь не может запускать задачи выборочной проверки.

Если во время установки приложения вы установили пакет графического интерфейса, для параметра `LimitNumberOfScanFileTasks` по умолчанию используется значение 5.

Настройка отправки информации в хранилище Kaspersky Security Center

В Kaspersky Security Center вы можете включать и выключать отправку в хранилище Kaspersky Security Center информации о необработанных файлах и о подключенных устройствах.

Информация о необработанных файлах отображается в списке активных угроз в Web Console (**Операции** → **Хранилища** → **Активные угрозы**) и в Консоли администрирования (**Дополнительно** → **Хранилища** → **Активные угрозы**).

Информация об устройствах, установленных на клиентском устройстве или подключенных к нему, отображается в списке оборудования в Web Console (**Операции** → **Хранилища** → **Оборудование**) и в Консоли администрирования (**Дополнительно** → **Хранилища** → **Оборудование**). Информация передается, если включен Контроль устройств (на стр. [464](#)).

Включение и выключение отправки информации в Web Console

В Web Console вы можете включать и выключать отправку информации в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры Хранилища**).

Таблица 215. Параметры отправки информации в хранилище Kaspersky Security Center

Параметр	Описание
Информирование о необработанных файлах включено / выключено	Переключатель включает или выключает отправку уведомлений о файлах, необработанных во время проверки, на Сервер администрирования. По умолчанию переключатель включен.
Информирование об установленных устройствах включено / выключено	Переключатель включает или выключает передачу на Сервер администрирования информации об устройствах, установленных на клиентском устройстве или подключенных к нему. По умолчанию переключатель включен.

Включение и выключение отправки информации в Консоли администрирования

В Консоли администрирования вы можете включать и выключать отправку информации в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры Хранилища**).

Таблица 216. Параметры отправки информации в хранилище Kaspersky Security Center

Параметр	Описание
Информировать о необработанных файлах	Флажок включает или выключает отправку уведомлений о файлах, необработанных во время проверки, на Сервер администрирования. По умолчанию флажок установлен.
Информировать об установленных устройствах	Флажок включает или выключает передачу на Сервер администрирования информации об устройствах, установленных на клиентском устройстве или подключенных к нему. По умолчанию флажок установлен.

Настройка разрешений на управление задачами

В Kaspersky Security Center вы можете настраивать следующие разрешения для пользователей:

- разрешение на просмотр задач, созданных в приложении Kaspersky Industrial CyberSecurity for Linux Nodes;
- разрешение на просмотр на клиентских устройствах задач, созданных в Kaspersky Security Center.

Настройка в Web Console

В Web Console вы можете настраивать разрешение на просмотр задач в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Локальные задачи** → **Управление задачами**).

Таблица 217. Параметры управления задачами

Параметр	Описание
Разрешить пользователям просмотр и управление локальными задачами	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в приложении Kaspersky Industrial CyberSecurity for Linux Nodes, и управление этими задачами на управляемых клиентских устройствах. По умолчанию флажок снят.
Разрешить пользователям просмотр и управление задачами, созданными через KSC	Флажок разрешает или запрещает пользователям просмотр задач, созданных через Kaspersky Security Center Web Console, и управление этими задачами на управляемых клиентских устройствах. По умолчанию флажок снят.

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать разрешение на просмотр задач в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Локальные задачи** → **Управление задачами**).

Таблица 218. Параметры управления задачами

Параметр	Описание
Разрешить пользователям просмотр и управление локальными задачами	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в приложении Kaspersky Industrial CyberSecurity for Linux Nodes, и управление этими задачами на управляемых клиентских устройствах. По умолчанию флажок снят.
Разрешить пользователям просмотр и управление задачами, созданными через KSC	Флажок разрешает или запрещает пользователям просмотр задач, созданных через Kaspersky Security Center, и управление этими задачами на управляемых клиентских устройствах. По умолчанию флажок снят.

Резервное хранилище

Если во время проверки защищенного устройства Kaspersky Industrial CyberSecurity for Linux Nodes обнаруживает в файле вредоносный код, приложение может заблокировать этот файл, присвоить ему статус *Заражен*, поместить его копию в резервное хранилище и попытаться провести лечение файла.

Резервное хранилище – это хранилище резервных копий файлов, которые были удалены или изменены в процессе лечения. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Если файл удастся вылечить, то статус резервной копии файла изменяется на *Вылечен*. Иногда при лечении файлов не удастся 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 вылеченной копии в директорию исходного размещения файла.

Рекомендуется восстанавливать файлы из резервных копий только в том случае, если им присвоен статус *Вылечен*. Восстановление зараженных объектов может привести к заражению устройства.

Резервные копии файлов в резервном хранилище могут содержать персональные данные. Для доступа к объектам резервного хранилища требуются root-права.

Вы можете настраивать следующие параметры резервного хранилища:

- Время хранения объектов в резервном хранилище. По умолчанию объекты хранятся 90 суток.
- Максимальный размер резервного хранилища. По умолчанию размер резервного хранилища не ограничен.
- Путь к резервному хранилищу. По умолчанию резервное хранилище расположено в директории `/var/opt/kaspersky/kics/common/objects-backup/`.

По истечении заданного времени или при достижении максимального размера резервного хранилища приложение автоматически удаляет из резервного хранилища резервные копии файлов с любым статусом.

Также вы можете самостоятельно удалить резервную копию как восстановленного, так и невосстановленного файла.

Общий список файлов, помещенных в резервное хранилище приложениями "Лаборатории Касперского" на клиентских устройствах, формируется в Kaspersky Security Center и доступен в Консоли администрирования (**Дополнительно** → **Хранилища** → **Резервное хранилище**) и в Web Console (**Операции** → **Хранилища** → **Резервное хранилище**). Вы можете просматривать свойства файлов, находящихся в резервных хранилищах на защищенных устройствах, запускать проверку на наличие вредоносного ПО в резервном хранилище и удалять из него файлы. Kaspersky Security Center не копирует файлы из резервных хранилищ на Сервер администрирования, все файлы размещаются в резервных хранилищах на защищенных устройствах. Восстановление файлов выполняется на защищенном устройстве.

В этом разделе

Настройка параметров резервного хранилища в Web Console	587
Настройка параметров резервного хранилища в Консоли администрирования	587
Настройка параметров резервного хранилища в командной строке	588
Работа с объектами резервного хранилища в командной строке	589

Настройка параметров резервного хранилища в Web Console

В Web Console вы можете настраивать параметры резервного хранилища в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры Хранилища**).

Таблица 219. Параметры резервного хранилища

Параметр	Описание
Информирование о файлах в резервном хранилище включено / выключено	Переключатель включает или выключает отправку уведомлений о файлах в резервном хранилище на Сервер администрирования. По умолчанию переключатель включен.
Хранить объекты не более (дней)	Поле ввода для указания периода хранения объектов в резервном хранилище. Доступные значения: 0–3653. Значение по умолчанию: 90. Если задано значение 0, период хранения объектов в резервном хранилище не ограничен.
Ограничить размер резервного хранилища до (МБ)	Поле ввода для указания максимального размера резервного хранилища (в мегабайтах). Доступные значения: 0–999999. Значение по умолчанию: 0 (размер резервного хранилища не ограничен).

Настройка параметров резервного хранилища в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры резервного хранилища в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры Хранилища**).

Таблица 220. Параметры резервного хранилища

Параметр	Описание
Информировать о файлах в резервном хранилище	Флажок включает или выключает отправку уведомлений о файлах в резервном хранилище на Сервер администрирования. По умолчанию флажок установлен.
Хранить объекты не более (дней)	Флажок включает или выключает ограничение срока хранения объектов в резервном хранилище заданным интервалом времени. Доступные значения: 0–3653. Значение по умолчанию: 90. Если задано значение 0, период хранения объектов в резервном хранилище не ограничен.
Ограничить размер резервного хранилища до (МБ)	Флажок включает или выключает ограничение максимального размера резервного хранилища заданным значением (в мегабайтах). Доступные значения: 0–999999. Значение по умолчанию: 0 (размер резервного хранилища не ограничен).

Настройка параметров резервного хранилища в командной строке

В командной строке вы можете настраивать параметры резервного хранилища с помощью предустановленной задачи Управление резервным хранилищем (*Backup*).

Задача Управление резервным хранилищем по умолчанию запущена. Вы не можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры резервного хранилища, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи Управление резервным хранилищем.

Таблица 221. Параметры задачи Управление резервным хранилищем

Параметр	Описание	Значение
DaysToLive	Интервал времени, в течение которого объекты хранятся в резервном хранилище (в сутках). Чтобы снять ограничение на время хранения объектов в резервном хранилище, укажите значение 0.	0 – время хранения объектов в резервном хранилище не ограничено. Значение по умолчанию: 90.
BackupSizeLimit	Максимальный размер резервного хранилища (в мегабайтах). При достижении максимального размера резервного хранилища, приложение удаляет самые старые объекты. Чтобы снять ограничение на размер резервного хранилища, укажите значение 0.	0 – 999999 0 – размер резервного хранилища не ограничен. Значение по умолчанию: 0.
BackupFolder	Путь к директории резервного хранилища. Вы можете указать в качестве резервного хранилища пользовательскую директорию, отличную от директории, заданной по умолчанию. В качестве резервного хранилища можно использовать директории на любых устройствах. Не рекомендуется указывать директории, расположенные на удаленных устройствах, например смонтированных по протоколам Samba и NFS. Приложение начинает перемещать объекты в выбранную директорию после изменения параметров и перезапуска приложения. Если указанной директории не существует или она недоступна, приложение использует директорию, заданную по умолчанию.	Значение по умолчанию: /var/opt/kaspersky/kics/common/objects-backup/ Для доступа к заданной по умолчанию директории резервного хранилища требуются root-права.

Работа с объектами резервного хранилища в командной строке

В командной строке с помощью команд управления резервным хранилищем (см. раздел «Команды управления резервным хранилищем» на стр. [696](#)) вы можете выполнять следующие действия с объектами резервного хранилища:

- Просматривать информацию об объектах резервного хранилища.
- Удалять из резервного хранилища все или только указанные объекты.

- Восстанавливать объекты из резервного хранилища.

Восстановление зараженных объектов может привести к заражению устройства.

Просмотр информации об объектах резервного хранилища

- Чтобы просмотреть информацию об объектах резервного хранилища, выполните следующую команду:

```
kics-control -B --query ["<условия фильтра>"] [-n <количество>] [--json]
```

где:

- <условия фильтра> – одно или несколько логических выражений (см. раздел "Использование фильтра для ограничения результатов запросов" на стр. 140) в формате <поле> <операция сравнения> '<значение>', скомбинированных с помощью логического оператора and, для ограничения результатов запроса. Если вы не укажете условия фильтра, приложение выведет информацию обо всех объектах резервного хранилища.
- <количество> – количество последних объектов из хранилища, которые нужно вывести. Если вы не укажете ключ -n, будут выведены последние 30 объектов. Чтобы показать все объекты, укажите значение 0.
- --json – выводить данные в формате JSON.

В строке `ObjectId` отобразится числовой идентификатор, который приложение присвоило объекту при помещении в резервное хранилище. Этот идентификатор используется для выполнения действий над объектом, таких как восстановление или удаление объекта из резервного хранилища.

Восстановление объектов из резервного хранилища

- Чтобы восстановить объект с исходным именем в исходное местоположение, выполните следующую команду:

```
kics-control --restore <идентификатор объекта>
```

где <идентификатор объекта> – числовой идентификатор, который приложение присвоило объекту при помещении в резервное хранилище.

- Чтобы восстановить объект с новым именем в указанную директорию, выполните следующую команду:

```
kics-control --restore <идентификатор объекта> --file <имя и путь к файлу>
```

где --file <имя и путь к файлу> – новое имя файла и путь к директории, в которой вы хотите его сохранить. Если указанной директории не существует, приложение создает ее.

Удаление объектов из резервного хранилища

- Чтобы удалить выбранные объекты из резервного хранилища, выполните следующую команду:

```
kics-control --mass-remove --query "<условия фильтра>"
```

где <условия фильтра> – одно или несколько логических выражений (см. раздел "Использование фильтра для ограничения результатов запросов" на стр. [140](#)) в формате <поле> <операция сравнения> '<значение>', скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.

Примеры:

Чтобы удалить объект с ID=15:

```
kics-control -B --mass-remove --query "ObjectId == '15'"
```

Чтобы удалить объекты, в названии которых или в пути к которым содержится "test":

```
kics-control -B --mass-remove --query "FileName like '%test%'"
```

- Чтобы удалить все объекты из резервного хранилища, выполните следующую команду:

```
kics-control -B --mass-remove
```

Интеграция с Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks – приложение для защиты инфраструктуры промышленных предприятий от угроз информационной безопасности и для обеспечения непрерывности технологических процессов. Kaspersky Industrial CyberSecurity for Networks анализирует трафик промышленной сети для выявления отклонений в значениях технологических параметров, обнаружения признаков сетевых атак, контроля работы и текущего состояния устройств в сети. Приложение входит в состав решения Kaspersky Industrial CyberSecurity.

Интеграция приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Industrial CyberSecurity for Networks расширяет возможности по расследованию и реагированию на угрозы в сетях промышленных предприятий. Если интеграция с Kaspersky Industrial CyberSecurity for Networks включена, данные о событиях на устройстве, полученные приложением Kaspersky Industrial CyberSecurity for Linux Nodes, отправляются на сервер интеграции Kaspersky Industrial CyberSecurity for Networks.

При взаимодействии с Kaspersky Industrial CyberSecurity for Networks приложение Kaspersky Industrial CyberSecurity for Linux Nodes может выполнять следующие действия, направленные на обеспечение функций безопасности:

- Отправлять данные о событиях на устройствах (телеметрию) на сервер интеграции Kaspersky Industrial CyberSecurity for Networks. Приложение Kaspersky Industrial CyberSecurity for Linux Nodes передает на сервер интеграции данные наблюдения за процессами, открытыми сетевыми соединениями и изменяемыми файлами, а также данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.
- Выполнять задачи проверки устройства на уязвимости, контроля оборудования на устройстве и сбора конфигураций на устройстве по командам, полученным от сервера интеграции.

Для интеграции с Kaspersky Industrial CyberSecurity for Networks должен быть включен компонент приложения Kaspersky Industrial CyberSecurity for Linux Nodes Анализ поведения (на стр. [544](#)).

Интеграция приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Industrial CyberSecurity for Networks возможна, только если включен компонент Анализ поведения. В противном случае необходимые данные телеметрии не передаются.

Дополнительно Kaspersky Industrial CyberSecurity for Networks может использовать данные, полученные от следующих компонентов:

- Защита от файловых угроз (на стр. [172](#)).
- Защита от сетевых угроз (на стр. [398](#)).
- Защита от веб-угроз (на стр. [378](#)).
- Защита от шифрования (см. раздел "Защита от удаленного вредоносного шифрования" на стр. [404](#)).
- Контроль приложений (на стр. [431](#)).
- Контроль устройств (на стр. [464](#)).
- Контроль целостности системы (на стр. [516](#)).

Подробнее о Kaspersky Industrial CyberSecurity for Networks см. в справке Kaspersky Industrial CyberSecurity for Networks.

Во время интеграции с Kaspersky Industrial CyberSecurity for Networks устройства с Kaspersky Industrial CyberSecurity for Linux Nodes устанавливают защищенные соединения с сервером интеграции по протоколу HTTPS. Для обеспечения безопасности соединения используются следующие сертификаты, выданные сервером Kaspersky Industrial CyberSecurity for Networks:

- Сертификат сервера интеграции. Использование сертификата сервера является обязательным условием для обеспечения безопасного соединения с сервером интеграции. Вам нужно добавить сертификат сервера интеграции перед включением интеграции с Kaspersky Industrial CyberSecurity for Networks.
- Сертификат клиента. Этот сертификат используется для дополнительной защиты подключения с помощью двусторонней аутентификации клиентов сервера интеграции, которыми являются устройства с Kaspersky Industrial CyberSecurity for Linux Nodes. Один и тот же сертификат клиента может использоваться несколькими устройствами. По умолчанию сервер интеграции не выполняет проверку сертификатов клиентов, но проверка может быть включена на стороне сервера интеграции для усиления защиты соединения. В этом случае вам нужно включить использование сертификата клиента в параметрах интеграции и добавить сертификат клиента (криптоконтейнер с сертификатом и закрытым ключом).

Сертификаты для защиты соединения с сервером интеграции предоставляет администратор Kaspersky Industrial CyberSecurity for Networks.

Для подключения к Kaspersky Industrial CyberSecurity for Networks используется прокси-сервер, если использование прокси-сервера настроено (см. раздел "Настройка прокси-сервера" на стр. [560](#)) в общих параметрах приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

По умолчанию интеграция с Kaspersky Industrial CyberSecurity for Networks выключена. Вы можете включать и выключать интеграцию, а также настраивать параметры интеграции с помощью Web Console (см. раздел "Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в Web Console" на стр. [594](#)), Консоли администрирования (см. раздел "Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в Консоли администрирования" на стр. [598](#)) и командной строки (см. раздел "Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в командной строке" на стр. [603](#)):

- Настраивать общие параметры подключения к серверам интеграции Kaspersky Industrial CyberSecurity for Networks.
- Добавлять и удалять сертификаты серверов интеграции.
- Настраивать двустороннюю аутентификацию при подключении к серверам интеграции и добавлять сертификаты клиента.
- Настраивать параметры отправки событий.
- Включать и выключать отправку телеметрии.

В этом разделе

Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в Web Console	594
Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в Консоли администрирования	598
Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в командной строке	603

Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в Web Console

В Web Console вы можете включать и выключать интеграцию приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Industrial CyberSecurity for Networks и настраивать параметры интеграции в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Detection and Response** → **Интеграция с KICS for Networks**).

Таблица 222. Параметры интеграции с Kaspersky Industrial CyberSecurity for Networks

Параметр	Описание
Интеграция с KICS for Networks включена/выключена	Включает или выключает интеграцию приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Industrial CyberSecurity for Networks. По умолчанию интеграция выключена.
Параметры подключения к серверам интеграции	По ссылке Настроить открывается окно (см. раздел "Окно настройки параметров подключения к серверу интеграции" на стр. 595), в котором вы можете настроить общие параметры подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверу интеграции.
Серверы интеграции KICS for Networks	Таблица содержит список серверов интеграции Kaspersky Industrial CyberSecurity for Networks, к которым настроено подключение. По кнопке Добавить открывается окно (см. раздел "Окно подключения к серверу интеграции" на стр. 598), в котором вы можете настроить подключение к серверу интеграции. С помощью кнопок над таблицей вы можете изменять и удалять ранее настроенные параметры подключения.
Максимальная задержка отправки событий (сек.)	Максимальная задержка отправки событий на сервер интеграции в секундах. Значение по умолчанию: 30.
Максимальное количество событий в одном пакете	Максимальное количество событий в одном пакете. Значение по умолчанию: 1024.
Периодичность опроса серверов (сек.)	Периодичность опроса серверов интеграции в секундах. Значение по умолчанию: 450.
Включить регулирование количества событий	Включает или выключает регулирование количества событий, отправляемых на сервер интеграции.
Максимальное количество событий в час	Максимальное количество событий в час. Значение по умолчанию: 3000.
Процент превышения лимита событий	Процент превышения лимита событий. Передача событий ограничивается, если соотношение событий одного типа (например, событий изменений в реестре) к общему количеству событий превышает указанное ограничение в процентах. Значение по умолчанию: 15.

В этом разделе

Окно настройки параметров подключения к серверу интеграции	595
Окно подключения к серверу интеграции.....	598

Окно настройки параметров подключения к серверу интеграции

В этом окне вы можете настроить общие параметры подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверу интеграции.

Таблица 223. *Параметры подключения к серверу интеграции Kaspersky Industrial CyberSecurity*

Параметр	Описание
Отправлять запрос на синхронизацию на сервер интеграции каждые (мин.)	Периодичность отправки запросов на синхронизацию на сервер интеграции в минутах. Значение по умолчанию: 5.
Максимальное время ожидания соединения с сервером (сек.)	Максимальное время ожидания соединения с сервером интеграции в секундах. Значение по умолчанию: 10.
Максимальное время ожидания ответа от сервера (сек.)	Максимальное время ожидания ответа от сервера интеграции в секундах. Значение по умолчанию: 10.
Разрешить отправку телеметрии	Включает или выключает отправку данных о событиях на устройствах (телеметрии) на сервер интеграции. По умолчанию отправка телеметрии включена.
Сертификат сервера	После добавления сертификата сервера интеграции отображается информация о сертификате: • серийный номер сертификата; • субъект сертификата; • издатель сертификата; • дата начала срока действия сертификата; • дата окончания срока действия сертификата.
Выбрать	Открывает стандартное окно выбора файла, в котором вы можете указать путь к сертификату сервера интеграции. Использование сертификата сервера является обязательным условием для обеспечения безопасного соединения с сервером интеграции.
Удалить	Удаляет ранее добавленный сертификат сервера интеграции. Кнопка отображается только если сертификат сервера добавлен.
Дополнительная защита подключения	Блок параметров позволяет включить или выключить двустороннюю аутентификацию при подключении к серверу интеграции и добавить сертификат клиента.
Использовать двустороннюю аутентификацию	Включает или выключает использование двусторонней аутентификации для дополнительной защиты соединения с сервером интеграции. Двусторонняя аутентификация должна быть включена на стороне сервера интеграции Kaspersky Industrial CyberSecurity for Networks. Чтобы использовать двустороннюю аутентификацию, вам нужно добавить сертификат клиента.
Добавить сертификат клиента	Открывает стандартное окно выбора файла, в котором вы можете указать путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ. Кнопка доступна, если установлен флажок Использовать двустороннюю аутентификацию .

Параметр	Описание
Изменить	Позволяет указать пароль криптоконтейнера с сертификатом клиента. Поле Пароль криптоконтейнера недоступно для редактирования. По умолчанию пароль пустой. Чтобы указать пароль, нажмите на кнопку Изменить, в открывшемся окне введите пароль и нажмите на кнопку ОК. При нажатии на кнопку Показать в окне ввода пароля пароль отображается в открытом виде. Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев. Кнопка доступна, если установлен флажок Использовать двустороннюю аутентификацию.

Окно подключения к серверу интеграции

В этом окне вы можете указать параметры подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks.

Таблица 224. Параметры подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks

Параметр	Описание
Адрес	Адрес сервера интеграции Kaspersky Industrial CyberSecurity for Networks. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером интеграции не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера. Значение по умолчанию: 127.0.0.1.
Порт	Порт для подключения к серверу интеграции. Значение по умолчанию: 8081.

Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в Консоли администрирования

В Консоли администрирования вы можете включать и выключать интеграцию приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Industrial CyberSecurity for Networks и настраивать параметры интеграции в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Detection and Response** → **Интеграция с KICS for Networks**).

Таблица 225. Параметры интеграции с Kaspersky Industrial CyberSecurity for Networks

Параметр	Описание
Включить интеграцию с KICS for Networks	Включает или выключает интеграцию приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Industrial CyberSecurity for Networks. По умолчанию интеграция выключена.
Серверы интеграции KICS for Networks	По кнопке Настроить открывается окно Серверы интеграции KICS for Networks (см. раздел "Окно Серверы интеграции KICS for Networks" на стр. 599). В этом окне вы можете настраивать подключение к серверам интеграции Kaspersky Industrial CyberSecurity for Networks, а также просматривать список серверов, к которым настроено подключение.
Параметры подключения к серверам интеграции	По кнопке Настроить открывается окно (см. раздел "Окно Параметры подключения к серверам интеграции" на стр. 600), в котором вы можете настроить общие параметры подключения к серверам интеграции Kaspersky Industrial CyberSecurity for Networks, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверам интеграции.
Параметры передачи данных	По кнопке Настроить открывается окно (см. раздел "Окно Параметры передачи данных" на стр. 602), в котором вы можете настроить параметры передачи данных на серверы интеграции.

В этом разделе

Окно Серверы интеграции KICS for Networks	599
Окно Сервер интеграции KICS for Networks.....	600
Окно Параметры подключения к серверам интеграции.....	600
Окно Добавление сертификата	602
Окно Добавление сертификата	602
Окно Параметры передачи данных	602

Окно Серверы интеграции KICS for Networks

В этом окне в таблице отображается список параметров подключения к серверам интеграции Kaspersky Industrial CyberSecurity for Networks. Для каждого сервера, к которому настроено подключение, в таблице указывается IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера и порт.

С помощью кнопок и меню над таблицей вы можете выполнить следующие действия:

- Добавить (см. раздел "Окно Сервер интеграции KICS for Networks" на стр. [600](#)) параметры подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks.
- Изменить или удалить ранее настроенные параметры подключения.
- Экспортировать или импортировать список настроенных параметров подключения.

Окно Сервер интеграции KICS for Networks

В этом окне вы можете указать параметры подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks.

Таблица 226. Параметры подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks

Параметр	Описание
Адрес	Адрес сервера интеграции. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером интеграции не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера. Значение по умолчанию: 127.0.0.1.
Порт	Порт для подключения к серверу интеграции. Значение по умолчанию: 8081.

Окно Параметры подключения к серверам интеграции

В этом окне вы можете настроить общие параметры подключения к серверам интеграции Kaspersky Industrial CyberSecurity for Networks.

Таблица 227. Параметры подключения к серверам интеграции Kaspersky Industrial

Параметр	Описание
Отправлять запрос на синхронизацию на сервер интеграции каждые (мин.)	Периодичность отправки запросов на синхронизацию на сервер интеграции в минутах. Значение по умолчанию: 5.
Максимальное время ожидания соединения с сервером (сек.)	Максимальное время ожидания соединения с сервером интеграции в секундах. Значение по умолчанию: 10.
Максимальное время ожидания ответа от сервера (сек.)	Максимальное время ожидания ответа от сервера интеграции в секундах. Значение по умолчанию: 10.
Разрешить отправку телеметрии	Включает или выключает отправку данных о событиях на устройствах (телеметрии) на сервер интеграции. По умолчанию отправка телеметрии включена.
Использовать двустороннюю аутентификацию	Включает или выключает использование двусторонней аутентификации для дополнительной защиты соединения с сервером интеграции. Чтобы использовать двустороннюю аутентификацию, вам нужно добавить сертификат клиента. Двусторонняя аутентификация должна быть включена на стороне сервера интеграции Kaspersky Industrial CyberSecurity for Networks.
Добавить (сертификат клиента)	Открывает окно добавления сертификата клиента (см. раздел "Окно Добавление сертификата" на стр. 602) для дополнительной защиты соединения с сервером интеграции. Кнопка отображается, если сертификат клиента еще не добавлен. Если вы хотите настроить дополнительную защиту соединения, вам нужно включить проверку сертификатов клиентов на стороне сервера интеграции Kaspersky Industrial CyberSecurity for Networks и установить флажок Использовать двустороннюю аутентификацию в этом окне.
Удалить (сертификат клиента)	Удаляет сертификат клиента. Кнопка отображается, если сертификат клиента добавлен.
Добавить (сертификат сервера)	Открывает окно добавления сертификата сервера. Кнопка отображается, если сертификат сервера еще не добавлен. Использование сертификата сервера является обязательным условием для обеспечения безопасного соединения с сервером интеграции.
Удалить (сертификат сервера)	Удаляет сертификат сервера. Кнопка отображается, если сертификат сервера добавлен.

Окно Добавление сертификата

В этом окне вы можете добавить сертификат клиента для дополнительной защиты соединения с сервером интеграции Kaspersky Industrial CyberSecurity for Networks.

Если вы хотите настроить дополнительную защиту соединения, вам нужно включить проверку сертификатов клиентов на стороне сервера интеграции Kaspersky Industrial CyberSecurity for Networks и установить флажок **Использовать двустороннюю аутентификацию** в окне настройки параметров подключения к серверам (см. раздел "Окно Параметры подключения к серверам интеграции" на стр. 600).

Чтобы добавить сертификат клиента, укажите путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ. По кнопке **Обзор** открывается стандартное окно для выбора файла. Если архив защищен паролем, введите пароль в поле **Пароль криптоконтейнера**.

Окно Добавление сертификата

В этом окне вы можете добавить или заменить сертификат сервера интеграции Kaspersky Industrial CyberSecurity for Networks.

Вы можете добавить или заменить сертификат сервера одним из следующих способов:

- Указать путь к файлу сертификата в поле **Добавить из файла**. По кнопке **Обзор** открывается стандартное окно для выбора файла. Укажите путь к файлу, содержащему сертификат формата DER или PEM.
- Скопировать содержимое файла сертификата в поле **Ввести данные сертификата**.

Если сертификат сервера добавлен, выполняется проверка сертификата сервера на стороне Kaspersky Industrial CyberSecurity for Linux Nodes, это позволяет повысить уровень безопасности соединения.

Окно Параметры передачи данных

В этом окне вы можете настроить параметры передачи данных на серверы интеграции Kaspersky Industrial CyberSecurity for Networks.

Таблица 228. Параметры передачи данных на серверы интеграции Kaspersky Industrial

Параметр	Описание
Максимальная задержка отправки событий (сек.)	Максимальная задержка отправки событий на сервер интеграции в секундах. Значение по умолчанию: 30.
Максимальное количество событий в пакете	Максимальное количество событий в одном пакете. Значение по умолчанию: 1024.
Периодичность опроса серверов (сек.)	Периодичность опроса серверов интеграции в секундах. Значение по умолчанию: 450.
Включить регулирование количества событий	Включает или выключает регулирование количества событий, отправляемых на сервер интеграции.
Максимальное количество событий в час	Максимальное количество событий в час. Значение по умолчанию: 3000.
Процент превышения лимита событий	Процент превышения лимита событий. Передача событий ограничивается, если соотношение событий одного типа (например, событий изменений в реестре) к общему количеству событий превышает установленное ограничение в процентах. Значение по умолчанию: 15.

Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks в командной строке

В командной строке вы можете управлять интеграцией приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Industrial CyberSecurity for Networks с помощью предустановленной задачи *Интеграция с Kaspersky Industrial CyberSecurity for Networks (KICS4Networks_Integration)*. По умолчанию задача Интеграция с Kaspersky Industrial CyberSecurity for Networks не запущена. Вы можете запускать и останавливать (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) эту задачу вручную.

Вы можете настраивать параметры (см. раздел "Параметры задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks" на стр. [604](#)) интеграции с Kaspersky Industrial CyberSecurity for Networks, изменяя (см. раздел "Изменение параметров задачи в командной строке" на стр. [129](#)) параметры предустановленной задачи.

С помощью команд управления параметрами интеграции с Kaspersky Industrial CyberSecurity for Networks (см. раздел "Команды управления параметрами интеграции с Kaspersky Industrial CyberSecurity for Networks" на стр. [698](#)) вы можете управлять сертификатами, которые используются для подключения к серверам интеграции Kaspersky Industrial CyberSecurity for Networks.

Использование сертификата сервера является обязательным условием для обеспечения безопасного соединения с сервером интеграции. Вам нужно добавить сертификат сервера (см. раздел "Управление сертификатами для подключения к серверу интеграции" на стр. [607](#)) перед запуском задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks.

В этом разделе

Параметры задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks.....	604
Управление сертификатами для подключения к серверу интеграции	607

Параметры задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks

В таблице ниже описаны все доступные параметры и значения по умолчанию для всех параметров, которые вы можете указать для задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks.

Таблица 229. Параметры задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks

Параметр	Описание	Значение
Address	Адрес сервера интеграции Kaspersky Industrial CyberSecurity for Networks. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером интеграции не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера.	Значение по умолчанию: 127.0.0.1.
Port	Порт для подключения к серверу интеграции.	Значение по умолчанию: 8081.
UseClientPinne dCertificate	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks. Если проверка сертификата клиента включена на стороне сервера интеграции, вам нужно включить использование сертификата клиента и добавить сертификат клиента (см. раздел "Управление сертификатами для подключения к серверу интеграции" на стр. 607) перед запуском задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks.	Yes – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks. No (значение по умолчанию) – не использовать двустороннюю аутентификацию.
Synchronizatio nPeriod	Периодичность отправки запросов на синхронизацию на сервер интеграции в минутах.	Значение по умолчанию: 5.
ConnectionTimeo ut	Максимальное время ожидания соединения с сервером интеграции в секундах.	Значение по умолчанию: 10.
RequestTimeout	Максимальное время ожидания ответа от сервера интеграции в секундах.	Значение по умолчанию: 10.
EnableTelemetry	Включение и выключение отправки данных о событиях на устройствах (телеметрии) на сервер интеграции.	Yes (значение по умолчанию) – отправлять телеметрию на сервер интеграции. No – не отправлять телеметрию.
Секция [EventTransferSettings] содержит параметры передачи событий на сервер интеграции Kaspersky Industrial CyberSecurity for Networks.		
MaximumDataTransf erTime	Максимальная задержка отправки событий на сервер интеграции.	Значение по умолчанию: 30.

Параметр	Описание	Значение
UseRequestCountLimits	Включение и выключение регулирования количества событий, отправляемых на сервер интеграции.	Yes (значение по умолчанию) – регулировать количество отправляемых событий. No – не регулировать количество событий.
MaximumNumberOfEventsInHour	Максимальное количество событий в час.	Значение по умолчанию: 3000.
EventLimitExceededPercentage	Процент превышения лимита событий. Передача событий ограничивается, если соотношение событий одного типа к общему количеству событий превышает установленное ограничение в процентах.	Значение по умолчанию: 15.
PingPeriod	Периодичность опроса серверов интеграции в секундах.	Значение по умолчанию: 450.

Управление сертификатами для подключения к серверу интеграции

Для управления сертификатами требуются root-права.

Вы можете управлять сертификатами, которые используются для подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks, с помощью команд. Вы можете выполнять следующие действия с сертификатами:

- добавлять или заменять сертификат сервера;
- выводить информацию о сертификате сервера;
- удалять сертификат сервера;
- добавлять или заменять сертификат клиента;
- выводить информацию о сертификате клиента;
- удалять сертификат клиента.

► Чтобы добавить или заменить сертификат сервера, выполните следующую команду:

```
kics-control [-K] --add-kics4networks-server-certificate <имя и путь к файлу>
```

где <имя и путь к файлу> – имя и путь к файлу, содержащему сертификат сервера формата DER или PEM.

Сертификат сервера используется для защиты соединения с сервером интеграции, если в параметрах задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks (см. раздел "Параметры задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks" на стр. 604) для параметра UseServerCertificate установлено значение yes.

► *Чтобы добавить или заменить сертификат клиента:*

1. Выполните команду:

```
kics-control [-K] --add-kics4networks-client-certificate <имя и путь к файлу>
```

где <имя и путь к файлу> – имя и путь к архиву формата PFX, содержащему сертификат клиента.

2. Введите пароль к архиву по запросу.

Сертификат клиента используется для дополнительной защиты соединения с сервером интеграции, если в параметрах сервера интеграции включена проверка сертификата клиента и в параметрах задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks (см. раздел "Параметры задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks" на стр. 604) для параметра UseClientCertificate установлено значение yes.

► *Чтобы вывести информацию о сертификате, выполните следующую команду:*

- для сертификата сервера:

```
kics-control [-K] --query-kics4networks-server-certificate
```

- для сертификата клиента:

```
kics-control [-K] --query-kics4networks-client-certificate
```

В результате выполнения команды выводится следующая информация о сертификате:

- серийный номер сертификата;
- субъект сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- SHA1 и SHA256 отпечатки сертификата.

► *Чтобы удалить сертификат сервера, выполните следующую команду:*

```
kics-control [-K] --remove-kics4networks-server-certificate
```

► *Чтобы удалить сертификат клиента, выполните следующую команду:*

```
kics-control [-K] --remove-kics4networks-client-certificate
```


Если использование сертификата настроено в параметрах задачи Интеграция с Kaspersky Industrial CyberSecurity for Networks и задача запущена, удаление этого сертификата завершается с ошибкой.

Интеграция с Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum – решение, предназначенное для защиты IT-инфраструктуры организации от таких угроз, как эксплойты (англ. exploits), программы-вымогатели (англ. ransomware), бесфайловые атаки (англ. fileless attacks) и использование злоумышленниками законных системных инструментов для нанесения вреда устройствам или данным.

Kaspersky Endpoint Detection and Response Optimum выполняет мониторинг и анализ развития угрозы, а также предоставляет сотруднику службы безопасности или администратору информацию о потенциальной атаке (см. раздел "Просмотр информации об обнаруженной угрозе и действиях по реагированию" на стр. [617](#)), необходимую для принятия своевременных действий по реагированию.

Интеграцию приложения Kaspersky Industrial CyberSecurity for Linux Nodes с решением Kaspersky Endpoint Detection and Response Optimum обеспечивает компонент приложения Kaspersky Industrial CyberSecurity for Linux Nodes – Endpoint Detection and Response Optimum (далее также EDR Optimum).

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes 1.5 совместимо с решением Kaspersky Endpoint Detection and Response Optimum версии 3.0.

В составе Kaspersky Industrial CyberSecurity for Linux Nodes версии ниже 1.5 компонент EDR Optimum отсутствует.

Kaspersky Endpoint Detection and Response Optimum использует следующие средства анализа угроз:

- Инфраструктура облачных служб Kaspersky Security Network (далее также KSN), предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-сайтов и программного обеспечения.
- Интеграция с порталом Kaspersky Threat Intelligence Portal <https://opentip.kaspersky.com/>, который содержит и отображает информацию о репутации файлов и веб-сайтов.
- База угроз "Лаборатории Касперского" Kaspersky Threats <https://threats.kaspersky.com/>.

При взаимодействии с Kaspersky Endpoint Detection and Response Optimum приложение Kaspersky Industrial CyberSecurity for Linux Nodes может выполнять следующие функции:

- Отправлять в Kaspersky Security Center данные о событиях на устройствах. Приложение Kaspersky Industrial CyberSecurity for Linux Nodes передает в Kaspersky Security Center данные наблюдения за процессами, открытыми сетевыми соединениями и изменяемыми файлами, а также данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.
- Выполнять ответные действия (см. раздел "Об ответных действиях по командам" на стр. [612](#)), направленные на обеспечение функций безопасности, по командам, полученным от Kaspersky Security Center.

Интеграция с Kaspersky Endpoint Detection and Response Optimum состоит из следующих этапов:

1. Включение необходимых компонентов Kaspersky Industrial CyberSecurity for Linux Nodes

Убедитесь, что следующие компоненты Kaspersky Industrial CyberSecurity for Linux Nodes включены и работают:

- Защита от файловых угроз (на стр. [172](#)).

- Защита от веб-угроз (на стр. [378](#)).
- Анализ поведения (на стр. [544](#)).

2. Включение средств анализа угроз

Убедитесь, что включен Kaspersky Security Network в стандартном или расширенном режиме.

Для наиболее эффективной работы Kaspersky Endpoint Detection and Response Optimum рекомендуется использовать Kaspersky Security Network в расширенном режиме.

3. Активация компонента EDR Optimum

Убедитесь, что соблюдено одно из следующих условий:

- Вы используете приложение Kaspersky Industrial CyberSecurity for Linux Nodes по лицензии, которая включает функциональность Kaspersky Endpoint Detection and Response Optimum.
- Вы приобрели отдельную лицензию на использование функциональности Kaspersky Endpoint Detection and Response Optimum и добавили в приложение (см. раздел "Активация приложения и управление лицензионными ключами" на стр. [154](#)) дополнительный лицензионный ключ EDR Optimum.

4. Включение интеграции с решением Kaspersky Endpoint Detection and Response Optimum

По умолчанию интеграция Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Endpoint Detection and Response Optimum выключена. Вы можете включать и выключать интеграцию, а также настраивать параметры интеграции:

- с помощью Web Console (см. раздел "Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console" на стр. [614](#));
- с помощью командной строки (см. раздел "Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в командной строке" на стр. [615](#)).

Управление компонентом EDR Optimum с помощью Консоли администрирования Kaspersky Security Center не поддерживается.

Вы можете проверить статус работы компонента EDR Optimum:

- С помощью *Отчета о статусе компонентов приложения* в Web Console.
В список компонентов Kaspersky Industrial CyberSecurity for Linux Nodes добавлен компонент **Endpoint Detection and Response Optimum**. Подробную информацию о работе с отчетами см. в справке Kaspersky Security Center (<https://support.kaspersky.com/KSCLinux/15.1/ru-RU/index.htm>).
- В свойствах устройства в Web Console (см. раздел "Просмотр статуса интеграции с Kaspersky Endpoint Detection and Response Optimum" на стр. [616](#)).
- С помощью командной строки (см. раздел "Просмотр статуса интеграции с Kaspersky Endpoint Detection and Response Optimum" на стр. [616](#)).

5. Включение передачи данных на Сервер администрирования

Для использования всех возможностей Kaspersky Endpoint Detection and Response Optimum вам нужно включить следующие параметры:

- **Информирование о файлах в резервном хранилище включено/выключено.**

Вы можете включить этот параметр в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) в разделе **Параметры приложения** → **Общие параметры** → **Параметры Хранилища**.

Включив этот параметр, вы разрешите передачу в Kaspersky Security Center информации о файлах, помещенных приложением Kaspersky Industrial CyberSecurity for Linux Nodes в резервное хранилище на устройстве.

- **Показать EDR-алерты.**

Вы можете включить этот параметр в главном окне Web Console в разделе **Параметры** → **Параметры интерфейса**.

Включив этот параметр, вы разрешите отображение списка алертов.

Параметр **Показать EDR-алерты** отсутствует в Web Console версии ниже 15.1.

В этом разделе

Об ответных действиях по командам	612
Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum	614
Просмотр статуса интеграции с Kaspersky Endpoint Detection and Response Optimum	616
Просмотр информации об обнаруженной угрозе и действиях по реагированию	617
Поиск индикаторов компрометации	617
Требования к IOC-файлам	619
Включение и выключение сетевой изоляции устройства	622
Настройка исключений из сетевой изоляции	626
Запуск процесса	629
Завершение процесса	631
Получение файла с устройства	634
Удаление файла с устройства	635

Об ответных действиях по командам

При взаимодействии с решением Kaspersky Endpoint Detection and Response Optimum приложение Kaspersky Industrial CyberSecurity for Linux Nodes может выполнять ответные действия, направленные на обеспечение функций безопасности.

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes может выполнять следующие ответные действия:

- Получать файлы с устройств.

Действие выполняется с помощью задачи *Получение файла с устройства* (Get file task). Например, вы можете настроить получение файла журнала событий, который создает сторонняя программа.

- Удалять файлы с устройств.

Действие выполняется с помощью задачи *Удаление файла с устройства* (Delete file task).

- Удаленно запускать процессы на устройствах.

Действие выполняется с помощью задачи *Запуск процесса* (Run process).

Например, вы можете удаленно запустить утилиту, которая создает файл с конфигурацией устройства, а затем получить созданный файл с помощью задачи *Получение файла с устройства*.

- Удаленно завершать процессы на устройствах.

Действие выполняется с помощью задачи *Завершение процесса* (Terminate process).

Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи запуска процесса.

- Обнаруживать *индикаторы компрометации* на устройствах и выполнять действия по реагированию на угрозы.

Действие выполняется с помощью задачи *Поиск IOC* (IOC Scan).

При выполнении задачи *Поиск IOC* проверка по IOC-терминам (свойствам IOC-объекта, например, хеш-сумме файла) выполняется только в основном пространстве имен операционной системы. Задача *Поиск IOC* не вычисляет хеш-суммы файлов размером более 200 МБ.

- Включать и выключать сетевую изоляцию устройства.

При взаимодействии Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Endpoint Detection and Response Optimum вы можете:

- Включать и выключать сетевую изоляцию в Web Console (см. раздел "Включение и выключение сетевой изоляции устройства" на стр. [622](#)).
- Выключать сетевую изоляцию в командной строке (см. раздел "Выключение сетевой изоляции устройства в командной строке" на стр. [625](#)).
- Настроить автоматическое выключение сетевой изоляции в Web Console (см. раздел "Настройка автоматического выключения сетевой изоляции" на стр. [623](#)).

Ограничения сетевой изоляции

При использовании сетевой изоляции настоятельно рекомендуется ознакомиться с ограничениями, описанными ниже.

Для работоспособности сетевой изоляции требуется, чтобы приложение Kaspersky Industrial CyberSecurity for Linux Nodes было запущено. Во время сбоя в работе приложения Kaspersky Industrial CyberSecurity for Linux Nodes (когда приложение не запущено), блокировка трафика при включении сетевой изоляции решением Kaspersky Endpoint Detection and Response Optimum не гарантируется.

Транзитный трафик при включенной сетевой изоляции поддерживается с ограничениями и может фильтроваться.

DHCP и DNS в исключения из сетевой изоляции автоматически не добавляются, поэтому если сетевой адрес какого-то ресурса был изменен во время сетевой изоляции, приложение Kaspersky Industrial CyberSecurity for Linux Nodes не сможет получить к нему доступ.

Прокси-сервер также в исключения из сетевой изоляции автоматически не добавляется, при необходимости вы можете добавить его в исключения вручную.

Добавление процесса в сетевую изоляцию и исключение процесса из сетевой изоляции по имени не поддерживается.

При использовании сетевой изоляции рекомендуется:

- Использовать прокси-сервер KSN для взаимодействия с Kaspersky Security Network.
- Использовать Kaspersky Security Center в качестве прокси-сервера для активации приложения.
В случае невозможности использования Kaspersky Security Center в качестве прокси-сервера настройте параметры нужного прокси-сервера и добавьте его в исключения.
- Указать Kaspersky Security Center в качестве источника обновлений баз.

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum

Вы можете включать и выключать интеграцию с Kaspersky Endpoint Detection and Response Optimum:

- с помощью Web Console (см. раздел "Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console" на стр. [614](#));
- с помощью командной строки (см. раздел "Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в командной строке" на стр. [615](#)).

Управление параметрами интеграции с Kaspersky Endpoint Detection and Response Optimum через Консоль администрирования не поддерживается.

В этом разделе

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console	614
Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в командной строке.....	615

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console

В Web Console вы можете включать и выключать интеграцию приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Endpoint Detection and Response Optimum и настраивать параметры интеграции:

- в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response Optimum**);
- в свойствах устройства (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → **Приложения** → ссылка <название приложения Kaspersky Industrial CyberSecurity for Linux Nodes> → **Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response Optimum**).

Включение и выключение интеграции приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Endpoint Detection and Response Optimum в свойствах устройства недоступно, если на устройство распространяется действие политики.

Таблица 230. Параметры интеграции с Kaspersky Endpoint Detection and Response Optimum

Параметр	Описание
Endpoint Detection and Response Optimum включен/выключен	Включает или выключает интеграцию приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Endpoint Detection and Response Optimum. По умолчанию интеграция выключена.
Сетевая изоляция	По ссылке Настроить разблокировку устройства открывается окно Настройка разблокировки устройства , в котором вы можете настроить длительность блокировки устройства.
Исключения	По ссылке Исключения открывается окно Исключения (см. раздел "Добавление и удаление исключений из сетевой изоляции в свойствах политики в Web Console" на стр. 627), в котором вы можете настроить исключения сетевой изоляции.

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в командной строке

В командной строке вы можете включать и выключать интеграцию с Kaspersky Endpoint Detection and Response Optimum с помощью параметра `UseEdrOptimum` в общих параметрах приложения.

Вы можете изменять значение параметра (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

- Чтобы включить интеграцию с Kaspersky Endpoint Detection and Response Optimum с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-app-settings UseEdrOptimum=Yes
```

- Чтобы выключить интеграцию с Kaspersky Endpoint Detection and Response Optimum с помощью ключей командной строки, выполните следующую команду:

```
kics-control --set-app-settings UseEdrOptimum=No
```

Просмотр статуса интеграции с Kaspersky Endpoint Detection and Response Optimum

Просмотр статуса интеграции в Web Console

Вы можете посмотреть статус интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console, выбрав раздел **Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → **Приложения** → ссылка <название приложения Kaspersky Industrial CyberSecurity for Linux Nodes> → **Общие** → **Компоненты**.

Просмотр статуса интеграции в командной строке

Вы можете посмотреть статус интеграции с Kaspersky Endpoint Detection and Response Optimum с помощью командной строки, выполнив команду `kics-control --app-info`.

Статусы интеграции

Для компонента EDR Optimum отображается один из следующих статусов:

- *Выполняется.*

Этот статус отображается при одновременном соблюдении следующих условий:

- добавлен лицензионный ключ, необходимый для работы EDR Optimum;
- текущая дата не превышает дату окончания срока действия лицензии;
- один или несколько компонентов Kaspersky Industrial CyberSecurity for Linux Nodes, необходимых для работы EDR Optimum, включены;
- на устройстве включена интеграция с Kaspersky Endpoint Detection and Response Optimum.

- *Остановлена.*

Этот статус отображается в следующих случаях:

- интеграция с Kaspersky Endpoint Detection and Response Optimum выключена;
- приложение Kaspersky Industrial CyberSecurity for Linux Nodes остановлено.

- *Не поддерживается лицензией.*

Этот статус отображается в следующих случаях:

- текущая дата превышает дату окончания срока действия лицензии;
- действующая лицензия не включает функциональность EDR Optimum.

- *Ошибка.*

Этот статус отображается при одновременном соблюдении следующих условий:

- текущая дата не превышает дату окончания срока действия лицензии;
- в работе одного или нескольких компонентов Kaspersky Industrial CyberSecurity for Linux Nodes, необходимых для работы EDR Optimum, произошла ошибка.

Просмотр информации об обнаруженной угрозе и действиях по реагированию

Для просмотра всей информации об обнаруженной угрозе и выполнения действий по реагированию на эту угрозу вы можете воспользоваться окном с деталями алерта, которое содержит:

- граф цепочки развития угрозы;
- рекомендации по реагированию на угрозу с возможностью выполнения выбранного действия;
- общую информацию об обнаружении угрозы (например, о режиме обнаружения);
- информацию о защищаемом устройстве;
- информацию об обнаруженном объекте;
- историю появления файлов на устройстве;
- информацию о выполненных приложением действиях по реагированию на обнаруженную угрозу.

Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm).

Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Industrial CyberSecurity for Linux Nodes автоматически удаляет старые записи.

Поиск индикаторов компрометации

Вы можете выполнять поиск индикаторов компрометации на устройстве, а также выполнять действия по реагированию на угрозы с помощью задачи *Поиск IOC*.

Для поиска индикаторов компрометации Kaspersky Industrial CyberSecurity for Linux Nodes использует IOC-файлы, подготовленные пользователем. IOC-файлы должны соответствовать требованиям к IOC-файлам (см. раздел "Требования к IOC-файлам" на стр. [619](#)).

Вы можете создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)) задачу *Поиск IOC*, а также изменять (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) ее параметры в Web Console:

- в разделе **Активы (Устройства)** → **Задачи**;
- в разделе **Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → **Задачи**;
- в окне с деталями алерта (см. раздел "Просмотр информации об обнаруженной угрозе и действиях по реагированию" на стр. [617](#)).

Вы не можете создавать, запускать или настраивать задачу *Поиск IOC* с помощью командной строки.

Просмотр задачи *Поиск IOC*, созданной в Web Console, недоступен по команде `kics-control --get-task-list` в командной строке.

Для этой задачи функция Wake-on-LAN в параметрах расписания недоступна. Убедитесь, что устройство включено для выполнения задачи.

Таблица 231. Параметры задачи Поиск ИОС

Параметр	Описание
Переопределить ИОС-файлы	При нажатии на кнопку открывается панель Переопределить ИОС-файлы . При нажатии на кнопку Добавить ИОС-файлы , расположенную в панели Переопределить ИОС-файлы , открывается окно, с помощью которого вы можете выбрать на устройстве и загрузить ИОС-файлы, необходимые для поиска индикаторов компрометации. После загрузки ИОС-файлов вы можете просмотреть список индикаторов из ИОС-файлов.
Экспортировать ИОС-коллекцию	При нажатии на кнопку выполняется скачивание ИОС-файлов на устройство.
Применять действия по реагированию при обнаружении ИОС	Флажок включает или выключает применение действий по реагированию при обнаружении индикаторов компрометации. Если флажок установлен, то при обнаружении индикаторов компрометации приложение выполняет выбранные вами действия: Изолировать устройство от сети. Если флажок установлен, то при обнаружении индикаторов компрометации приложение изолирует устройство от сети для предотвращения распространения угрозы. Вы можете настроить время изоляции (см. раздел "Настройка автоматического выключения сетевой изоляции" на стр. 623). Запускать проверку важных областей. Если флажок установлен, то при обнаружении индикаторов компрометации приложение запускает задачу <i>Проверка важных областей</i>. По умолчанию Kaspersky Industrial CyberSecurity for Linux Nodes проверяет память ядра, запущенные процессы и загрузочные секторы. Если флажок снят, то при обнаружении индикаторов компрометации приложение не выполняет действия по реагированию. Информация об обнаружении индикаторов компрометации отображается в окне с деталями алерта (см. раздел "Просмотр информации об обнаруженной угрозе и действиях по реагированию" на стр. 617) и в свойствах задачи.
Области проверки	Отображаются области проверки файлов: важные области системных дисков и путь из ИОС.

Не рекомендуется добавлять или удалять ИОС-файлы после запуска задачи. Это может привести к некорректному отображению результатов поиска ИОС для предыдущих запусков задачи. Для поиска индикаторов компрометации по новым ИОС-файлам рекомендуется добавлять новые задачи.

Результат выполнения задачи *Поиск ИОС* можно посмотреть в разделе **Активы (Устройства)** → **Задачи** → <название задачи> → **Параметры приложения** → **Результаты поиска ИОС**.

Таблица в разделе **Результаты поиска ИОС** содержит список устройств, на которых выполнена задача *Поиск ИОС*, а также результаты выполнения задачи. В раскрывающемся списке **Устройство** вы можете

выбрать результаты выполнения задачи для всех управляемых устройств группы администрирования или для конкретного устройства.

Таблица содержит следующие столбцы:

- **Статус.**
Статус обнаружения индикаторов компрометации, отображающийся в виде значка.
- **Устройство.**
Имя устройства, на котором выполнена задача *Поиск IOC*.
- **Время.**
Дата и время выполнения задачи *Поиск IOC*.
- **Результаты.**
Информация о результате выполнения задачи *Поиск IOC*. В результате выполнения задачи может отображаться один из следующих статусов:
 - *обнаружены IOC*;
Этот статус отображается в виде ссылки, при переходе по которой открывается окно с деталями алерта (см. раздел "Просмотр информации об обнаруженной угрозе и действиях по реагированию" на стр. [617](#)).
 - *IOC не обнаружены*.

Также результат выполнения задачи можно посмотреть в разделе **Активы (Устройства) → Задачи → <название задачи>** на закладке **Результаты** в столбце **Описание**.

Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Industrial CyberSecurity for Linux Nodes автоматически удаляет старые записи.

Требования к IOC-файлам

При создании задач поиска IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- Приложение поддерживает IOC-файлы с расширением IOC и XML открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- Семантические ошибки и неподдерживаемые IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов приложение фиксирует отсутствие совпадения.
- Идентификаторы всех IOC-файлов, которые используются в одной задаче поиска IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи *Поиск IOC*.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC.



ЗАГРУЗИТЬ ФАЙЛ IOC TERMS.XLSX

https://support.kaspersky.com/Help/KICS4Linux/IOC_Terms/IOC_Terms.xlsx

Особенности и ограничения поддержки стандарта OpenIOC приложением приведены в таблице ниже.

Таблица 232. Особенности и ограничения поддержки стандарта OpenIOC версий 1.0 и 1.1

Поддерживаемые условия	OpenIOC 1.0: • is • isnot (как исключение из множества) • contains • containsnot (как исключение из множества) OpenIOC 1.1: • is • contains • starts-with • ends-with • matches • greater-than • less-than
Поддерживаемые атрибуты условий	OpenIOC 1.1: • preserve-case • negate
Поддерживаемые операторы	AND OR
Поддерживаемые типы данных	"date": дата (применимые условия: is, greater-than, less-than) "int": целое число (применимые условия: is, greater-than, less-than) "string": строка (применимые условия: is, contains, matches, starts-with, ends-with) "duration": продолжительность в секундах (применимые условия: is, greater-than, less-than)
Особенности интерпретации типов данных	Типы данных "boolean string", "restricted string", "md5", "IP", "sha256", "base64Binary" интерпретируются как строка (string). Приложение поддерживает интерпретацию параметра Content для типов данных int и date, заданного в виде промежутков: • OpenIOC 1.0: С использованием оператора TO в поле Content: <pre><Content type="int">49600 TO 50700</Content></pre> <pre><Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content></pre> <pre><Content type="int">[154192 TO 154192]</Content></pre> • OpenIOC 1.1: С помощью условий greater-than и less-than С использованием оператора TO в поле Content Приложение поддерживает интерпретацию типов данных date и duration, если индикаторы заданы в формате ISO 8601, Zulu time zone, UTC.

Включение и выключение сетевой изоляции устройства

Вы можете включать сетевую изоляцию устройства следующими способами:

- С помощью задачи *Поиск ИОС* (см. раздел "*Поиск индикаторов компрометации*" на стр. [617](#)).
Если при создании и настройке параметров задачи *Поиск ИОС* в блоке **Действия при обнаружении ИОС** вы установили флажки **Применять действия по реагированию при обнаружении ИОС** и **Изолировать устройство от сети**, то включение сетевой изоляции происходит автоматически при обнаружении приложением индикаторов компрометации (ИОС).
- В окне с деталями алерта (см. раздел "Просмотр информации об обнаруженной угрозе и действиях по реагированию" на стр. [617](#)).
- В свойствах устройства в Web Console (см. раздел "Включение и выключение сетевой изоляции устройства вручную в Web Console" на стр. [623](#)).

Включение сетевой изоляции доступно только при условии, что включена интеграция с решением Kaspersky Endpoint Detection and Response Optimum и компонент EDR Optimum находится в статусе *Выполняется* (см. раздел "*Просмотр статуса интеграции с Kaspersky Endpoint Detection and Response Optimum*" на стр. [616](#)).

Вы можете выключать сетевую изоляцию устройства следующими способами:

- Вручную в свойствах устройства в Web Console (см. раздел "Включение и выключение сетевой изоляции устройства вручную в Web Console" на стр. [623](#)).
- Вручную в командной строке (см. раздел "Выключение сетевой изоляции устройства в командной строке" на стр. [625](#)).
- В окне с деталями алерта (см. раздел "Просмотр информации об обнаруженной угрозе и действиях по реагированию" на стр. [617](#)).
- Настроив автоматическое выключение в свойствах устройства или в свойствах политики (см. раздел "Настройка автоматического выключения сетевой изоляции" на стр. [623](#)).

Выключение сетевой изоляции в свойствах устройства и в командной строке доступно вне зависимости от того, включена ли интеграция с решением Kaspersky Endpoint Detection and Response Optimum и активирован ли компонент EDR Optimum, а также вне зависимости от того, распространяется ли на устройство действие политики.

Вы можете настраивать исключения (см. раздел "Настройка исключений из сетевой изоляции" на стр. [626](#)) для сетевых соединений, которые не нужно изолировать при включении сетевой изоляции.

Вы можете проверять статус сетевой изоляции в командной строке (см. раздел "Выключение сетевой изоляции устройства в командной строке" на стр. [625](#)).

После включения сетевой изоляции приложение разрывает все активные и блокирует все новые сетевые соединения TCP/IP на устройстве, кроме следующих:

- соединений, указанных в исключениях из сетевой изоляции;
- соединений, инициированных службами Kaspersky Industrial CyberSecurity for Linux Nodes;
- соединений, инициированных Агентом администрирования Kaspersky Security Center.

Изолированному устройству EDR Optimum автоматически присваивает тег **ISOLATED FROM NETWORK**. После выключения сетевой изоляции этот тег автоматически снимается.

Общую информацию о получении списка изолированных устройств по тегу см. в справке Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm).

В этом разделе

Включение и выключение сетевой изоляции устройства вручную в Web Console	623
Настройка автоматического выключения сетевой изоляции.....	623
Выключение сетевой изоляции устройства в командной строке	625

Включение и выключение сетевой изоляции устройства вручную в Web Console

► *Чтобы включить или выключить сетевую изоляцию устройства:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
Откроется список управляемых устройств.
2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и в открывшемся окне выберите группу администрирования.
В списке отобразятся только управляемые устройства выбранной группы администрирования.
3. В списке найдите нужное устройство и нажмите на его имя.
4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.
5. В списке приложений, установленных на устройстве, нажмите на название приложения **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5**.
Откроется окно свойств приложения.
6. Перейдите на закладку **Параметры приложения**.
7. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response Optimum**.
8. В блоке параметров **Сетевая изоляция** выполните одно из следующих действий:
 - чтобы включить сетевую изоляцию устройства, нажмите на кнопку **Изолировать устройство от сети**;
 - чтобы выключить сетевую изоляцию устройства, нажмите на кнопку **Разблокировать изолированное устройство**.

Если вы включили сетевую изоляцию устройства, то Kaspersky Industrial CyberSecurity for Linux Nodes присвоит устройству тег **ISOLATED FROM NETWORK**. Если вы выключили сетевую изоляцию устройства, то Kaspersky Industrial CyberSecurity for Linux Nodes снимет этот тег с устройства.

Настройка автоматического выключения сетевой изоляции

Вы можете настроить автоматическое выключение сетевой изоляции по истечении заданного периода времени:

- В свойствах устройства.

Настройка автоматического выключения сетевой изоляции в свойствах устройства недоступна, если на устройство распространяется действие политики.

- В свойствах политики.

Параметры автоматического выключения сетевой изоляции, указанные в свойствах политики, применяются только к тем устройствам, которые были изолированы в результате обнаружения индикаторов компрометации (IOC) при выполнении задачи *Поиск IOC*.

По умолчанию приложение выключает сетевую изоляцию через 5 часов с момента включения. После выключения сетевой изоляции устройство может работать в сети без ограничений.

Настройка автоматического выключения сетевой изоляции в свойствах устройства

► *Чтобы настроить автоматическое выключение сетевой изоляции устройства:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
Откроется список управляемых устройств.
2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и выберите в открывшемся окне группу администрирования.
В списке отобразятся только управляемые устройства выбранной группы администрирования.
3. Найдите нужное устройство в списке и нажмите на его имя.
4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.
5. В списке приложений, установленных на устройстве, нажмите на название приложения **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5**.
Откроется окно свойств приложения.
6. Перейдите на закладку **Параметры приложения**.
7. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response Optimum**.
8. В блоке параметров **Сетевая изоляция** нажмите на ссылку **Настроить разблокировку устройства**.
9. В открывшемся окне **Настройка разблокировки устройства** задайте параметры разблокировки устройства (см. таблицу ниже).
10. Сохраните внесенные изменения.

Таблица 233. Параметры разблокировки устройства

Параметр	Описание
Разблокировать автоматически изолированное устройство через	Флажок включает или выключает автоматическую разблокировку изолированного устройства по истечении временного периода, указанного в поле ввода ниже. По умолчанию флажок установлен.

Настройка автоматического выключения сетевой изоляции в свойствах политики

► Чтобы настроить автоматическое выключение сетевой изоляции устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.
Откроется список политик.
2. Выберите группу администрирования, содержащую устройства, на которых применяется политика. Для этого нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите группу администрирования в открывшемся окне.
В списке отобразятся политики, настроенные для выбранной группы администрирования.
3. Нажмите на название нужной политики в списке.
Откроется окно свойств политики.
4. Перейдите на закладку **Параметры приложения**.
5. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response Optimum**.
6. В блоке параметров **Сетевая изоляция** нажмите на ссылку **Настроить разблокировку устройства**.
7. В открывшемся окне **Настройка разблокировки устройства** задайте параметры разблокировки устройства (см. таблицу ниже).
8. Сохраните внесенные изменения.

Таблица 234. Параметры разблокировки устройства

Параметр	Описание
Разблокировать автоматически изолированное устройство через	Флажок включает или выключает автоматическую разблокировку изолированного устройства по истечении временного периода, указанного в поле ввода ниже. По умолчанию флажок установлен.

Выключение сетевой изоляции устройства в командной строке

► Чтобы выключить сетевую изоляцию устройства с помощью командной строки, выполните следующую команду:

```
kics-control [-R] --isolation-off
```

Вы можете проверить статус сетевой изоляции и просмотреть список исключений из сетевой изоляции с помощью следующей команды:

```
kics-control [-R] --isolation-stat
```

Для сетевой изоляции в командной строке отображается один из следующих статусов:

- *Сетевая изоляция включена.*
- *Сетевая изоляция выключена.*

Настройка исключений из сетевой изоляции

Вы можете настраивать исключения:

- в свойствах политики (см. раздел "Добавление и удаление исключений из сетевой изоляции в свойствах политики в Web Console" на стр. [627](#));
- в свойствах устройства (см. раздел "Добавление и удаление исключения из сетевой изоляции в свойствах устройства" на стр. [627](#)).

Сетевые соединения, на которые распространяются заданные правила, не будут заблокированы на устройстве после включения сетевой изоляции.

По умолчанию из сетевой изоляции исключаются сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент.

Исключения, заданные в свойствах политики, применяются, только если сетевая изоляция включена приложением автоматически, в результате реагирования на обнаружение индикаторов компрометации (ИОС) (см. раздел "Поиск индикаторов компрометации" на стр. [617](#)).

Исключения, заданные в свойствах устройства, применяются, только если сетевая изоляция включена вручную в свойствах устройства (см. раздел "Включение и выключение сетевой изоляции устройства вручную в Web Console" на стр. [623](#)) или в окне с деталями алерта (см. раздел "Просмотр информации об обнаруженной угрозе и действиях по реагированию" на стр. [617](#)).

Активная политика не блокирует применение исключений из сетевой изоляции, заданных в свойствах устройства.

Вы можете просматривать перечень исключений из сетевой изоляции:

- в свойствах политики (см. раздел "Добавление и удаление исключений из сетевой изоляции в свойствах политики в Web Console" на стр. [627](#)) (**Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response Optimum** → ссылка **Исключения**);
- в свойствах устройства (см. раздел "Добавление и удаление исключения из сетевой изоляции в свойствах устройства" на стр. [627](#)) (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → ссылка <название приложения Kaspersky Industrial CyberSecurity for Linux Nodes> → **Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response Optimum** → ссылка **Исключения**);
- в командной строке (см. раздел "Выключение сетевой изоляции устройства в командной строке" на стр. [625](#)).

В этом разделе

Добавление и удаление исключений из сетевой изоляции в свойствах политики в Web Console ...	627
Добавление и удаление исключения из сетевой изоляции в свойствах устройства	627
Окно добавления исключения из сетевой изоляции	628
Окно Словарь сетевых профилей	628

Добавление и удаление исключений из сетевой изоляции в свойствах политики в Web Console

В Web Console вы можете добавлять и удалять исключения из сетевой изоляции в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response Optimum** → ссылка **Исключения**).

В окне **Исключения** с помощью кнопок над таблицей вы можете выполнить следующие действия:

- добавить информацию об исключаемом сетевом соединении одним из следующих способов:
 - нажать на кнопку **Добавить**, а затем ввести информацию о сетевом соединении (см. раздел "Окно добавления исключения из сетевой изоляции" на стр. [628](#));
 - нажать на кнопку **Добавить из профиля**, а затем выбрать сетевой профиль из словаря (см. раздел "Окно Словарь сетевых профилей" на стр. [628](#));
- удалить информацию о сетевом соединении.

Добавление и удаление исключения из сетевой изоляции в свойствах устройства

Добавление и удаление исключений из сетевой изоляции в свойствах устройства недоступно, если устройство распространяется действие политики.

► Чтобы добавить или удалить исключение из сетевой изоляции в свойствах устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
Откроется список управляемых устройств.
2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и выберите в открывшемся окне группу администрирования.
В списке отобразятся только управляемые устройства выбранной группы администрирования.
3. Найдите нужное устройство в списке и нажмите на его имя.
4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.
5. В списке приложений, установленных на устройстве, нажмите на название приложения **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5**.

Откроется окно свойств приложения.

6. Перейдите на закладку **Параметры приложения**.
7. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response Optimum**.
8. В блоке параметров **Сетевая изоляция** по ссылке **Исключения** откройте окно **Исключения**.
9. В открывшемся окне с помощью кнопок над таблицей выполните необходимое действие:
 - Если вы хотите добавить информацию об исключаемом сетевом соединении, сделайте это одним из следующих способов:
 - нажмите на кнопку **Добавить** и ввести информацию о сетевом соединении (см. раздел "Окно добавления исключения из сетевой изоляции" на стр. [628](#));
 - нажмите на кнопку **Добавить из профиля** и выбрать сетевой профиль из словаря (см. раздел "Окно Словарь сетевых профилей" на стр. [628](#)).
 - Если вы хотите удалить информацию об исключаемом сетевом соединении, установите флажок напротив удаляемого сетевого соединения и нажмите на кнопку **Удалить**;
10. Сохраните внесенные изменения.

Окно добавления исключения из сетевой изоляции

В этом окне вы можете ввести информацию о сетевом соединении, которое не нужно блокировать после включения сетевой изоляции.

Таблица 235. Параметры сетевого соединения

Параметр	Описание
Название	Название сетевого соединения.
Направление	Направление сетевого соединения.
Протокол	Протокол, используемый сетевым соединением.
Номер	Номер сетевого соединения.
Локальный порт(ы) / диапазон(ы)	Номер локального порта(ов) или диапазон(ы) локальных портов.
Удаленный порт(ы) / диапазон(ы)	Номер удаленного порта(ов) или диапазон(ы) удаленных портов.
Удаленный адрес	IP-адрес удаленного устройства.

Окно Словарь сетевых профилей

В этом окне вы можете выбрать профиль исключаемого сетевого соединения.

Таблица 236. Профили сетевых соединений

Профиль сетевого соединения	Описание
DNS-сервер	Служба, обеспечивающая разрешение DNS-имен, отвечая на запросы получения IP-адресов и запросы обновления DNS-записей.
DNS-клиент	Служба, обеспечивающая разрешение DNS-имен, выполняя запросы DNS-имен.
Службы сертификатов Active Directory®	Службы, используемые для создания, проверки и отзыва сертификатов открытых ключей для внутреннего пользования в организации.
Службы федерации Active Directory	Службы, используемые для предоставления пользователям доступа к нескольким веб-службам или сетевым ресурсам при помощи единых наборов учетных данных, хранящихся централизованно.
Службы Active Directory облегченного доступа к каталогам	Службы с теми же функциями, что и доменные службы Active Directory, но не требующие создания доменов или контроллеров домена.
Службы управления правами Active Directory	Службы, используемые для управления доступом пользователей к документам.
DHCP	Служба, использующая протокол динамической конфигурации узлов (DHCP) для автоматического распределения IP-адресов.
Протокол передачи файлов (FTP)	Стандартный сетевой протокол, используемый для передачи файлов между клиентом и сервером в сети.
Центр распространения ключей Kerberos	Сетевая служба, используемая для предоставления тикетов (TGS) и временных ключей сеанса пользователям и устройствам в домене Active Directory.
Безопасная оболочка (SSH)	Протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений.
Системные компоненты Linux	Системные компоненты Linux.

Запуск процесса

Вы можете удаленно запускать необходимые процессы и исполняемые файлы на устройствах с помощью задачи *Запуск процесса*.

Например, вы можете запускать:

- Процессы, остановленные в результате вредоносной активности на устройстве.
- Процессы, остановленные вами.

Например, вы можете удаленно запустить процесс, который был завершен вами с помощью задачи *Завершение процесса* (см. раздел "*Завершение процесса*" на стр. [631](#)).

- Скрипты.

Например, вы можете запустить скрипт, чтобы собрать с устройства данные, необходимые для расследования возникновения угрозы.

- Утилиты.

Например, вы можете запустить утилиту, которая сохраняет в файл информацию о конфигурации устройства.

- Приложения.

Если в вашей операционной системе установлена система SELinux в режиме `Enforcing`, то для запуска задачи *Запуск процесса* вам нужно дополнительно настроить систему SELinux (см. раздел "Настройка разрешающих правил в системе SELinux" на стр. [66](#)).

Вы можете создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)) задачу *Запуск процесса*, а также изменять (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) ее параметры в Web Console.

Вы не можете создавать, запускать или настраивать задачу *Запуск процесса* с помощью командной строки. Просмотр задачи *Запуск процесса*, созданной в Web Console, недоступен по команде `kics-control --get-task-list` в командной строке.

Таблица 237. Параметры задачи Запуск процесса

Параметр	Описание
Исполняемая команда	Поле ввода команды запуска процесса. Например, если вы хотите запустить утилиту <code>klnagchk</code>, которая предназначена для проверки подключения к Серверу администрирования, вам нужно ввести команду <code>/абсолютный путь к директории с утилитой>/klnagchk</code>, а затем, если необходимо, заполнить остальные поля, описанные в этой таблице ниже.
Аргументы командной строки (необязательно)	Поле ввода аргументов командной строки для передачи дополнительной информации в скрипт, утилиту или приложение при запуске. Например, вы можете ввести аргумент <code>-logfile /tmp/klnagchk.log</code>. Этот аргумент указывает утилите, что результат работы нужно сохранить в файл с именем <code>klnagchk.log</code> в директории <code>/tmp</code>. Если вам нужно передать несколько аргументов, требуется разделять их пробелами. Например, вы можете ввести аргументы <code>-logfile /tmp/klnagchk.log -savecert /home/user/certificate.cer</code>. Эти аргументы указывают утилите, что нужно сохранить результат работы в файл с именем <code>klnagchk.log</code> в директории <code>/tmp</code>, а также сохранить сертификат, используемый для проверки доступа к Серверу администрирования, в файле <code>certificate.cer</code> в директории <code>/home/user/</code>.
Путь к рабочей директории (необязательно)	Поле ввода пути к рабочей директории, в которой выполняется команда из поля Исполняемая команда. Например, вы можете ввести значение <code>/tmp</code> и запустить утилиту <code>klnagchk</code> с аргументами <code>-logfile klnagchk.log -savecert certificate.cer</code>. В этом случае оба файла будут созданы в директории <code>/tmp</code>.

Результат выполнения задачи можно посмотреть в разделе **Активы (Устройства) → Задачи → <название задачи>** на закладке **Результаты** в столбце **Описание**.

Завершение процесса

Вы можете удаленно завершать процессы на устройстве с помощью задачи *Завершение процесса*.

Например, вы можете завершать:

- Процессы, запущенные на устройстве в результате вредоносной активности.
- Процессы, запущенные вами.

Например, вы можете удаленно завершить процесс, который был запущен вами с помощью задачи *Запуск процесса* (см. раздел "*Запуск процесса*" на стр. [629](#)).

- Скрипты.

Например, вы можете удаленно завершить работу скрипта, который был запущен вами с помощью задачи *Запуск процесса* (см. раздел "*Запуск процесса*" на стр. [629](#)).

- Утилиты.

Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена вами с помощью задачи *Запуск процесса* (см. раздел "*Запуск процесса*" на стр. [629](#)).

- Приложения.

Завершать процессы критически важных системных объектов (англ. System Critical Object, SCO) невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

Вы можете создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) и запускать задачу *Завершение процесса* (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)), а также изменять ее параметры в Web Console (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)). Вы не можете создавать, запускать или настраивать задачу *Завершение процесса* с помощью командной строки. Просмотр задачи *Завершение процесса*, созданной из Web Console, недоступен по команде `kics-control --get-task-list` в командной строке.

Таблица 238. Параметры задачи Завершение процесса

Параметр	Описание
Укажите файл, процессы которого требуется завершить	В раскрывающемся списке вы можете выбрать способ указания пути к файлу: - По пути к директории и контрольной сумме. - По полному пути. - По PID. Значение По PID отображается в раскрывающемся списке только для задач, создаваемых в свойствах устройства.
Полный путь к файлу	Поле ввода полного пути к файлу. Это поле отображается, если в раскрывающемся списке Укажите файл, процессы которого требуется завершить вы выбрали значение По полному пути.
Тип контрольной суммы	В раскрывающемся списке вы можете выбрать тип контрольной суммы файла: - MD5. - SHA256. Этот раскрывающийся список отображается, если в раскрывающемся списке Укажите файл, процессы которого требуется завершить вы выбрали значение По пути к директории и контрольной сумме.
Контрольная сумма файла	Поле ввода контрольной суммы файла. Это поле отображается, если в раскрывающемся списке Укажите файл, процессы которого требуется завершить вы выбрали значение По пути к директории и контрольной сумме, а в раскрывающемся списке Тип контрольной суммы значение MD5.
Путь к директории	Поле ввода пути к директории файла. Это поле отображается, если в раскрывающемся списке Укажите файл, процессы которого требуется завершить вы выбрали значение По пути к директории и контрольной сумме.
Идентификатор процесса	Поле ввода идентификатора процесса (PID). Это поле отображается, если в раскрывающемся списке Укажите файл, процессы которого требуется завершить вы выбрали значение По PID.

Результат выполнения задачи можно посмотреть в разделе **Активы (Устройства) → Задачи → <название задачи>** на закладке **Результаты** в столбце **Описание**.

Получение файла с устройства

Вы можете получать файлы с устройств пользователей с помощью задачи *Получение файла с устройства*.

Например, вы можете получить файл журнала событий, который создало стороннее приложение.

Вы можете создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)) задачу *Получение файла с устройства*, а также изменять (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) ее параметры в Web Console.

Вы не можете создавать, запускать или настраивать задачу *Получение файла с устройства* с помощью командной строки. Просмотр задачи *Получение файла с устройства*, созданной из Web Console, недоступен по команде `kics-control --get-task-list` в командной строке.

Таблица **Получение файла** на закладке **Параметры приложения** содержит следующие столбцы:

- **Путь к директории.** Путь к директории файла, находящегося на устройстве.
- **Тип проверки контрольной суммы.** Тип проверки контрольной суммы файла, находящегося на устройстве.

С помощью кнопок над таблицей вы можете добавлять, изменять или удалять данные файлов, находящихся на устройстве. Задача *Получение файла с устройства* выполняется для файлов, указанных в таблице **Получение файла**.

При нажатии на кнопку **Добавить** открывается окно **Получение файла**, в котором вы можете настроить параметры задачи *Получение файла с устройства*.

Таблица 239. Параметры задачи *Получение файла с устройства*

Параметр	Описание
Укажите файл, который требуется получить	В раскрывающемся списке вы можете выбрать способ указания пути к файлу: • По пути к директории и контрольной сумме. • По полному пути.
Полный путь к файлу	Поле ввода полного пути к файлу. Это поле отображается, если в раскрывающемся списке Укажите файл, который требуется получить вы выбрали значение По полному пути.
Тип контрольной суммы	В раскрывающемся списке вы можете выбрать тип контрольной суммы файла: • MD5. • SHA256. Этот раскрывающийся список отображается, если в раскрывающемся списке Укажите файл, который требуется получить вы выбрали значение По пути к директории и контрольной сумме.

Параметр	Описание
Контрольная сумма файла	Поле ввода контрольной суммы файла. Это поле отображается, если в раскрывающемся списке Укажите файл, который требуется получить вы выбрали значение По пути к директории и контрольной сумме.
Путь к директории с файлом	Поле ввода пути к директории файла. Это поле отображается, если в раскрывающемся списке Укажите файл, который требуется получить вы выбрали значение По пути к директории и контрольной сумме.

В результате выполнения задачи *Получение файла с устройства* копия файла сохраняется в резервном хранилище устройства. Вы можете загрузить эту копию из резервного хранилища через Web Console на то устройство, с которого вы инициировали загрузку.

Размер файла не должен превышать 100 МБ.

Оригинал файла на устройстве пользователя остается в исходной директории.

Все файлы, полученные через задачу *Получение файла с устройства*, будут иметь статус **Заражен** в резервном хранилище Kaspersky Security Center независимо от результатов проверки файла.

Результат выполнения задачи можно посмотреть в разделе **Активы (Устройства)** → **Задачи** → <название задачи> на закладке **Результаты** в столбце **Описание**.

Удаление файла с устройства

Вы можете удалять файлы с устройства с помощью задачи *Удаление файла с устройства*. Это может быть необходимо, например, при реагировании на угрозы.

Критически важные системные объекты (англ. System Critical Object, SCO) удалить невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

Вы можете создавать (см. раздел "Создание задач в Web Console" на стр. [113](#)) и запускать (см. раздел "Запуск, остановка, приостановка и возобновление задач в Web Console" на стр. [115](#)) задачу *Удаление файла с устройства*, а также изменять (см. раздел "Изменение параметров задач в Web Console" на стр. [114](#)) ее параметры в Web Console.

Вы не можете создавать, запускать или настраивать задачу *Удаление файла с устройства* с помощью командной строки. Просмотр задачи *Удаление файла с устройства*, созданной из Web Console, недоступен по команде `kics-control --get-task-list` в командной строке.

Таблица 240. Параметры задачи *Удаление файла с устройства*

Параметр	Описание
Укажите файл, который нужно удалить	В раскрывающемся списке вы можете выбрать способ указания пути к удаляемому файлу: - По пути и контрольной сумме. - По полному пути.
Полный путь к файлу	Поле ввода полного пути к удаляемому файлу. Это поле отображается, если в раскрывающемся списке Укажите файл, который нужно удалить вы выбрали значение По полному пути .
Тип контрольной суммы	В раскрывающемся списке вы можете выбрать тип контрольной суммы удаляемого файла: - MD5. - SHA256. Этот раскрывающийся список отображается, если в раскрывающемся списке Укажите файл, который нужно удалить вы выбрали значение По пути и контрольной сумме .
Контрольная сумма файла	Поле ввода контрольной суммы удаляемого файла. Это поле отображается, если в раскрывающемся списке Укажите файл, который нужно удалить вы выбрали значение По пути и контрольной сумме .
Путь к директории	Поле ввода пути к директории удаляемого файла. Это поле отображается, если в раскрывающемся списке Укажите файл, который нужно удалить вы выбрали значение По пути и контрольной сумме .
Включать вложенные директории	Флажок включает или выключает вложенные директории.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки устройства. После перезагрузки устройства убедитесь, что файл удален.

Задача *Удаление файла с устройства* может быть завершена с ошибкой *Доступ запрещен*, если вы пытаетесь удалить запущенный исполняемый файл. Создайте и выполните задачу *Завершение процесса* (см. раздел "*Завершение процесса*" на стр. [631](#)) для этого файла, а затем повторите попытку.

Результат выполнения задачи можно посмотреть в разделе **Активы (Устройства) → Задачи →** <название задачи> на закладке **Результаты** в столбце **Описание**.

Просмотр событий и отчетов

В процессе работы приложения возникают различного рода *события*. Они могут иметь информационный характер или нести важную информацию. Например, с помощью события приложение может уведомлять об успешно выполненном обновлении баз приложения или может фиксировать ошибку в работе компонента, которую требуется устранить.

Kaspersky Industrial CyberSecurity for Linux Nodes позволяет вносить информацию о событиях, возникающих в работе приложения, в следующие журналы:

- Журнал событий приложения. По умолчанию приложение сохраняет информацию о событиях в базе данных `/var/opt/kaspersky/kics/private/storage/events.db`. Вы можете настраивать параметры журнала событий приложения (см. раздел "Настройка параметров журнала событий приложения" на стр. [642](#)) в командной строке.
- Журнал операционной системы (syslog). По умолчанию журнал операционной системы не используется. Вы можете включить запись событий в этот журнал (см. раздел "Настройка записи событий в журнал операционной системы" на стр. [641](#)).

Для доступа к журналу событий приложения и к журналу операционной системы требуются root-права.

Если управление приложением Kaspersky Industrial CyberSecurity for Linux Nodes осуществляется с помощью Kaspersky Security Center, данные о событиях могут передаваться на Сервер администрирования Kaspersky Security Center. Для некоторых событий действуют правила агрегирования. В случае, если за короткий промежуток времени в процессе работы приложения создается много событий одного типа, приложение переключается в режим агрегирования событий и отправляет в Kaspersky Security Center одно агрегированное событие с описанием параметров этих событий. Для разных событий могут использоваться разные правила агрегирования. Подробнее о событиях см. в справке Kaspersky Security Center.

Вы можете получать информацию о событиях приложения следующими способами:

- В Консоли администрирования и в Web Console (см. раздел "Просмотр событий в Kaspersky Security Center" на стр. [642](#)).
- В командной строке (см. раздел "Просмотр событий в командной строке" на стр. [642](#)).
- Если вы используете графический пользовательский интерфейс (на стр. [646](#)) Kaspersky Industrial CyberSecurity for Linux Nodes – во всплывающих окнах приложения.

Некоторые события могут содержать пути к файлам. При выводе путь к файлу рассматривается как строка в кодировке UTF-8. В случае если какой-то из байт в пути не соответствует правилам кодирования UTF-8, он заменяется на символ `?`. Также на символ `?` заменяется последовательность из четырех байт, кодирующая код символов, выходящих за пределы диапазона Unicode (больше `0x10FFFF`). Специальные символы экранируются (заменяются) определенным образом.

Правила экранирования символов в путях к файлам в событиях при выводе по команде `kics-control -E --query`:

- символы `'\a'`, `'\b'`, `'\t'`, `'\n'`, `'\v'`, `'\f'`, `'\r'` заменяются двумя символами следующим образом:
`'\a' -> "\\a"`
`'\b' -> "\\b"`
`'\t' -> "\\t"`

`'\n' -> "\\n"`

`'\v' -> "\\v"`

`'\f' -> "\\f"`

`'\r' -> "\\r"`

- все прочие специальные символы выводятся без изменений.

Правила экранирования символов в путях к файлам в событиях при выводе по команде `kics-control -E --query --json`:

- символы `'\b'`, `'\f'`, `'\n'`, `'\r'`, `'\t'`, `'\"'`, `'\\'` экранируются, в соответствии с форматом JSON, следующим образом:

`'\b' -> "\\b"`

`'\f' -> "\\f"`

`'\n' -> "\\n"`

`'\r' -> "\\r"`

`'\t' -> "\\t"`

`'\"' -> "\\\""`

`'\\' -> "\\\""`

- все прочие специальные символы экранируются в соответствии с общими правилами экранирования специальных символов для формата JSON (`'\a' -> '\u0007'`).

Правила экранирования символов в путях к файлам в событиях при передаче в syslog зависят от значения параметра `SyslogFormatType`:

- если `SyslogFormatType=JSON`:

- символы `'\b'`, `'\f'`, `'\n'`, `'\r'`, `'\t'`, `'\"'`, `'\\'` экранируются, в соответствии с форматом JSON, следующим образом:

`'\b' -> "\\b"`

`'\f' -> "\\f"`

`'\n' -> "\\n"`

`'\r' -> "\\r"`

`'\t' -> "\\t"`

`'\"' -> "\\\""`

`'\\' -> "\\\""`

- все прочие специальные символы экранируются в соответствии с общими правилами экранирования специальных символов для формата JSON (`'\a' -> '\u0007'`).

- если `SyslogFormatType=CEF`:

- символы `'\n'`, `'\r'`, `'\"'`, `'='` экранируются следующим образом:

`'\n' -> "\\n"`

`'\r' -> "\\r"`

`'\"' -> "\\\""`

'=' -> "\\='"

- все прочие специальные символы передаются без изменений.

Первый обратный слеш в последовательности при описании правил – это символ экранирования.

Примеры:

' \a ' – это один символ (управляющий);

' \\a ' – это два символа (обратный слеш + символ a);

' \ \ ' – это один символ (обратный слеш), ' \ \ \ \ ' – это два символа (обратный слеш + обратный слеш).

На основе событий, происходящих во время работы приложения, можно формировать различные *отчеты*. В отчеты записывается информация о работе каждого компонента приложения Kaspersky Industrial CyberSecurity for Linux Nodes и результаты выполнения каждой задачи и работы всего приложения в целом.

Вы можете просматривать отчеты следующими способами:

- В Консоли администрирования и в Web Console доступны отчеты Kaspersky Security Center. С их помощью вы можете, например, получить сведения о зараженных файлах, использовании ключей и баз приложения. Подробную информацию о работе с отчетами Kaspersky Security Center см. в справке Kaspersky Security Center.
- В графическом пользовательском интерфейсе Kaspersky Industrial CyberSecurity for Linux Nodes доступны отчеты приложения (см. раздел "Просмотр отчетов" на стр. [650](#)).

В событиях и отчетах могут содержаться следующие персональные данные:

- имена и идентификаторы пользователей в операционной системе;
- пути к файлам пользователя;
- IP-адреса удаленных устройств, проверяемых компонентом Защита от шифрования (см. раздел "Защита от удаленного вредоносного шифрования" на стр. [404](#));
- IP-адреса отправителей и получателей сетевых пакетов, проверяемых компонентом Управление сетевым экраном;
- веб-адреса источников обновлений;
- значения общих параметров приложения;
- имена и параметры задач командной строки;
- обнаруженные вредоносные, фишинговые, рекламные веб-адреса и веб-адреса, содержащие легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным;
- названия контейнеров и образов;
- пути к контейнерам и образам;
- названия и идентификаторы устройств;
- веб-адреса репозиторий;
- имена файлов, пути к файлам и хеш-суммы исполняемых файлов приложений;
- названия категорий приложений.

В этом разделе

Настройка записи событий в журнал операционной системы.....	641
Настройка параметров журнала событий приложения.....	642
Просмотр событий в Kaspersky Security Center	642
Просмотр событий в командной строке	642

Настройка записи событий в журнал операционной системы

По умолчанию события, возникающие в работе приложения Kaspersky Industrial CyberSecurity for Linux Nodes, не записываются в журнал операционной системы. Вы можете включить запись событий в этот журнал с помощью Web Console, Консоли администрирования или командной строки.

В Kaspersky Security Center вы также можете выбрать события, которые будут записываться в журнал операционной системы.

Настройка в Web Console

В Web Console вы можете настраивать запись событий в журнал операционной системы в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры приложения**).

По ссылке **Настроить уведомления** в блоке **Уведомления** открывается окно **Уведомления**. В этом окне вы можете с помощью флажков выбрать события, которые приложение будет записывать в журнал операционной системы.

Вы можете выбирать отдельные типы событий или все типы событий определенного уровня важности.

По умолчанию все флажки сняты.

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать запись событий в журнал операционной системы в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры приложения**).

По ссылке **Настроить** в блоке **Уведомления** открывается окно **Параметры уведомлений**. В этом окне вы можете с помощью флажков выбрать события, которые приложение будет записывать в журнал операционной системы.

Вы можете выбирать отдельные типы событий или все типы событий определенного уровня важности.

По умолчанию все флажки сняты.

Настройка в командной строке

В командной строке вы можете включать и выключать запись событий в журнал операционной системы с помощью параметра `UseSyslog` из общих параметров приложения.

Вы можете изменять значение параметра (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `UseSyslog` может принимать следующие значения:

- `Yes` – включить запись событий в syslog.
- `No` (значение по умолчанию) – выключить запись событий в syslog.

Настройка параметров журнала событий приложения

По умолчанию информация о событиях сохраняется в журнале событий приложения, расположенном на устройстве. В командной строке вы можете настраивать следующие параметры журнала событий приложения с помощью общих параметров приложения:

- Изменять путь к базе данных журнала событий приложения с помощью параметра `EventsStoragePath`. Значение по умолчанию: `/var/opt/kaspersky/kics/private/storage/events.db`.
- Задавать максимальное количество событий, которые будет хранить приложение с помощью параметра `MaxEventsNumber`. Значение по умолчанию: `500000`. При превышении заданного количества событий приложение удаляет наиболее давние события.

Вы можете изменять значение параметров (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Просмотр событий в Kaspersky Security Center

Список всех событий в работе приложения Kaspersky Industrial CyberSecurity for Linux Nodes отображается в Web Console и в Консоли администрирования.

Вы можете настроить уведомления о событиях. *Уведомление* – это сообщение с информацией о событии, которое произошло защищенном устройстве. С помощью уведомлений вы можете своевременно получать информацию о событиях в работе приложения. Вы можете настроить выполнение скрипта при получении события из приложения или получение уведомлений о событиях по электронной почте.

Подробнее о работе с событиями в Kaspersky Security Center см. в справке Kaspersky Security Center.

Просмотр событий в командной строке

С помощью командной строки вы можете просматривать:

- текущие события приложения;
- события из журнала событий приложения.

Вывод текущих событий

Вы можете выводить в консоль информацию обо всех текущих событиях приложения или о текущих событиях, связанных с запуском или остановкой указанной задачи. С помощью фильтра (см. раздел "Использование фильтра для ограничения результатов запросов" на стр. [140](#)) вы так же можете выводить определенные текущие события, например, события указанного типа.

- Чтобы вывести в консоль информацию обо всех текущих событиях приложения, выполните следующую команду:

```
kics-control -W
```

Команда возвращает название события и дополнительную информацию о событии.

- Чтобы вывести в консоль информацию только о текущих событиях, связанных с запущенной задачей, выполните следующую команду:

```
kics-control --start-task <идентификатор/имя задачи> -W
```

Пример:

Включить вывод текущих событий запущенной задачи с ID=1:

```
kics-control --start-task 1 -W
```

- Чтобы вывести в консоль информацию о текущих событиях, соответствующих условиям фильтра, выполните следующую команду:

```
kics-control -W --query "<условия фильтра>"
```

Условия фильтра задаются с помощью одного или нескольких логических выражений (см. раздел "Использование фильтра для ограничения результатов запросов" на стр. [140](#)) в формате <поле> <операция сравнения> '<значение>', скомбинированных с помощью логического оператора and.

Пример:

Вывести события TaskStateChanged:

```
kics-control -W --query "EventType == 'TaskStateChanged'"
```

Вывести события TaskSettingsChanged, инициированных пользователем User:

```
kics-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

Вывод событий из журнала событий

Вы можете выводить в консоль или в файл информацию о событиях из журнала событий приложения. Вы можете использовать фильтр для вывода определенных событий.

- Чтобы вывести в консоль информацию обо всех событиях в журнале событий приложения, выполните следующую команду:

```
kics-control -E --query [--db <файл базы данных>]
```

где:

- <файл базы данных> – полный путь к файлу базы данных журнала событий, из которого вы хотите вывести события. По умолчанию приложение сохраняет информацию о событиях в базе данных /var/opt/kaspersky/kics/private/storage/events.db. Расположение базы данных определяется общим параметром приложения EventsStoragePath.

Вы можете использовать утилиту `less`, чтобы перемещаться по списку отображаемых событий.

По умолчанию в приложении хранится до 500 000 событий. Максимальное количество событий, которые хранит приложение, определяется общим параметром приложения `MaxEventsNumber`.

Если журнал событий расположен в базе данных по умолчанию, вы можете выводить в консоль информацию обо всех событиях с помощью команды:

```
kics-control -E
```

- Чтобы вывести в консоль информацию о событиях в журнале событий приложения, соответствующих определенным условиям, выполните следующую команду:

```
kics-control -E --query "<условия фильтра>" [--db <файл базы данных>] [-n  
<количество>] [--json] [--reverse]
```

где:

- `<условия фильтра>` – одно или несколько логических выражений (см. раздел "Использование фильтра для ограничения результатов запросов" на стр. 140) в формате `<поле> <операция сравнения> ' <значение> '`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.
 - `<количество>` – количество последних событий из выборки (то есть количество записей от конца выборки), которые нужно вывести.
 - `--json` – выводить события в формате JSON.
 - `--reverse` – выводить события в обратном порядке (от самого нового события наверху к более старым внизу).
- Чтобы вывести в файл информацию о событиях в журнале событий приложения, соответствующих определенным условиям, выполните следующую команду:

```
kics-control -E --query "<условия фильтра>" [--db <файл базы данных>] [-n  
<количество>] --file <имя и путь к файлу> [--json]
```

где `--file <имя и путь к файлу>` – полный путь к файлу, в который вы хотите вывести события.

Управление приложением через графический пользовательский интерфейс

С помощью графического пользовательского интерфейса приложения Kaspersky Industrial CyberSecurity for Linux Nodes вы можете:

- Просматривать информацию о состоянии защиты устройства.
- Включать и выключать компоненты приложения (см. раздел "Включение и выключение компонентов приложения" на стр. [648](#)):
 - Защита от файловых угроз (на стр. [172](#)).
 - Проверка съемных дисков (на стр. [314](#)).
 - Защита от веб-угроз (на стр. [378](#)).
 - Защита от сетевых угроз (на стр. [398](#)).
 - Защита от шифрования (см. раздел "Защита от удаленного вредоносного шифрования" на стр. [404](#)).
 - Управление сетевым экраном.
 - Контроль приложений (на стр. [431](#)).
 - Контроль устройств (на стр. [464](#)).
 - Анализ поведения (на стр. [544](#)).
 - Контроль целостности системы (см. раздел "Контроль целостности системы в реальном времени" на стр. [516](#)).
- Запускать и останавливать задачи проверки (см. раздел "Запуск и остановка задач проверки" на стр. [648](#)):
 - Поиск вредоносного ПО (на стр. [225](#)).
 - Проверка важных областей (на стр. [274](#)).
 - Проверка контейнеров (см. раздел "Проверка контейнеров и образов по требованию" на стр. [328](#)).
- Запускать и останавливать задачи обновления и отката обновления баз (см. раздел "Запуск и остановка задачи обновления" на стр. [649](#)).
- Запускать выборочную проверку файлов и директорий (запускается при нажатии кнопкой мыши на файле или директории, которые вы хотите проверить).
- Включать и выключать использование Kaspersky Security Network.
- Просматривать статистику работы и отчеты приложения (см. раздел "Просмотр отчетов" на стр. [650](#)).
- Управлять лицензионными ключами приложения (см. раздел "Управление лицензионными ключами" на стр. [652](#)) и просматривать информацию о лицензии, по которой используется приложение, и о связанном с лицензией ключе.
- Просматривать информацию об объектах, помещенных в резервное хранилище (см. раздел "Просмотр объектов резервного хранилища" на стр. [652](#)).

- Создавать файлы трассировки (см. раздел "Создание файла трассировки" на стр. [655](#)) приложения.

Если компонент и задача приложения работает в информирующем режиме, в графическом пользовательском интерфейсе приложения для каждого компонента и задачи отображается предупреждение *Выбран информирующий режим работы*.

Информирующий режим — это такой режим работы приложения, при котором в случае обнаружения угрозы компоненты и задачи приложения не пытаются лечить или удалять вредоносные объекты, запрещать доступ или блокировать активность приложений, а только информируют пользователя об обнаружении угрозы.

В этом разделе

Графический пользовательский интерфейс	646
Включение и выключение компонентов приложения	648
Запуск и остановка задач проверки	648
Запуск и остановка задачи обновления	649
Настройка использования Kaspersky Security Network	649
Просмотр отчетов	650
Просмотр объектов резервного хранилища	652
Управление лицензионными ключами	652
Создание файла трассировки	655

Графический пользовательский интерфейс

Значок приложения в области уведомлений

После установки пакета графического пользовательского интерфейса приложения Kaspersky Industrial CyberSecurity for Linux Nodes на устройстве в области уведомлений панели задач справа появляется значок приложения.

Значок приложения обеспечивает доступ к контекстному меню и главному окну приложения.

Контекстное меню значка приложения содержит следующие пункты:

- **Kaspersky Industrial CyberSecurity for Linux Nodes 1.5.** Открывает главное окно приложения, в котором отображается состояние защиты устройства и находятся элементы интерфейса, предоставляющие доступ к функциям приложения.
- **Выход.** Выполняет выход из графического пользовательского интерфейса приложения.

Главное окно приложения

Вы можете открыть главное окно приложения одним из следующих способов:

- С помощью правой кнопки мыши или двойным щелчком мыши по значку приложения в области уведомлений панели задач.
- Выбрав название приложения в меню приложений оконного менеджера операционной системы.

Главное окно приложения разделено на несколько частей:

- В центральной части главного окна приложения отображается статус защиты устройства. При нажатии кнопкой мыши на этой области окна открывается окно **Центр защиты**. В этом окне отображается информация о состоянии защиты устройства и рекомендации о действиях, которые вам нужно выполнить для устранения проблем в защите (при их наличии).
 - На кнопке **Проверка** отображается состояние задачи поиска вредоносного ПО и количество обнаруженных угроз. При нажатии на эту кнопку открывается окно **Проверка**. В этом окне вы можете запустить и остановить задачи (см. раздел "Запуск и остановка задач проверки" на стр. [648](#)) *Поиск вредоносного ПО, Проверка важных областей и Проверка контейнеров*. Вы также можете просмотреть отчеты для этих задач.
 - На кнопке **Обновление** отображается состояние задачи *Обновление*. При нажатии на эту кнопку открывается окно **Обновление**. В этом окне вы можете запустить задачи (см. раздел "Запуск и остановка задачи обновления" на стр. [649](#)) *Обновление и Откат обновления баз*. Вы также можете просмотреть отчеты для этих задач.
 - В нижней части главного окна приложения находятся следующие элементы:
 - Кнопка **Отчеты**. При нажатии на эту кнопку открывается окно **Отчеты**, в котором вы можете просмотреть статистику работы компонентов и задач и различные отчеты (см. раздел "Просмотр отчетов" на стр. [650](#)).
 - Кнопка **Резервное хранилище**. При нажатии на эту кнопку открывается окно **Резервное хранилище**, в котором содержится информация об объектах в резервном хранилище (см. раздел "Просмотр объектов резервного хранилища" на стр. [652](#)).
 - Кнопка **Настройка**. При нажатии на эту кнопку открывается окно **Настройка**, в котором вы можете включить или выключить компоненты приложения (см. раздел "Включение и выключение компонентов приложения" на стр. [648](#)), а также настроить использование KSN.
 - Кнопка **Поддержка**. При нажатии на эту кнопку открывается окно **Поддержка**, в котором отображается текущая версия приложения и следующая информация:
 - **Ключ** – активный лицензионный ключ, добавленный в приложение, или информация об отсутствии ключа. По ссылке в этом поле вы можете открыть окно **Лицензия**, в котором отображается подробная информация о лицензии (см. раздел "Просмотр информации о лицензии" на стр. [654](#)).
 - **Статус ключа** – информация о статусе активного лицензионного ключа или информация об отсутствии ключа.
 - **Дата выпуска баз** – состояние и дата выпуска баз приложения.
 - **Операционная система** – сведения об операционной системе устройства.
- В нижней части окна **Поддержка** отображаются ссылки на информационные ресурсы "Лаборатории Касперского" и ссылка, по которой открывается окно **Трассировка**. В этом окне вы можете создавать файлы трассировки приложения и настраивать уровень детализации файлов трассировки (см. раздел "Создание файла трассировки" на стр. [655](#)).
- В нижней части главного окна приложения отображается информация о лицензии и о ключе, а также о проблемах лицензирования (при их наличии). При нажатии кнопкой мыши на этой области окна открывается окно **Лицензия**, в котором отображается информация о лицензии (см. раздел "Просмотр информации о лицензии" на стр. [654](#)). По кнопке **Приобрести лицензию** в этом окне вы можете открыть сайт интернет-магазина "Лаборатории Касперского", где вы можете приобрести лицензию. После приобретения лицензии вы получите файл ключа, с помощью которого нужно активировать приложение (см. раздел "Добавление лицензионного ключа" на стр. [653](#)).

Включение и выключение компонентов приложения

С помощью графического пользовательского интерфейса вы можете включать и выключать компоненты приложения. Если компонент включен, доступна кнопка **Выключить**. По умолчанию включены компоненты Защита от файловых угроз, Контроль устройств и Анализ поведения. Компонент Защита от веб-угроз может включаться автоматически, если на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен) и в системе обнаружен один из поддерживаемых браузеров (см. раздел "Защита от веб-угроз" на стр. [378](#)).

Если компонент выключен, доступна кнопка **Включить**.

► *Чтобы включить или выключить компонент приложения:*

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Настройка**.
Откроется окно **Настройка**.
3. Нажмите на кнопку **Включить** или **Выключить** для нужного компонента.

Запуск и остановка задач проверки

► *Чтобы запустить или остановить задачу проверки:*

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на кнопку **Проверка**.
Откроется окно **Проверка**.
3. Выполните одно из следующих действий:
 - Если вы хотите запустить задачу проверки, нажмите на кнопку **Запустить**, расположенную под той задачей проверки, которую вы хотите запустить.
Отобразится ход выполнения задачи проверки.
 - Если вы хотите остановить задачу проверки, нажмите на кнопку **Остановить**, расположенную под той задачей проверки, которую вы хотите остановить.
Задача проверки остановится, отобразится информация о проверенных объектах и обнаруженных угрозах.
4. Если вы хотите просмотреть отчет по задаче проверки, нажмите на кнопку **Показать отчет**.

При обнаружении зараженного объекта или при завершении задачи проверки отображается всплывающее окно в области уведомлений рядом со значком приложения в правой части панели задач.

Также в окне **Проверка** отображается ход и результат выполнения временных задач проверки загрузочных секторов (*Scan_Boot_Sectors_{идентификатор}*) и временных задач выборочной проверки файлов (*Scan_File_{идентификатор}*). Вы можете скрыть информацию о выполненных временных задачах, нажав на крестик или закрыв окно **Проверка** (при переходе в главное окно или при выходе из приложения (см. раздел "Графический пользовательский интерфейс " на стр. [646](#))).

Запуск и остановка задачи обновления

► *Чтобы запустить или остановить задачу обновления:*

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на кнопку **Обновление**.
Откроется окно **Обновление**.
3. Выполните одно из следующих действий:
 - Если вы хотите запустить задачу, нажмите на кнопку **Запустить**, расположенную под той задачей, которую вы хотите запустить.
Отобразится ход выполнения задачи обновления.
При успешном завершении задачи обновления становится доступна ссылка **Откатить обновление**, с помощью которой вы можете откатить последнее успешное обновление баз.
 - Если вы хотите остановить задачу, нажмите на кнопку **Остановить**, расположенную под той задачей, которую вы хотите остановить.
Задача обновления остановится.
4. Если вы хотите просмотреть отчет по задаче, нажмите на кнопку **Показать отчет**.

► *Чтобы запустить задачу отката обновления:*

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на раздел **Обновление**.
Откроется окно **Обновление**.
3. Запустите задачу отката обновления баз по ссылке **Откатить обновление**.

Настройка использования Kaspersky Security Network

С помощью графического пользовательского интерфейса вы можете включать или выключать использование Kaspersky Security Network.

В сертифицированной версии приложения допускается только использование KPSN. Использование KSN не допускается, так как приводит к выходу приложения из сертифицированного состояния. Рекомендуется использовать KPSN или отказаться от использования KSN.

► *Чтобы включить использование Kaspersky Security Network:*

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Настройка**.
Откроется окно **Настройка**.
3. В окне **Настройка** выберите один из следующих вариантов:

- **Расширенный режим KSN**, если вы хотите использовать Kaspersky Security Network, получать информацию из базы знаний и отправлять анонимную статистику и данные о типах и источниках угроз.
 - **Стандартный режим KSN**, если вы хотите использовать Kaspersky Security Network, получать информацию из базы знаний, но не отправлять анонимную статистику и данные о типах и источниках угроз.
4. Нажмите на кнопку **Включить**.
Откроется окно **Использование Kaspersky Security Network**.
 5. В окне **Использование Kaspersky Security Network** внимательно прочитайте Положение о Kaspersky Security Network и выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.
 6. Нажмите **ОК**.
Кнопка **ОК** недоступна, если в окне **Использование Kaspersky Security Network** не выбран ни один из вариантов.

► *Чтобы выключить использование Kaspersky Security Network:*

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Настройка**.
Откроется окно **Настройка**.
3. Нажмите на кнопку **Выключить**.
4. В открывшемся окне нажмите на кнопку **Да**, чтобы отказаться от использования Kaspersky Security Network.

Просмотр отчетов

С помощью графического пользовательского интерфейса вы можете просматривать отчеты приложения. В отчеты записывается информация о работе компонентов и задач приложения.

Данные в отчетах представлены в виде таблицы, которая содержит список событий. Каждая строка в таблице содержит информацию об отдельном событии. Атрибуты события отображаются в столбцах таблицы. События, зарегистрированные в работе разных компонентов и задач, имеют разный набор атрибутов.

В отчетах предусмотрены следующие уровни важности событий:

- *Критический* – события критической важности, на которые нужно обратить внимание, поскольку они указывают на проблемы в работе приложения или на уязвимости в защите устройства.
- *Высокий*.
- *Средний*.
- *Низкий*.
- *Информационный*.
- *Ошибка*.

Отчеты отображаются в окне, которое открывается по кнопке **Отчеты**, расположенной в нижней части главного окна приложения (см. раздел "Графический пользовательский интерфейс " на стр. [646](#)).

В приложении доступны следующие отчеты:

- **Статистика.** Этот отчет содержит статистические данные о работе компонента Защита от файловых угроз и о задачах проверки. Вы можете обновить отображаемый отчет, нажав на кнопку **Обновить**.
- **Системный аудит.** Этот отчет содержит информацию о событиях, которые произошли во время работы приложения и во время взаимодействия пользователя с приложением.
- **Защита от угроз.** Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы следующих компонентов приложения:
 - Защита от файловых угроз.
 - Проверка съемных дисков.
 - Защита от шифрования.
 - Защита от веб-угроз.
 - Защита от сетевых угроз.
 - Управление сетевым экраном.
 - Контроль приложений.
 - Контроль устройств.
 - Анализ поведения.
 - Контроль целостности системы.
- **Задачи по требованию.** Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время выполнения задач проверки, задач обновления и проверки целостности системы.

► *Чтобы просмотреть отчет:*

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Отчеты**.
Откроется окно **Отчеты**.
3. В левой части окна **Отчеты** выберите нужный тип отчета.
В правой части окна отобразится отчет, содержащий список событий.
По умолчанию события в отчете отсортированы по возрастанию значений столбца **Дата**.
4. Если вы хотите посмотреть подробную информацию о событии, выберите это событие в отчете.
В нижней части окна отобразится блок, который содержит атрибуты этого события.

Для удобства работы с отчетами вы можете изменять представление данных на экране следующими способами:

- фильтровать список событий по времени возникновения;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке.

Просмотр объектов резервного хранилища

С помощью графического пользовательского интерфейса вы можете выполнять следующие действия с объектами резервного хранилища (см. раздел "Резервное хранилище" на стр. [586](#)):

- Просматривать информацию об объектах, помещенных в резервное хранилище на устройстве.
- Восстанавливать объекты из резервного хранилища в их исходные директории.
- Удалять объекты из резервного хранилища. Удаленные объекты восстановить невозможно.

Информация о восстановлении и удалении объектов записывается в журнал событий.

► *Чтобы просмотреть объекты в резервном хранилище:*

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Резервное хранилище**.

Откроется окно **Резервное хранилище**.

В окне отображается следующая информация об объектах резервного хранилища:

- название объекта;
- полный путь к объекту;
- дата добавления объекта в резервное хранилище;
- дата удаления объекта из резервного хранилища (это поле отображается, если задано ограничение на время хранения объектов в резервном хранилище);
- размер объекта.

Управление лицензионными ключами

С помощью графического пользовательского интерфейса вы можете добавлять (см. раздел "Добавление лицензионного ключа" на стр. [653](#)) и удалять (см. раздел "Удаление лицензионного ключа" на стр. [654](#)) лицензионные ключи приложения, а также просматривать информацию о лицензии (см. раздел "Просмотр информации о лицензии" на стр. [654](#)), по которой используется приложение, и о связанном с лицензией ключе.

Вы можете активировать приложение, добавив активный лицензионный ключ.

Активация – это процедура введения в действие лицензии (см. раздел "О лицензии" на стр. [81](#)), дающей право на использование полнофункциональной версии приложения в течение срока действия лицензии.

Если вы используете приложение по лицензии, которая не включает функциональность Kaspersky Endpoint Detection and Response Optimum (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response Optimum" на стр. [610](#)), для активации этой функциональности вам нужно добавить дополнительный лицензионный ключ Kaspersky Endpoint Detection and Response Optimum Add-on (далее также "ключ EDR Optimum").

Вы также можете добавить в приложение резервный ключ. Резервный ключ становится активным либо по истечении срока действия лицензии, связанной с активным ключом, либо при удалении активного ключа.

Наличие резервного ключа позволяет избежать ограничения функциональности приложения в момент окончания срока действия лицензии.

Резервный ключ может быть добавлен только после добавления активного лицензионного ключа.

В этом разделе

Добавление лицензионного ключа.....	653
Удаление лицензионного ключа.....	654
Просмотр информации о лицензии.....	654

Добавление лицензионного ключа

► Чтобы добавить активный лицензионный ключ в приложение:

1. Откройте главное окно приложения.
2. Выполните одно из следующих действия:
 - В нижней части главного окна приложения нажмите на область окна, в которой отображается информация о лицензии и о ключе.
 - В нижней части главного окна приложения нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** откройте окно **Лицензия** по ссылке в поле **Ключ**.

Откроется окно **Лицензия**. По кнопке **Приобрести лицензию** в этом окне вы можете открыть веб-сайт интернет-магазина "Лаборатории Касперского", где вы можете приобрести лицензию.

3. Вы можете активировать приложение по коммерческой лицензии или по пробной лицензии (см. раздел "О лицензии" на стр. [81](#)).

Чтобы активировать приложение по коммерческой лицензии:

- a. Нажмите на кнопку **Добавить** в блоке **Коммерческий ключ** и выполните следующие действия в зависимости от способа добавления ключа:
 - Если вы хотите добавить ключ с помощью кода активации, введите код активации и нажмите на кнопку **Далее**.
 - Если вы хотите добавить ключ с помощью файла ключа, нажмите на кнопку **Добавить ключ** и в открывшемся окне выберите файл с расширением key.

В окне отобразится информация о ключе и связанной с ним лицензии (см. раздел "Просмотр информации о лицензии" на стр. [654](#)).

- b. Нажмите на кнопку **Активировать**.

Чтобы активировать приложение по пробной лицензии, нажмите на кнопку **Активировать** в блоке **Пробный ключ**. В окне отобразится информация о пробной лицензии и связанном с ней ключе (см. раздел "Просмотр информации о лицензии" на стр. [654](#)).

Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

После добавления активного ключа приложения вы можете добавить резервный ключ и, если требуется, дополнительный ключ EDR Optimum. Для запуска процедуры добавления резервного или дополнительного ключа используйте кнопку **Добавить** в верхней части окна **Лицензия**.

Удаление лицензионного ключа

► Чтобы удалить лицензионный ключ, добавленный в приложение:

1. Откройте главное окно приложения.
2. Выполните одно из следующих действий:
 - В нижней части главного окна приложения нажмите на область окна, в которой отображается информация о лицензии и о ключе.
 - В нижней части главного окна приложения нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** откройте окно **Лицензия** по ссылке в поле **Ключ**.Откроется окно **Лицензия**.
3. Нажмите на кнопку **Удалить**, расположенную справа от информации о ключе, который вы хотите удалить.
4. Подтвердите удаление в открывшемся окне.

Просмотр информации о лицензии

► Чтобы просмотреть информацию о лицензии:

1. Откройте главное окно приложения.
2. Выполните одно из следующих действий:
 - В нижней части главного окна приложения нажмите на область окна, в которой отображается информация о лицензии и о ключе.
 - В нижней части главного окна приложения нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** откройте окно **Лицензия** по ссылке в поле **Ключ**.Откроется окно **Лицензия**.

В окне отображается информация о лицензии, по которой используется приложение, и о лицензии, связанной с резервным ключом, если резервный ключ добавлен в приложение. По ссылке **Подробнее** вы можете просматривать полную информацию о лицензиях и ключах.

В блоке **Действующие лицензии** отображается информация об активных ключах и связанных с ними лицензиях:

- Тип активной лицензии приложения, лицензионное ограничение и срок действия лицензии.
- **Ключ** – уникальная буквенно-цифровая последовательность.
- **Статус ключа** – статус ключа или сообщение о каких-либо проблемах, связанных с ключом.

- **Действует с** – дата активации приложения путем добавления этого ключа.
- **Истекает** – количество дней до истечения срока действия лицензии и дата окончания срока действия лицензии в формате UTC.
- **Название приложения** – название приложения, для активации которого предназначен ключ.
- **Защита** – информация об ограничении функций защиты и функции обновления баз приложения.

Если вы добавили в приложение активный ключ EDR Optimum, информация об этом ключе и связанной с ним лицензии также отображается в блоке **Действующие лицензии**.

В блоке **Резервные ключи** отображается информация о резервных ключах и связанных с ними лицензиях:

- Тип резервного ключа, лицензионное ограничение и срок действия лицензии, связанной с ключом.
- **Ключ** – уникальная буквенно-цифровая последовательность.
- **Тип лицензии** – тип лицензии, связанной с резервным ключом.
- **Название приложения** – название приложения, для активации которого предназначен ключ.
- **Защита** – информация об ограничении функций защиты и функции обновления баз приложения.

Если вы добавили в приложение резервный ключ EDR Optimum, информация об этом ключе и связанной с ним лицензии также отображается в блоке **Резервные ключи**.

Создание файла трассировки

С помощью графического пользовательского интерфейса вы можете создавать файлы трассировки приложения (см. раздел "О файлах трассировки приложения" на стр. [663](#)) и настраивать уровень детализации файлов трассировки.

► Чтобы создать файл трассировки:

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Поддержка**.
Откроется окно **Поддержка**.
3. По ссылке **Трассировка** откройте окно **Трассировка**.
4. В раскрывающемся списке **Уровень** выберите уровень детализации файла трассировки.
Рекомендуется уточнить требуемый уровень детализации у специалистов Службы технической поддержки "Лаборатории Касперского". По умолчанию установлено значение **Диагностический (300)**.
5. Нажмите на кнопку **Включить**, чтобы запустить процесс трассировки.
6. Воспроизведите ситуацию, при которой у вас возникает проблема.
7. Нажмите на кнопку **Выключить**, чтобы остановить процесс трассировки.

Созданные файлы трассировки хранятся в директории `/var/log/kaspersky/kics/`.

Проверка целостности компонентов приложения

Приложение Kaspersky Industrial CyberSecurity for Linux Nodes содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленники могут заменить один или несколько исполняемых модулей или файлов приложения другими файлами, содержащими вредоносный код. Чтобы предотвратить такую замену модулей и файлов, в приложении Kaspersky Industrial CyberSecurity for Linux Nodes предусмотрена проверка целостности компонентов приложения. Приложение проверяет модули и файлы на наличие неавторизованных изменений и повреждений. Если модуль или файл приложения имеет некорректную контрольную сумму, то он считается поврежденным.

Проверка целостности выполняется для следующих компонентов приложения, если они установлены на устройстве:

- пакет приложения;
- пакет графического пользовательского интерфейса;
- пакет Агента администрирования Kaspersky Security Center;
- плагин управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes.

Приложение проверяет целостность файлов, перечисленных в специальных списках, которые называются *файлы манифеста*. Для каждого компонента приложения существует свой файл манифеста, содержащий список файлов приложения, целостность которых важна для корректной работы этого компонента. Имя файла манифеста для каждого компонента одно и то же, но содержимое файлов манифестов различается. Файлы манифеста подписаны цифровой подписью, их целостность также проверяется.

Проверка целостности компонентов приложения выполняется с помощью утилиты проверки целостности.

Утилиту проверки целостности требуется запускать под учетной записью с root-правами.

Для проверки целостности вы можете использовать как утилиту, устанавливаемую вместе с приложением, так и утилиту, поставляемую на сертифицированном CD-диске.

Рекомендуется запускать утилиту проверки целостности с сертифицированного CD-диска, чтобы гарантировать целостность утилиты проверки. При запуске утилиты с CD-диска требуется указать полный путь к файлу манифеста.

Утилита проверки целостности, устанавливаемая вместе с приложением, расположена по следующим путям:

- для проверки пакета приложения, пакета графического пользовательского интерфейса и Агента администрирования: `/opt/kaspersky/kics/bin/integrity_checker`;
- для проверки плагина управления Kaspersky Industrial CyberSecurity for Linux Nodes – в директории, где расположены исполняемые модули (DLL) плагина управления:
 - `%ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kics_<версия плагина>.plg\integrity_checker.exe` – для 32-битных операционных систем;
 - `%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kics_<версия плагина>.plg\integrity_checker.exe` – для 64-битных операционных систем.

Файлы манифеста расположены по следующим путям:

- /opt/kaspersky/kics/bin/integrity_check.xml – для проверки целостности пакета приложения;
- /opt/kaspersky/kics/bin/gui_integrity_check.xml – для проверки целостности пакета графического пользовательского интерфейса;
- /opt/kaspersky/klagent/bin/kl_file_integrity_manifest.xml – для проверки Агента администрирования для 32-битных операционных систем;
- /opt/kaspersky/klagent64/bin/kl_file_integrity_manifest.xml – для проверки Агента администрирования для 64-битных операционных систем.

► Чтобы проверить целостность компонентов приложения, выполните следующую команду:

- для проверки пакета приложения и пакета графического пользовательского интерфейса:

```
integrity_checker [<путь к файлу манифеста>] --signature-type kds-with-filename
```
- для проверки плагина управления Kaspersky Industrial CyberSecurity for Linux Nodes и Агента администрирования:

```
integrity_checker [<путь к файлу манифеста>]
```

По умолчанию используется путь к файлу манифеста, расположенному в той же директории, в которой расположена утилита проверки целостности.

Вы можете запустить утилиту со следующими необязательными параметрами:

- `--crl <директория>` – путь к директории, содержащей список отозванных сертификатов (Certificate Revocation List).
- `--version` – отобразить версию утилиты.
- `--verbose` – детализировать вывод информации о выполненных действиях и результатах. Если вы не укажете этот параметр, будут отображаться только ошибки, объекты, не прошедшие проверку, и общая статистика проверки.
- `--trace <имя файла>`, где `<имя файла>` – имя файла, в который будут записываться события с уровнем детализации DEBUG, произошедшие во время проверки.
- `--signature-type kds-with-filename` – тип проверяемой сигнатуры (этот параметр является обязательным для проверки пакета приложения, пакета графического пользовательского интерфейса и Агента администрирования).
- `--single-file <файл>` – проверить только один файл, входящий в состав манифеста, остальные объекты манифеста игнорировать.

Вы можете просмотреть описание всех доступных параметров утилиты проверки целостности в справке параметров утилиты, выполнив команду `integrity_checker --help`.

Результат проверки файла манифеста отображается в следующем виде:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата 0).
- `FAILED` – целостность файлов не подтверждена (код возврата отличен от 0).

Если при запуске приложения обнаружено нарушение целостности приложения или Агента администрирования, приложение Kaspersky Industrial CyberSecurity for Linux Nodes формирует событие `IntegrityCheckFailed` в журнале событий и в Kaspersky Security Center.

Обновление баз приложения в изолированном сегменте сети

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

1. В приложении Kaspersky Security Center, находящемся в открытом сегменте сети, настройте задачу *Загрузка обновлений в хранилище Сервера администрирования*.
2. Убедитесь в том, что под управлением Kaspersky Security Center в открытом сегменте есть управляемые устройства с установленными приложениями, для которых нужно обновить базы.
3. Запустите задачу *Загрузка обновлений в хранилище Сервера администрирования*. В процессе загрузки обновлений с открытых серверов «Лаборатории Касперского» Kaspersky Security Center выполнит проверку целостности обновлений, прежде чем добавить их в свое хранилище.
4. Удобным вам способом перенесите содержимое хранилища Kaspersky Security Center в изолированный сегмент сети.
5. Запустите на средствах антивирусной защиты внутри изолированного сегмента сети задачу обновления баз с указанием перенесенного хранилища в качестве источника обновлений. При загрузке обновлений из хранилища приложения еще раз выполнят проверку целостности загружаемых обновлений баз.

Устранение уязвимостей и установка критических обновлений в приложении

"Лаборатория Касперского" может выпускать обновления приложения, 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 приложения, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: <http://support.kaspersky.ru/subscribe>).

Порядок получения критических обновлений изложен в формуляре.

Лицо, ответственное за эксплуатацию приложения, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в приложении, используя веб-сайт "Лаборатории Касперского" (<https://support.kaspersky.ru/vulnerability>), банк данных угроз безопасности информации ФСТЭК России (<http://www.bdu.fstec.ru>) и иные общедоступные источники.

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

- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (<https://community.kaspersky.com/>).

Действия после сбоя или неустранимой ошибки в работе приложения

Приложение автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда приложение не может восстановить свою работу, вам требуется переустановить приложение или его компонент. Вы также можете обратиться за помощью в Службу технической поддержки.

Обращение в Службу технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о приложении, рекомендуется обратиться в Службу технической поддержки.

Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Industrial CyberSecurity for Linux Nodes.

Kaspersky предоставляет поддержку Kaspersky Industrial CyberSecurity for Linux Nodes в течение жизненного цикла (см. страницу <https://support.kaspersky.com/corporate/lifecycle>). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules/ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки (<https://support.kaspersky.ru/b2b>);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

В этом разделе

Техническая поддержка через Kaspersky CompanyAccount	661
Получение информации для Службы технической поддержки	662
Об удаленной диагностике устройства с помощью Kaspersky Security Center	669

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;

- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

Получение информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас прислать *файл трассировки* (см. раздел "О файлах трассировки приложения" на стр. [663](#)) или *файл дампа* (см. раздел "О файлах дампа" на стр. [667](#)).

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на устройстве, подробные отчеты работы компонентов приложения.

Во время работ по диагностике специалисты Службы технической поддержки могут попросить вас изменить параметры приложения:

- активировать функциональность получения расширенной диагностической информации;
- выполнить более тонкую настройку работы отдельных компонентов приложения, 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 устройстве пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия требуется выполнять только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы приложения способами, не описанными в документации к приложению или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе приложения и операционной системы, снижению уровня защиты вашего устройства, а также к нарушению доступности и целостности обрабатываемой информации.

В этом разделе

О файлах трассировки приложения.....	663
Настройка параметров трассировки приложения.....	664
О файлах трассировки плагинов управления приложением	666
О файлах дампа.....	667
Включение и выключение записи дампов	667

О файлах трассировки приложения

Файл трассировки приложения Kaspersky Industrial CyberSecurity for Linux Nodes позволяет отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка.

По умолчанию файлы трассировки приложения не создаются. Вы можете включать и выключать создание файлов трассировки приложения и настраивать уровень детализации (см. раздел "Настройка параметров трассировки приложения" на стр. [664](#)) файлов трассировки в командной строке с помощью общих параметров приложения, а также с помощью графического пользовательского интерфейса (см. раздел "Создание файла трассировки" на стр. [655](#)).

Если вы включили создание файлов трассировки приложения, по умолчанию файлы трассировки хранятся в директории `/var/log/kaspersky/kics/`. Для доступа к этой директории требуются root-права.

Файлы трассировки хранятся на устройстве в течение всего времени использования приложения и удаляются без возможности восстановления при удалении приложения. Автоматическая отправка файлов трассировки в "Лабораторию Касперского" не выполняется.

Файлы трассировки хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Содержимое файлов трассировки приложения

В файлах трассировки содержатся следующие общие данные:

- время возникновения события;
- номер потока исполнения;
- компонент приложения, инициировавший событие;
- уровень важности события (информационное событие, предупреждение, критическое событие, ошибка);
- описание события, связанного с выполнением команды компонентом приложения, и результат выполнения этой команды.

В файлах трассировки могут храниться следующие данные в дополнение к общим данным:

- статусы компонентов приложения и их рабочие данные;
- данные о действиях пользователей в приложении;

- данные об оборудовании, установленном на устройстве;
- данные обо всех объектах и событиях операционной системы, а также данные о действиях пользователей;
- данные, содержащиеся в объектах операционной системы (например, содержимое файлов, в которых могут находиться персональные данные пользователей);
- данные о сетевом трафике (например, содержимое полей ввода на веб-сайте, которые могут включать данные банковской карты или любые другие конфиденциальные данные);
- данные, полученные с серверов "Лаборатории Касперского" (например, версия баз приложения);
- данные о потребленных ресурсах центрального процессора;
- данные о потребленных ресурсах оперативной памяти;
- данные об операциях чтения и записи файлов приложениями;
- данные о количестве кешированной информации, необходимой для работы приложения.

Настройка параметров трассировки приложения

Если вы управляете приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Kaspersky Security Center, вы можете настраивать параметры трассировки приложения в параметрах политики Kaspersky Industrial CyberSecurity for Linux Nodes с помощью Web Console или Консоли администрирования.

Если вы управляете приложением через командную строку, вы можете настраивать параметры трассировки приложения в общих параметрах приложения.

Настройка параметров трассировки в Web Console

В Web Console вы можете настраивать параметры трассировки приложения в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Параметры трассировки и записи дампов**) (см. таблицу ниже).

Таблица 241. Параметры трассировки приложения

Параметр	Описание
Путь к директории с файлами трассировки	Поле ввода пути к директории, в которой хранятся файлы трассировки. Значение по умолчанию: /var/log/kaspersky/kics. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, под которой работает Kaspersky Industrial CyberSecurity for Linux Nodes. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права.
Максимальное количество файлов трассировки	Поле ввода максимального количества файлов трассировки приложения. Значение по умолчанию: 10.
Максимальный размер файла трассировки (МБ)	Поле ввода максимального размера файла трассировки приложения (в мегабайтах). Значение по умолчанию: 500.

Для применения параметров трассировки требуется перезапустить приложение.

Настройка параметров трассировки в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры трассировки приложения в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры приложения**).

В блоке **Параметры трассировки и записи дампов** по ссылке **Настроить** открывается окно, в котором вы можете настроить параметры трассировки (см. таблицу ниже).

Таблица 242. Параметры трассировки приложения

Параметр	Описание
Путь к директории с файлами трассировки	Поле ввода пути к директории, в которой хранятся файлы трассировки. Значение по умолчанию: /var/log/kaspersky/kics. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, под которой работает Kaspersky Industrial CyberSecurity for Linux Nodes. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права.
Максимальный размер файла трассировки (МБ)	Поле ввода максимального размера файла трассировки приложения (в мегабайтах). Значение по умолчанию: 500.
Максимальное количество файлов трассировки	Поле ввода максимального количества файлов трассировки приложения. Значение по умолчанию: 10.

Для применения параметров трассировки требуется перезапустить приложение.

Настройка параметров трассировки в командной строке

В командной строке вы можете настраивать параметры трассировки приложения с помощью параметров `TraceLevel`, `TraceFolder`, `TraceMaxFileCount` и `TraceMaxFileSize` в общих параметрах приложения.

Параметр `TraceLevel` позволяет включить или выключить создание трассировки приложения и указать уровень детализации файлов трассировки. Параметр может принимать следующие значения:

- `Detailed` – создавать детализированный файл трассировки.
- `MediumDetailed` – создавать файл трассировки, содержащий информационные сообщения и сообщения об ошибках.
- `NotDetailed` – создавать файл трассировки, содержащий сообщения об ошибках.
- `None` (значение по умолчанию) – не создавать файл трассировки.

Параметр `TraceFolder` позволяет указать директорию, в которой хранятся файлы трассировки приложения. Значение по умолчанию: /var/log/kaspersky/kics. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, под которой работает Kaspersky

Industrial CyberSecurity for Linux Nodes. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права.

`TraceMaxFileSize` позволяет указать максимальное количество файлов трассировки приложения. Параметр может принимать значения от 1 до 10000. Значение по умолчанию: 10.

`TraceMaxFileSize` позволяет указать максимальный размер файла трассировки приложения в мегабайтах. Параметр может принимать значения от 1 до 1000. Значение по умолчанию: 500.

Вы можете изменять значение параметров (см. раздел "Изменение общих параметров приложения" на стр. [139](#)) с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

После изменения значений параметров `TraceFolder`, `TraceMaxFileSize`, `TraceMaxFileSize` требуется перезапустить приложение.

О файлах трассировки плагинов управления приложением

Автоматическая отправка файлов трассировки плагинов управления в "Лабораторию Касперского" не выполняется.

Файлы трассировки хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Файлы трассировки mmsc-плагина управления

Если для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes вы используете Консоль администрирования, информация о событиях, возникающих во время работы mmsc-плагина управления, может записываться в файл трассировки mmsc-плагина Kaspersky Industrial CyberSecurity for Linux Nodes на устройстве, где установлен Сервер администрирования. Имя файла содержит номер версии приложения, дату и время создания файла и идентификатор процесса (PID). В этот файл записывается информация о событиях, возникающих во время работы mmsc-плагина, в частности, о работе политик и задач.

По умолчанию файлы трассировки mmsc-плагина не создаются. Вы можете создать файл трассировки mmsc-плагина с помощью ключей реестра. За подробной информацией о том, как создать файлы трассировки, вы можете обратиться к специалистам Службы технической поддержки.

Все созданные файлы трассировки mmsc-плагина расположены в папке, указанной пользователем во время настройки ключей реестра.

Файлы трассировки веб-плагина управления

Если для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes вы используете Web Console, информация о событиях, возникающих во время работы веб-плагина управления, может записываться в файлы трассировки веб-плагина.

Файлы трассировки веб-плагина создаются автоматически, если в мастере установки Web Console включена запись в журнал активности Web Console (см. подробнее в справке Kaspersky Security Center).

Файлы трассировки веб-плагинов сохраняются в папке установки Web Console во вложенной папке logs.

Содержимое файлов трассировки плагинов управления

В файлах трассировки содержатся следующие общие данные:

- время возникновения события;
- номер потока исполнения;
- компонент приложения, инициировавший событие;
- уровень важности события (информационное событие, предупреждение, критическое событие, ошибка);
- описание события, связанного с выполнением команды компонентом приложения, и результат выполнения этой команды.

Помимо общих данных файлы трассировки могут содержать следующую информацию:

- персональные данные, в том числе фамилию, имя и отчество, если эти данные являются частью пути к файлам;
- имя учетной записи для входа в операционную систему, если имя учетной записи является частью имени файла.

О файлах дампа

Файл дампа содержит всю информацию о рабочей памяти процессов приложения Kaspersky Industrial CyberSecurity for Linux Nodes на момент создания файла дампа. По умолчанию файлы дампа не создаются. Вы можете включать и выключать запись дампов (см. раздел "Включение и выключение записи дампов" на стр. [667](#)) при сбое в работе приложения.

Если вы включили запись дампов, по умолчанию файлы дампа хранятся в директориях `/var/opt/kaspersky/kics/common/dumps` и `/var/opt/kaspersky/kics/common/dumps-user`.

Для доступа к файлам дампа требуются root-права.

Файлы дампа хранятся на устройстве в течение всего времени использования приложения и удаляются без возможности восстановления при удалении приложения. Автоматическая отправка файлов дампа в "Лабораторию Касперского" не выполняется.

Файлы дампа могут содержать персональные данные. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Включение и выключение записи дампов

Если вы управляете приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Kaspersky Security Center, вы можете включать и выключать запись дампов в параметрах политики Kaspersky Industrial CyberSecurity for Linux Nodes с помощью Web Console или Консоли администрирования.

Если вы управляете приложением через командную строку, вы можете включать и выключать запись дампов с помощью конфигурационного файла `kics.ini` (см. раздел "Предустановленные конфигурационные файлы" на стр. [702](#)).

Максимальное количество файлов дампов ограничено.

При некоторых параметрах операционной системы пользовательские файлы дампа могут не создаваться. Убедитесь, что значение параметра `sysctl kernel.yama.ptrace_scope=0`.

Включение и выключение записи дампов в Web Console

В Web Console вы можете включать и выключать запись дампов в свойствах политики (см. раздел "Управление политиками в Web Console" на стр. [102](#)) (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Параметры трассировки и записи дампов**) (см. таблицу ниже).

Таблица 243. Параметры записи дампов

Параметр	Описание
Создавать файл дампа при сбое в работе приложения	Флажок включает или выключает создание файла дампа (см. раздел "О файлах дампа" на стр. 667) при сбое в работе приложения. По умолчанию флажок снят.
Путь к директории с файлами дампа	Поле ввода пути к директории, в которой хранятся файлы дампа. Размер поля ввода ограничен 128 символами. Значение по умолчанию: <code>/var/opt/kaspersky/kics/common/dumps</code> .

Для применения параметров записи дампов требуется перезапустить приложение.

Включение и выключение записи дампов в Консоли администрирования

В Консоли администрирования вы можете включать и выключать запись дампов в свойствах политики (см. раздел "Управление политиками в Консоли администрирования" на стр. [107](#)) (**Общие параметры** → **Параметры приложения**).

В блоке **Параметры трассировки и записи дампов** по ссылке **Настроить** открывается окно, в котором вы можете настроить параметры записи дампов (см. таблицу ниже).

Таблица 244. Параметры записи дампов

Параметр	Описание
Создавать файл дампа при сбое в работе приложения	Флажок включает или выключает создание файла дампа (см. раздел "О файлах дампа" на стр. 667) при сбое в работе приложения. По умолчанию флажок снят.
Путь к директории с файлами дампа	Поле ввода пути к директории, в которой хранятся файлы дампа. Размер поля ввода ограничен 128 символами. Значение по умолчанию: <code>/var/opt/kaspersky/kics/common/dumps</code> .

Для применения параметров записи дампов требуется перезапустить приложение.

Включение и выключение записи дампов в командной строке

► Чтобы включить или выключить запись дампов с помощью конфигурационного файла `kics.ini`:

1. Остановите Kaspersky Industrial CyberSecurity for Linux Nodes.
2. Откройте файл `/var/opt/kaspersky/kics/common/kics.ini` на редактирование.
3. В секции **[General]** установите значение параметра:
 - `CoreDumps=yes` – включить запись дампов при сбое в работе приложения.
 - `CoreDumps=no` – выключить запись дампов.
4. Если вы хотите изменить директорию, в которой сохраняются файлы дампа по умолчанию, укажите путь к директории в параметре `CoreDumpsPath`.
5. Запустите Kaspersky Industrial CyberSecurity for Linux Nodes.

Об удаленной диагностике устройства с помощью Kaspersky Security Center

В Kaspersky Security Center вы можете выполнять удаленную диагностику клиентских устройств. Процедура удаленной диагностики позволяет удаленно выполнять следующие операции:

- включать и выключать трассировку;
- изменять уровень трассировки;
- загружать файлы трассировки;
- загружать журнал удаленной установки приложения;
- загружать системные журналы событий (syslog);
- запускать, останавливать и перезапускать приложения.

Удаленная диагностика с помощью Web Console

Если вы управляете приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Web Console, удаленная диагностика клиентского устройства выполняется в окне удаленной диагностики.

► Чтобы открыть окно удаленной диагностики устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
Откроется список управляемых устройств.
2. Выберите устройство, для которого вы хотите выполнить удаленную диагностику, и нажмите на название устройства.
Откроется окно свойств устройства.
3. На закладке **Дополнительно** выберите раздел **Удаленная диагностика**.

В окне удаленной диагностики устройства вы можете посмотреть журнал удаленной установки приложения.

► *Чтобы просмотреть журнал удаленной установки приложения на устройстве:*

1. Откройте окно удаленной диагностики устройства.
2. На закладке **Журналы событий** в блоке **Файлы трассировки** нажмите на ссылку **Журналы удаленной установки**.

Откроется окно **Журналы событий трассировки устройства**.

Подробнее об удаленной диагностике см. в справке Kaspersky Security Center.

Удаленная диагностика с помощью Консоли администрирования

Если вы управляете приложением Kaspersky Industrial CyberSecurity for Linux Nodes через Консоль администрирования, удаленная диагностика выполняется с помощью специальной утилиты удаленной диагностики Kaspersky Security Center, которая автоматически устанавливается на устройство совместно с Консолью администрирования.

► *Чтобы открыть главное окно утилиты удаленной диагностики устройства:*

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите закладку **Устройства**.
3. В списке управляемых устройств выберите устройство, к которому вы хотите подключить утилиту удаленной диагностики, и в контекстном меню устройства выберите пункт **Внешние инструменты** → **Удаленная диагностика**.

Откроется главное окно утилиты удаленной диагностики **Утилита удаленной диагностики Kaspersky Security Center**.

С помощью утилиты удаленной диагностики устройства вы можете посмотреть журнал удаленной установки приложения.

► *Чтобы просмотреть журнал удаленной установки приложения на устройстве:*

1. Откройте главное окно утилиты удаленной диагностики устройства.
2. Если требуется, настройте параметры подключения утилиты к устройству. В главном окне утилиты удаленной диагностики нажмите на кнопку **Войти**.
3. В открывшемся окне в дереве объектов выберите папку **Журналы удаленной установки**.

Подробнее об утилите удаленной диагностики см. в справке Kaspersky Security Center (<https://support.kaspersky.com/KSC/14.2/ru-RU/13052.htm>).

Приложения

Этот раздел содержит информацию, которая дополняет основной текст справки.

В этом разделе

Приложение 1. Оптимизация потребления ресурсов.....	671
Приложение 2. Команды управления Kaspersky Industrial CyberSecurity for Linux Nodes	676
Приложение 3. Конфигурационные файлы и параметры приложения по умолчанию	700
Приложение 4. Коды возврата командной строки	735
Приложение 5. Настройка совместной работы с SIEM-системами.....	735
Приложение 6. Значения параметров приложения в сертифицированной конфигурации	737

Приложение 1. Оптимизация потребления ресурсов

При проверке объектов Kaspersky Industrial CyberSecurity for Linux Nodes использует ресурсы процессора, ввод-вывод дисковой подсистемы и оперативную память.

► Чтобы посмотреть потребление ресурсов приложением, выполните следующую команду:

```
top -bn1|grep kics
```

Выполнять команду требуется в момент нагрузки на систему.

Вывод команды показывает количество потребляемой памяти и занимаемого процессорного времени:

```
651 root 20 0 3014172 2.302g 154360 S 120.0 30.0 0:32.80 kics
```

В столбце 6 отображается количество резидентной памяти – 2.302g.

В столбце 9 отображается процент использования ядер процессора – 120.0, где каждое ядро принимается за 100 процентов. Таким образом, 120% означает, что одно ядро занято полностью, а второе – на 20%.

Если работа Kaspersky Industrial CyberSecurity for Linux Nodes при проверке объектов критически замедляет работу системы, требуется провести настройку приложения для оптимизации потребления ресурсов системы.

В этом разделе

Определение задачи, которая занимает ресурсы	672
Настройка задачи Защита от файловых угроз.....	674
Настройка задачи проверки по требованию.....	675
Установка ограничения на использование памяти приложением.....	675

Определение задачи, которая занимает ресурсы

Для того чтобы определить, какая задача или задачи приложения занимают ресурсы системы, требуется разделить потребление ресурсов задачами Защита от файловых угроз (см. раздел "Анализ работы задачи Защита от файловых угроз" на стр. [672](#)) (тип OAS) и задачами проверки по требованию (см. раздел "Анализ работы задач проверки по требованию" на стр. [673](#)) (типы ODS и ContainerScan).

Если приложение находится под управлением политики Kaspersky Security Center, требуется на время проведения исследования разрешить управление локальными задачами.

В этом разделе

Анализ работы задачи Защита от файловых угроз	672
Анализ работы задач проверки по требованию	673

Анализ работы задачи Защита от файловых угроз

► Чтобы проанализировать работу задачи Защита от файловых угроз:

1. Остановите все задачи проверки и мониторинга.
2. Убедитесь, что задачи проверки по требованию не будут запущены во время проверки или не имеют расписания. Вы можете сделать это через Kaspersky Security Center или локально, выполнив следующие действия:
 - a. Получите список всех задач приложения, выполнив следующую команду:

```
kics-control --get-task-list
```

- b. Получите параметры расписания задачи поиска вредоносного ПО, выполнив следующую команду:

```
kics-control --get-schedule <ID задачи>
```

Если команда выводит RuleType=Manual, то задача запускается только вручную.

- c. Получите параметры расписания всех ваших задач поиска вредоносного ПО и выборочной проверки, если такие были созданы, и укажите им запуск вручную, выполнив следующую команду:

```
kics-control --set-schedule <ID задачи> RuleType=Manual
```

3. Включите создание файлов трассировки приложения с высоким уровнем детализации, выполнив следующую команду:

```
kics-control --set-app-settings TraceLevel=Detailed
```

4. Запустите задачу Защита от файловых угроз, если она не была запущена, выполнив следующую команду:

```
kics-control --start-task 1
```

5. Создайте нагрузку на систему в том же режиме, который вызвал проблемы с производительностью, достаточно нескольких часов.

Под нагрузкой приложение записывает много информации в файлы трассировки, при этом по умолчанию хранится 5 файлов по 500 МБ, поэтому старая информация будет перезаписываться. Если проблемы с производительностью и потреблением ресурсов перестали проявляться, значит, скорее всего, проблемы вызывают задачи проверки по требованию и можно перейти к анализу

работы задач проверки с типами ContainerScan и ODS (см. раздел "Анализ работы задач проверки по требованию" на стр. [673](#)).

6. Выключите создание файлов трассировки приложения, выполнив следующую команду:

```
kics-control --set-app-settings TraceLevel=None
```

7. Определите список объектов, которые были проверены наибольшее количество раз, выполнив следующую команду:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kics/kics.* | awk '{print $8}' |  
sort | uniq -c | sort -k1 -n -r | less
```

Результат загружается в приложение просмотра текста less, где в самом начале отображаются те объекты, которые были проверены наибольшее количество раз.

8. Определите, являются ли опасными объекты, которые были проверены наибольшее количество раз. В случае затруднения обратитесь в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. [661](#)).

Например, неопасными можно признать директории и файлы журналов, если запись в них ведет доверенный процесс, файлы баз данных.

9. Запишите пути к неопасным, по вашему мнению, объектам, они потребуются в дальнейшем для настройки исключений из проверки.
10. Если в системе осуществляется частая запись файлов различными сервисами, такие файлы будут повторно проверяться в отложенной очереди. Определите список путей, которые были проверены в отложенной очереди наибольшее количество раз, выполнив следующую команду:

```
fgrep 'SYSCALL' /var/log/kaspersky/kics/kics.* | fgrep  
'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $9}' | sort | uniq -c | sort -  
k1 -n -r
```

Файлы, проверенные наибольшее количество раз, будут отображаться в начале списка.

11. Если счетчик по одному файлу превышает несколько тысяч за несколько часов, определите, можно ли доверять этому файлу, чтобы исключить его из проверки.

Логика определения такая же, как и для предыдущего исследования (см. п. 8): файлы журналов можно признать неопасными, так как они не могут быть запущены.

12. Даже если некоторые файлы исключены из проверки постоянной защитой, они все равно могут перехватываться приложением. Если исключение определенных файлов из постоянной защиты не приносит существенного прироста производительности, вы можете полностью исключить из перехвата приложением точку монтирования, где расположены эти файлы. Для этого выполните следующие действия:

- a. Получите список файлов, перехваченных приложением, выполнив следующую команду:

```
grep 'FACACHE.*needs' /var/log/kaspersky/kics/kics.* | awk '{print  
$9}' | sort | uniq -c | sort -k1 -n -r
```

- b. С помощью полученного списка определите пути, по которым происходит большое количество перехватов файловых операций, и настройте исключения из перехвата (см. раздел "Настройка задачи Защита от файловых угроз" на стр. [674](#)).

Анализ работы задач проверки по требованию

Также большое потребление ресурсов может быть вызвано использованием задач с типами ODS и ContainerScan. Следуйте следующим рекомендациям по использованию задач с типом ODS:

- Убедитесь, что не выполняется запуск нескольких задач проверки по требованию одновременно. Приложение позволяет работать в таком режиме, но потребление ресурсов может сильно увеличиться. Проверьте расписание всех задач с типами ODS и ContainerScan локально (как описано для задачи Защита от файловых угроз (см. раздел "Анализ работы задачи Защита от файловых угроз" на стр. [672](#))) или через Kaspersky Security Center.
- Запускайте проверку во время наименьшей нагрузки на сервер.
- Убедитесь, что по указанному пути проверки нет примонтированных удаленных ресурсов (SMB / NFS). Если задача состоит в проверке удаленного ресурса и нет возможности выполнять ее непосредственно на сервере, предоставляющем ресурс, не выполняйте проверку на серверах с критическими сервисами, так как такая задача может выполняться достаточно долго (в зависимости от скорости соединения и количества файлов).
- Выполните оптимизацию параметров задачи проверки по требованию перед запуском.

Настройка задачи Защита от файловых угроз

Если после выполнения анализа работы задачи Защита от файловых угроз (см. раздел "Анализ работы задачи Защита от файловых угроз" на стр. [672](#)) вы сформировали список директорий и файлов, которые можно исключить из проверки задачи, вам нужно добавить их в исключения.

Исключения из проверки

- Чтобы исключить директорию `/tmp/logs` и все поддиректории и файлы рекурсивно, выполните следующую команду:

```
kics-control --set-settings 1 --add-exclusion /tmp/logs
```

- Чтобы исключить конкретный файл или файлы по маске в директории `/tmp/logs`, выполните следующую команду:

```
kics-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

- Чтобы исключить по рекурсивной маске все файлы с расширением `.log` в директории `/tmp/` и поддиректориях, выполните следующую команду:

```
kics-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Исключения из перехвата

Если вы хотите исключить файлы определенной директории не только из проверки, но и из перехвата, вы можете исключить точку монтирования целиком.

- Чтобы исключить точку монтирования целиком:

1. Если директория не является точкой монтирования, нужно создать из нее точку монтирования. Например, чтобы создать точку монтирования из директории `/tmp`, выполнив следующую команду:

```
mount --bind /tmp/ /tmp
```

2. Чтобы точка монтирования сохранилась после перезагрузки сервера, добавьте в файл `/etc/fstab` следующую строку:

```
/tmp /tmp none defaults,bind 0 0
```

3. Добавьте директорию /tmp в глобальные исключения, выполнив следующую команду:

```
kics-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
```
4. Если требуется добавить несколько директорий, увеличивайте счетчик item_0000 на единицу (item_0001, item_0002 и так далее).

Исключать точки монтирования также рекомендуется, если это примонтированный удаленный ресурс с нестабильным или медленным соединением.

Изменение типа проверки

По умолчанию задача Защита от файловых угроз может проверять файлы при открытии и закрытии. Если в ходе анализа работы задачи Защита от файловых угроз (см. раздел "Анализ работы задачи Защита от файловых угроз" на стр. [672](#)) было выявлено слишком много записываемых файлов, вы можете перевести задачу в режим работы только при открытии файлов, выполнив следующую команду:

```
kics-control --set-set 1 ScanByAccessType=Open
```

При таком режиме работы изменения, внесенные в файл после открытия, не будут проверяться до следующего обращения к файлу.

Настройка задачи проверки по требованию

Исключения из проверки

Для задач проверки по требованию с типами ODS и ContainerScan вы можете настроить исключения из проверки. Настройка выполняется аналогично настройке исключений из проверки для задачи Защита от файловых угроз (см. раздел "Настройка задачи Защита от файловых угроз" на стр. [674](#)).

Параметры исключений из проверки для одной задачи проверки не действуют на другие задачи проверки. Для каждой задачи проверки требуется настроить свои исключения.

Ограничение использования памяти для распаковки архивов

Задача проверки по требованию при рекурсивной проверке во время проверки архивов будет распаковывать их, используя оперативную память. По умолчанию приложение имеет ограничение в 40% от всей доступной оперативной памяти, но не менее 2 ГБ. Поэтому если система имеет более 5 ГБ оперативной памяти, можно установить ограничение на использование памяти вручную (см. раздел "Установка ограничения на использование памяти приложением" на стр. [675](#)). Это особенно актуально для серверов, имеющих сотни гигабайт оперативной памяти.

Установка ограничения на использование памяти приложением

Вы можете ограничивать количество оперативной памяти, которое приложением Kaspersky Industrial CyberSecurity for Linux Nodes использует во время выполнения задач проверки с типами OAS, ODS и ContainerScan. По умолчанию приложение использует не более 40% от всей доступной оперативной памяти. Для систем с большим объемом оперативной памяти (более 5 ГБ) ограничение на использование памяти может быть полезным.

Вы можете регулировать размер оперативной памяти, используемой приложением при проверке файлов, с помощью параметра `ScanMemoryLimit` в конфигурационном файле `kics.ini`. Значение параметра по умолчанию: 8192 МБ.

Параметр ограничивает только количество памяти, которое используется при проверке файлов, то есть общий размер памяти, потребляемый приложением, может быть больше значения, заданного этим параметром.

► Чтобы указать ограничение на использование памяти при проверке файлов:

1. Остановите Kaspersky Industrial CyberSecurity for Linux Nodes.
2. Откройте файл `/var/opt/kaspersky/kics/common/kics.ini` на редактирование.
3. В секции **[General]**: укажите нужное количество оперативной памяти в значении параметра `ScanMemoryLimit`:

```
ScanMemoryLimit=<количество памяти в мегабайтах>
```

Минимальное значение параметра: 2048 МБ. Если вы указали значение меньше 2048 МБ, приложение будет использовать минимальное значение.

Если вы указали значение, превышающее размер оперативной памяти системы, приложение будет использовать до 40% от всей доступной оперативной памяти.

4. Запустите Kaspersky Industrial CyberSecurity for Linux Nodes.

Ограничение на использование памяти при проверке файлов изменится при перезапуске приложения.

Приложение 2. Команды управления Kaspersky Industrial CyberSecurity for Linux Nodes

Управление приложением Kaspersky Industrial CyberSecurity for Linux Nodes в командной строке выполняется с помощью команд управления Kaspersky Industrial CyberSecurity for Linux Nodes.

Вы можете посмотреть справку по командам управления с помощью команды:

```
kics-control --help <префикс группы команд>
```

где `<префикс группы команд>` может принимать следующие значения:

- -A – команды управления контролем приложений (см. раздел "Контроль приложений" на стр. [431](#)).
- -B – команды управления резервным хранилищем (см. раздел "Резервное хранилище" на стр. [586](#)).
- -C – команды управления общими параметрами проверки контейнеров (см. раздел "Мониторинг контейнеров" на стр. [322](#)).
- -D – команды управления контролем устройств (см. раздел "Контроль устройств" на стр. [464](#)).
- -E – команды управления событиями приложения (см. раздел "Просмотр событий в командной строке" на стр. [642](#)).
- -F – команды управления сетевым экраном.

- -H – команды управления заблокированными устройствами (см. раздел "Управление заблокированными устройствами" на стр. [429](#)).
- -L – команды управления лицензионными ключами.
- -N – команды управления параметрами проверки защищенных соединений (см. раздел "Проверка защищенных соединений" на стр. [388](#)).
- -K – команды управления параметрами интеграции приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Industrial CyberSecurity for Networks (см. раздел "Интеграция с Kaspersky Industrial CyberSecurity for Networks" на стр. [592](#)).
- -R – команды управления параметрами интеграции приложения Kaspersky Industrial CyberSecurity for Linux Nodes с Kaspersky Endpoint Detection and Response Optimum (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response Optimum" на стр. [610](#)).
- -S – команды статистики.
- -T – команды управления задачами и параметрами приложения (см. раздел "Управление приложением через командную строку" на стр. [118](#)).
- -U – команды управления пользователями и ролями пользователей (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. [77](#)).
- -W – команды вывода событий (см. раздел "Просмотр событий в командной строке" на стр. [642](#)).

В этом разделе

Команды управления параметрами и задачами приложения	677
Команды статистики	688
Команды вывода событий	688
Команды управления событиями приложения	689
Команды управления лицензионными ключами	690
Команды управления сетевым экраном	691
Команды управления заблокированными устройствами	693
Команды управления Контролем устройств	694
Команды управления Контролем приложений	694
Команды управления Веб-Контролем	696
Команды управления резервным хранилищем	696
Команды управления пользователями и ролями	698
Команды управления параметрами интеграции с Kaspersky Industrial CyberSecurity for Networks ..	698
Команды управления параметрами интеграции с Kaspersky Endpoint Detection and Response Optimum	699

Команды управления параметрами и задачами приложения

-T – префикс, указывающий, что команда принадлежит к группе команд управления параметрами и задачами приложения.

-C – префикс, указывающий, что команда принадлежит к группе команд управления общими параметрами проверки контейнеров (см. раздел "Мониторинг контейнеров" на стр. [322](#)).

-N – префикс, указывающий, что команда принадлежит к группе команд управления параметрами проверки защищенных соединений (см. раздел "Проверка защищенных соединений" на стр. [388](#)).

Команда kics-control --export-settings

Команда позволяет вывести в консоль или экспортировать в конфигурационный файл все параметры приложения (включая общие параметры проверки контейнеров, параметры проверки защищенных соединений, общие параметры приложения и параметры задач).

Синтаксис команды

```
kics-control [-T] --export-settings [--file <путь к конфигурационному файлу>] [-json]
```

Аргументы и ключи

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу, в который будут сохранены параметры приложения.

--json – выводить параметры в формате JSON. Если вы не укажете ключ --json, параметры будут выведены в формате INI.

Команда kics-control --import-settings

Команда позволяет импортировать из конфигурационного файла все параметры приложения (включая общие параметры проверки контейнеров, параметры проверки защищенных соединений, общие параметры приложения и параметры задач).

Синтаксис команды

```
kics-control [-T] --import-settings --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу, параметры из которого будут импортированы в приложение.

--json – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ --json, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команда kics-control --update-application

Команда позволяет установить загруженное обновление модулей приложения.

Синтаксис команды

```
kics-control [-T] --update-application
```

В этом разделе

Команды управления общими параметрами приложения	679
Команды управления параметрами задач	680
Команды управления задачами.....	682
Команды управления общими параметрами проверки контейнеров.....	685
Команды управления параметрами проверки защищенных соединений	686

Команды управления общими параметрами приложения

Команда `kics-control --get-app-settings`

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения общих параметров приложения.

Синтаксис команды

```
kics-control [-T] --get-app-settings [--file <путь к конфигурационному файлу>]
[--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены общие параметры приложения. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда `kics-control --set-app-settings`

Команда позволяет устанавливать значения общих параметров приложения с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kics-control [-T] --set-app-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kics-control [-T] --set-app-settings --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`<имя параметра>=<значение параметра>` – имя и значение одного из общих параметров приложения.

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, параметры из которого будут импортированы в приложение.

`--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команды управления параметрами задач

Команда `kics-control --get-settings`

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения параметров указанной задачи.

Синтаксис команды

```
kics-control [-T] --get-settings <идентификатор/имя задачи> [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены параметры задачи. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда `kics-control --set-settings`

Команда позволяет устанавливать значения параметров указанной задачи с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kics-control [-T] --set-settings <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>] [--add-path <путь>] [--del-path <путь>] [--add-exclusion <путь>] [--del-exclusion <путь>]
```

Задать параметры с помощью конфигурационного файла:

```
kics-control [-T] --set-settings <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

`<имя параметра>=<значение параметра>` – имя и значение одного из параметров задачи.

`--add-path <путь>` – добавить путь к директории с проверяемыми объектами.

`--del-path <путь>` – удалить путь к директории с проверяемыми объектами.

`--add-exclusion <путь>` – добавить путь к директории с объектами, которые нужно исключить из проверки.

`--del-exclusion <путь>` – удалить путь к директории с исключаемыми объектами.

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры задачи.

`--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команда `kics-control --set-to-default`

Команда позволяет восстановить значения по умолчанию для параметров указанной задачи.

Синтаксис команды

```
kics-control [-T] --set-settings <идентификатор/имя задачи> --set-to-default
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда `kics-control --get-schedule`

Команда позволяет вывести в консоль или в конфигурационный файл текущее расписание запуска указанной задачи.

Синтаксис команды

```
kics-control [-T] --get-schedule <идентификатор/имя задачи> [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены параметры расписания задачи. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kics-control --set-schedule

Команда позволяет устанавливать расписание указанной задачи с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kics-control [-T] --set-schedule <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kics-control [-T] --set-schedule <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

<идентификатор/имя задачи> – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

<имя параметра>=<значение параметра> – имя и значение одного из параметров расписания задач (см. раздел "Параметры расписания задач" на стр. [734](#)).

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу, из которого будут импортированы параметры расписания задачи.

--json – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ --json, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команды управления задачами

Команда kics-control --get-task-list

Команда позволяет вывести список существующих задач (см. раздел "Просмотр списка задач в командной строке" на стр. [126](#)) приложения.

Синтаксис команды

```
kics-control [-T] --get-task-list [--json]
```

Аргументы и ключи

--json – выводить параметры в формате JSON.

Команда kics-control --get-task-state

Команда позволяет вывести состояние (см. раздел "Просмотр состояния задачи в командной строке" на стр. [126](#)) указанной задачи.

Синтаксис команды

```
kics-control [-T] --get-task-state <идентификатор/имя задачи> [--json]
```

Аргументы и ключи

<идентификатор/имя задачи> – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

`--json` – выводить параметры в формате JSON.

Команда `kics-control --create-task`

Команда позволяет создать задачу (см. раздел "Создание задачи в командной строке" на стр. [127](#)) указанного типа с параметрами по умолчанию или с параметрами, указанными в конфигурационном файле.

Синтаксис команды

Создать задачу с параметрами по умолчанию:

```
kics-control [-T] --create-task <имя задачи> --type <тип задачи>
```

Создать задачу с параметрами из конфигурационного файла:

```
kics-control [-T] --create-task <имя задачи> --type <тип задачи> [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`<имя задачи>` – имя, которое вы задаете для новой задачи.

`<тип задачи>` – обозначение типа создаваемой задачи (см. раздел "Управление задачами в командной строке" на стр. [119](#)).

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу (см. раздел "Параметры задач командной строки по умолчанию" на стр. [711](#)), параметры из которого будут использоваться при создании задачи.

`--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команда `kics-control --delete-task`

Команда позволяет удалить (см. раздел "Удаление задачи в командной строке" на стр. [128](#)) задачу.

Синтаксис команды

```
kics-control [-T] --delete-task <идентификатор/имя задачи>
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда `kics-control --start-task`

Команда позволяет запустить (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачу.

Синтаксис команды

```
kics-control [-T] --start-task <идентификатор/имя задачи> [-W] [--progress]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

`[-W]` – включить вывод текущих событий (см. раздел "Команды вывода событий" на стр. [688](#)).

[--progress] – отображать ход выполнения задачи.

Команда kics-control --stop-task

Команда позволяет остановить (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачу.

Синтаксис команды

```
kics-control [-T] --stop-task <идентификатор/имя задачи> [-W]
```

Аргументы и ключи

<идентификатор/имя задачи> – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

[-W] – включить вывод текущих событий (см. раздел "Команды вывода событий" на стр. [688](#)).

Команда kics-control --suspend-task

Команда позволяет приостановить (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) задачу.

Синтаксис команды

```
kics-control [-T] --suspend-task <идентификатор/имя задачи>
```

Аргументы и ключи

<идентификатор/имя задачи> – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда kics-control --resume-task

Команда позволяет возобновить (см. раздел "Запуск, остановка, приостановка и возобновление задачи в командной строке" на стр. [128](#)) выполнение задачи.

Синтаксис команды

```
kics-control [-T] --resume-task <идентификатор/имя задачи>
```

Аргументы и ключи

<идентификатор/имя задачи> – идентификатор (см. раздел "Управление задачами в командной строке" на стр. [119](#)), присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда kics-control --scan-file

Команда позволяет создать и запустить задачу выборочной проверки (см. раздел "Выборочная проверка файлов и директорий" на стр. [265](#)).

Синтаксис команды

```
kics-control [-T] --scan-file <путь> [--action <действие>]
```

Аргументы и ключи

<путь> – путь к файлу или директории, которые нужно проверить. Вы можете указать несколько путей, разделяя их пробелами.

`--action <действие>` – действие, которое приложение будет выполнять над зараженными объектами. Если вы не укажете ключ `--action`, приложение будет выполнять рекомендуемое действие.

Команда `kics-control --scan-container`

Команда позволяет создать и запустить задачу выборочной проверки контейнера или образа (см. раздел "Выборочная проверка контейнеров и образов" на стр. [352](#)).

Синтаксис команды

```
kics-control [-T] --scan-container <контейнер/образ[:тер]>
```

Аргументы и ключи

`<контейнер/образ[:тер]>` – имя или идентификатор контейнера или образа. Для проверки нескольких объектов можно использовать маски.

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/**/*.file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `.`. Например, `/dir/**/file*` или `/dir/file**/.`

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Команды управления общими параметрами проверки контейнеров

Команда `kics-control --get-container-settings`

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения общих параметров проверки контейнеров.

Синтаксис команды

```
kics-control [-C] --get-container-settings [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены общие параметры проверки контейнеров. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kics-control --set-container-settings

Команда позволяет устанавливать значения общих параметров проверки контейнеров с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kics-control [-C] --set-container-settings <имя параметра>=<значение параметра>
[<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kics-control [-C] --set-container-settings --file <путь к конфигурационному файлу>
[--json]
```

Аргументы и ключи

<имя параметра>=<значение параметра> – имя и значение одного из общих параметров проверки контейнеров (см. раздел "Общие параметры проверки контейнеров" на стр. [728](#)).

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу, из которого в приложение будут импортированы общие параметры проверки контейнеров.

--json – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ --json, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команды управления параметрами проверки защищенных соединений

-N – префикс, указывающий, что команда принадлежит к группе команд управления параметрами проверки защищенных соединений (см. раздел "Проверка защищенных соединений" на стр. [388](#)).

Команда kics-control -N --query

Команда позволяет выводить списки исключений из проверки защищенных соединений:

- список исключений, добавленных пользователем;
- список исключений, добавленных приложением;
- список исключений, полученных из баз приложения.

Синтаксис команды

```
kics-control -N --query user
kics-control -N --query auto
kics-control -N --query kl
```

Команда kics-control --clear-web-auto-excluded

Команда позволяет очистить список доменов, которые приложение автоматически исключило из проверки.

Синтаксис команды

```
kics-control -N --clear-web-auto-excluded
```

Команда kics-control --get-net-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения параметров проверки защищенных соединений.

Синтаксис команды

```
kics-control [-N] --get-net-settings [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены параметры проверки защищенных соединений. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kics-control --set-net-settings

Команда позволяет устанавливать значения параметров проверки защищенных соединений с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kics-control [-N] --set-net-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kics-control [-N] --set-net-settings --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`<имя параметра>=<значение параметра>` – имя и значение одного из параметров проверки защищенных соединений (см. раздел "Параметры проверки защищенных соединений" на стр. [731](#)).

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры проверки защищенных соединений.

`--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команда kics-control --add-certificate

Команда позволяет добавить сертификат в список сертификатов, которые приложение будет считать доверенными.

Синтаксис команды

```
kics-control [-N] -add-certificate <путь к сертификату>
```

Аргументы и ключи

<путь к сертификату> – путь к файлу сертификата, который вы хотите добавить, в формате PEM или DER.

Команда `kics-control --remove-certificate`

Команда позволяет удалить сертификат из списка доверенных сертификатов.

Синтаксис команды

```
kics-control [-N] --remove-certificate <субъект сертификата>
```

Команда `kics-control --list-certificates`

Команда позволяет вывести список доверенных сертификатов (см. раздел "Управление списком доверенных сертификатов" на стр. [397](#)).

Синтаксис команды

```
kics-control [-N] --list-certificates
```

Команды статистики

-S – префикс указывающий, что команда принадлежит к группе команд статистики.

Команда `kics-control --app-info`

Команда позволяет вывести информацию о приложении.

Синтаксис команды

```
kics-control [-S] --app-info [--json]
```

Аргументы и ключи

--json – выводить параметры в формате JSON.

Команда `kics-control --omsinfo`

Команда позволяет создать файл формата JSON для интеграции с Microsoft Operations Management Suite.

Синтаксис команды

```
kics-control [-S] --omsinfo --file <имя и путь к файлу>
```

Команды вывода событий

Команда `kics-control -W`

Команда включает вывод текущих событий приложения. Команда возвращает название события и дополнительную информацию о событии. Вы можете использовать команду для вывода всех текущих событий приложения или только событий, связанных с запущенной задачей (см. раздел "Об источниках и схемах обновления" на стр. [160](#)).

Синтаксис команды

```
kics-control -W [--query "<условия фильтра>"]
```

Аргументы и ключи

<условия фильтра> – одно или несколько логических выражений (см. раздел "Использование фильтра для ограничения результатов запросов" на стр. [140](#)) в формате <поле> <операция сравнения> '<значение>', скомбинированных с помощью логического оператора and, для вывода определенных текущих событий.

Команды управления событиями приложения

-E – префикс, указывающий, что команда принадлежит к группе команд управления событиями приложения (см. раздел "Просмотр событий в командной строке" на стр. [642](#)).

Команда kics-control -E

Команда позволяет вывести информацию обо всех событиях из журнала событий приложения. С помощью утилиты less вы можете перемещаться по списку отображаемых событий.

Синтаксис команды

```
kics-control -E
```

Команда kics-control -E --query

Команда позволяет вывести информацию о событиях из журнала событий приложения. С помощью утилиты less вы можете перемещаться по списку отображаемых событий. Вы можете использовать фильтр для вывода определенных событий, а также выводить список событий в указанный файл.

Синтаксис команды

```
kics-control -E --query "<условия фильтра>" [--db <файл базы данных>] [-n <количество>] [--file <имя и путь к файлу>] [--json] [--reverse]
```

Аргументы и ключи

<файл базы данных> – полный путь к файлу базы данных журнала событий, из которого вы хотите вывести события. По умолчанию приложение сохраняет информацию о событиях в базе данных /var/opt/kaspersky/kics/private/storage/events.db. Расположение базы данных определяется общим параметром приложения EventsStoragePath.

<условия фильтра> – одно или несколько логических выражений (см. раздел "Использование фильтра для ограничения результатов запросов" на стр. [140](#)) в формате <поле> <операция сравнения> '<значение>', скомбинированных с помощью логического оператора and, для ограничения результатов запроса.

<количество> – количество последних событий из выборки (то есть количество записей от конца выборки), которые нужно вывести.

--file <имя и путь к файлу> – полный путь к файлу, в который вы хотите вывести события. Если вы укажете имя файла, не указав путь к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, файл не будет создан.

Если вы не укажете ключ `--file`, список событий будет выведен в консоль.

`--json` – выводить события в формате JSON.

`--reverse` – выводить события в обратном порядке (от самого нового события наверху к более старым внизу).

Команды управления лицензионными ключами

`-L` – префикс, указывающий, что команда принадлежит к группе команд управления лицензионными ключами.

Команда `kics-control --add-active-key`

Команда позволяет добавить в приложение активный лицензионный ключ с помощью файла ключа.

С помощью этой команды вы можете добавить как активный лицензионный ключ приложения, так и активный лицензионный ключ EDR Optimum. Указывать тип ключа в команде не требуется.

Синтаксис команды

```
kics-control [-L] --add-active-key <путь к файлу ключа>
```

Аргументы и ключи

`<путь к файлу ключа>` – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

Добавить ключ с помощью файла `/home/test/00000001.key` в качестве активного ключа:

```
kics-control --add-active-key /home/test/00000001.key
```

Команда `kics-control --add-reserve-key`

Команда позволяет добавить в приложение резервный лицензионный ключ с помощью файла ключа.

С помощью этой команды вы можете добавить как резервный лицензионный ключ приложения, так и резервный лицензионный ключ EDR Optimum. Указывать тип ключа в команде не требуется.

Если активный ключ еще не добавлен в приложение на устройстве, команда завершается с ошибкой.

Синтаксис команды

```
kics-control [-L] --add-reserve-key <путь к файлу ключа>
```

Аргументы и ключи

`<путь к файлу ключа>` – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

Добавить резервный ключ с помощью файла `/home/test/00000002.key`:

```
kics-control --add-reserve-key /home/test/00000002.key
```

Команда `kics-control --remove-active-key`

Команда позволяет удалить активный лицензионный ключ.

Синтаксис команды

```
kics-control [-L] --remove-active-key [--edr-optimum]
```

Аргументы и ключи

`--edr-optimum` – удалить активный лицензионный ключ EDR Optimum.

Если вы не укажете ключ `--edr-optimum`, будет удален активный лицензионный ключ приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

Команда `kics-control --remove-reserve-key`

Команда позволяет удалить резервный лицензионный ключ.

Синтаксис команды

```
kics-control [-L] --remove-reserve-key [--edr-optimum]
```

Аргументы и ключи

`--edr-optimum` – удалить резервный лицензионный ключ EDR Optimum.

Если вы не укажете ключ `--edr-optimum`, будет удален резервный лицензионный ключ приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

Команда `kics-control -L --query`

Команда `-L --query` позволяет вывести информацию о лицензии, по которой активировано приложение, и об используемых ключах (см. раздел "Просмотр информации о лицензии и ключе в командной строке" на стр. [155](#)).

Синтаксис команды

```
kics-control -L --query [--json]
```

Аргументы и ключи

`--json` – выводить данные в формате JSON.

Команды управления сетевым экраном

`-F` – префикс, указывающий, что команда принадлежит к группе команд управления сетевым экраном.

Команда `kics-control --add-rule`

Команда позволяет добавить новое сетевое пакетное правило.

Синтаксис команды

```
kics-control [-F] --add-rule [--name <название правила>] [--action <действие>]  
[--protocol <протокол>] [--direction <направление>] [--remote <удаленный  
адрес>[:<диапазон портов>]] [--local <локальный адрес>[:<диапазон портов>]] [--at  
<индекс>]
```

Аргументы и ключи

`--name <название правила>` – название сетевого пакетного правила.

`--action <действие>` – действие, применяемое к соединениям, указанным в сетевом пакетном правиле.

`--protocol <протокол>` – тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность.

`--direction <направление>` – направление отслеживаемой сетевой активности.

`--remote <удаленный адрес>[:<диапазон портов>]` – сетевой адрес удаленного устройства.

`--local <локальный адрес>[:<диапазон портов>]` – сетевой адрес устройства с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes.

`--at <индекс>` – порядковый номер правила в списке сетевых пакетных правил. Если ключ `--at` не указан или его значение больше количества правил в списке, новое правило добавляется в конец списка.

Для параметров, значения которых вы не указали в команде, устанавливаются значения по умолчанию (см. раздел "Управление сетевым экраном в командной строке" на стр. [370](#)).

Команда `kics-control --del-rule`

Команда позволяет удалить сетевое пакетное правило с указанным названием или с указанным индексом в списке правил.

Синтаксис команды

```
kics-control [-F] --del-rule --name <название правила>
```

```
kics-control [-F] --del-rule --index <индекс>
```

Аргументы и ключи

`--name <название правила>` – название сетевого пакетного правила.

`--index <индекс>` – порядковый номер правила в списке сетевых пакетных правил.

Команда `kics-control --move-rule`

Команда позволяет изменить приоритет выполнения сетевого пакетного правила.

Синтаксис команды

```
kics-control [-F] --move-rule --name <название правила> --at <индекс>
```

```
kics-control [-F] --move-rule --index <индекс> --at <индекс>
```

Аргументы и ключи

`--name <название правила>` – название сетевого пакетного правила.

`--index <индекс>` – текущий порядковый номер правила в списке сетевых пакетных правил.

`--at <индекс>` – новый порядковый номер правила в списке сетевых пакетных правил.

Команда `kics-control --add-zone`

Команда позволяет добавить адрес в сетевую зону.

Синтаксис команды

```
kics-control [-F] --add-zone --zone <зона> --address <адрес>
```

Аргументы и ключи

--zone <зона> – предустановленное имя сетевой зоны.

--address <адрес> – сетевой адрес или подсеть.

Команда kics-control --del-zone

Команда позволяет удалить адрес из сетевой зоны.

Синтаксис команды

```
kics-control [-F] --del-zone --zone <зона> --address <адрес>
```

```
kics-control [-F] --del-zone --zone <зона> --index <индекс адреса>
```

Аргументы и ключи

--zone <зона> – предустановленное имя сетевой зоны.

--address <адрес> – сетевой адрес или подсеть.

--index <индекс адреса> – порядковый номер адреса в сетевой зоне.

Команда kics-control -F --query

Команда позволяет посмотреть правила сетевого экрана, созданные с помощью приложения Kaspersky Industrial CyberSecurity for Linux Nodes.

Синтаксис команды

```
kics-control -F --query
```

Команды управления заблокированными устройствами

-H –префикс, указывающий, что команда принадлежит к группе команд управления устройствами, заблокированными Защитой от шифрования (см. раздел "Защита от удаленного вредоносного шифрования" на стр. [404](#)) и Защитой от сетевых угроз (см. раздел "Защита от сетевых угроз" на стр. [398](#)).

Команда kics-control --get-blocked-hosts

Команда позволяет вывести в консоль список заблокированных устройств.

Синтаксис команды

```
kics-control [-H] --get-blocked-hosts
```

Команда kics-control --allow-hosts

Команда позволяет разблокировать заблокированные устройства.

Синтаксис команды

```
kics-control [-H] --allow-hosts <адрес>
```

Аргументы и ключи

<адрес> – IP-адрес устройства или подсети (IPv4/IPv6, включая адреса в короткой форме). Вы можете указать несколько IP-адресов устройств или подсетей, разделяя их пробелами.

Команды управления Контролем устройств

-D – префикс, указывающий, что команда принадлежит к группе команд управления контролем устройств.

Команда kics-control --get-device-list

Команда позволяет вывести в консоль список устройств (см. раздел "Просмотр списка подключенных устройств в командной строке" на стр. [488](#)), которые установлены на клиентском устройстве или подключены к нему.

Синтаксис команды

```
kics-control [-D] --get-device-list [--json]
```

Аргументы и ключи

--json – выводить данные в формате JSON.

Команды управления Контролем приложений

-A – префикс, указывающий, что команда принадлежит к группе команд управления контролем приложений.

Команда kics-control --get-app-list

Команда позволяет вывести список приложений, обнаруженных на клиентском устройстве во время выполнения задачи Инвентаризация.

Синтаксис команды

```
kics-control [-A] --get-app-list [--json]
```

Аргументы и ключи

--json – выводить данные в формате JSON.

Команда kics-control --get-categories

Команда позволяет вывести список созданных категорий контроля приложений.

Синтаксис команды

```
kics-control [-A] --get-categories [--names <название категории 1> <название категории 2> ... <название категории N>] [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

<название категории 1> <название категории 2> ... <название категории N> – названия категорий, информацию о которых вы хотите просмотреть. Если вы хотите просмотреть информацию о нескольких категориях, укажите названия категорий через пробел.

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу формата JSON, в который будут выведены параметры.

--json – выводить данные в формате JSON.

Команда kics-control --set-categories

Команда позволяет создать или изменить список созданных категорий контроля приложений.

Синтаксис команды

```
kics-control [-A] --set-categories [--names <название категории 1> <название категории 2> ... <название категории N>] --file <путь к конфигурационному файлу>
```

Аргументы и ключи

<название категории 1> <название категории 2> ... <название категории N> – названия категорий, информацию о которых вы хотите изменить. Если вы хотите изменить информацию о нескольких категориях, укажите названия категорий через пробел. Если вы не укажите название категории, она будет удалена из списка.

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу с параметрами категорий.

Команда kics-control --get-settings 21

Команда позволяет вывести список созданных правил контроля приложений.

Синтаксис команды

```
kics-control --get-settings 21 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу, в который будут выведены параметры.

--json – выводить данные в формате JSON.

Команда kics-control --set-settings 21

Команда позволяет изменить список созданных категорий приложений и правил контроля приложений.

Синтаксис команды

```
kics-control --set-settings 21 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу, из которого будут импортированы параметры.

--json – импорт данных из файла в формате JSON.

Команда kics-control --set-to-default 21

Команда позволяет удалить список категорий приложений и правил контроля приложений.

Синтаксис команды

```
kics-control --set-settings 21 --set-to-default
```

Команды управления Веб-Контролем

Команда `kics-control --get-settings 26`

Команда позволяет вывести список настроенных параметров Веб-Контроля.

Синтаксис команды

```
kics-control --get-settings 26 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут выведены параметры.

`--json` – выводить данные в формате JSON.

Команда `kics-control --set-settings 26`

Команда позволяет изменить список настроенных параметров Веб-Контроля.

Синтаксис команды

```
kics-control --set-settings 26 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры.

`--json` – импорт данных из файла в формате JSON.

Команда `kics-control --set-to-default 26`

Команда позволяет удалить настроенные параметры и восстановить значения параметров Веб-Контроля до правила по умолчанию (см. раздел "Веб-Контроль" на стр. [489](#)).

Синтаксис команды

```
kics-control --set-settings 26 --set-to-default
```

Команды управления резервным хранилищем

`-B` – префикс, указывающий, что команда принадлежит к группе команд управления резервным хранилищем (см. раздел "Резервное хранилище" на стр. [586](#)).

Команда `kics-control --mass-remove`

Команда позволяет удалить из резервного хранилища все или только указанные объекты.

Синтаксис команды

Удалить все объекты:

```
kics-control [-B] --mass-remove
```

Удалить объекты, соответствующие условиям фильтра:


```
kics-control [-B] --mass-remove --query "<условия фильтра>"
```

Аргументы и ключи

<условия фильтра> – одно или несколько логических выражений (см. раздел "Использование фильтра для ограничения результатов запросов" на стр. [140](#)) в формате <поле> <операция сравнения> '<значение>', скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.

Команда `kics-control -B --query`

Команда позволяет вывести информацию об объектах резервного хранилища.

Синтаксис команды

Вывести информацию обо всех объектах резервного хранилища:

```
kics-control -B --query [-n <количество>] [--json] [--reverse]
```

Вывести информацию об объектах резервного хранилища, соответствующих условиям фильтра:

```
kics-control -B --query ["<условия фильтра>"] [-n <количество>] [--json] [--reverse]
```

Аргументы и ключи

<условия фильтра> – одно или несколько логических выражений (см. раздел "Использование фильтра для ограничения результатов запросов" на стр. [140](#)) в формате <поле> <операция сравнения> '<значение>', скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса. Если вы не укажете условия фильтра, приложение выведет информацию обо всех объектах резервного хранилища.

<количество> – количество последних объектов из хранилища, которые нужно вывести. Если вы не укажете ключ `-n`, будут выведены последние 30 объектов. Чтобы показать все объекты, укажите значение 0.

`--json` – выводить данные в формате JSON.

Команда `kics-control --restore`

Команда позволяет восстановить объект из резервного хранилища.

Синтаксис команды

```
kics-control [-B] --restore <идентификатор объекта> [--file <имя и путь к файлу>]
```

Аргументы и ключи

<идентификатор объекта> – идентификатор объекта в резервном хранилище.

`--file <имя и путь к файлу>` – новое имя файла и путь к директории, в которой его требуется сохранить. Если вы не укажете ключ `--file`, объект будет восстановлен с исходным именем в исходное местоположение.

Команды управления пользователями и ролями

-U – префикс, указывающий, что команда принадлежит к группе команд управления пользователями и ролями.

Команда `kics-control --get-user-list`

Команда позволяет вывести список пользователей и ролей.

Синтаксис команды

```
kics-control [-U] --get-user-list
```

Команда `kics-control --grant-role`

Команда позволяет присвоить роль определенному пользователю.

Синтаксис команды

```
kics-control [-U] --grant-role <роль> <пользователь>
```

Команда `kics-control --revoke-role`

Команда позволяет отозвать роль у определенного пользователя.

Синтаксис команды

```
kics-control [-U] --revoke-role <роль> <пользователь>
```

Команды управления параметрами интеграции с Kaspersky Industrial CyberSecurity for Networks

-K – префикс, указывающий, что команда принадлежит к группе команд управления параметрами интеграции с Kaspersky Industrial CyberSecurity for Networks (см. раздел "Интеграция с Kaspersky Industrial CyberSecurity for Networks" на стр. [592](#)).

Команда `kics-control --add-kics4networks-server-certificate`

Команда позволяет добавить или заменить ранее добавленный сертификат сервера интеграции Kaspersky Industrial CyberSecurity for Networks.

Синтаксис команды

```
kics-control [-K] --add-kics4networks-server-certificate <имя и путь к файлу>
```

Аргументы и ключи

<имя и путь к файлу> – имя и путь к файлу, содержащему сертификат сервера интеграции формата DER или PEM.

Команда `kics-control --remove-kics4networks-server-certificate`

Команда позволяет удалить сертификат сервера интеграции Kaspersky Industrial CyberSecurity for Networks.

Синтаксис команды

```
kics-control [-K] --remove-kics4networks-server-certificate
```

Команда `kics-control --query-kics4networks-server-certificate`

Команда позволяет вывести информацию о сертификате сервера интеграции Kaspersky Industrial CyberSecurity for Networks.

Синтаксис команды

```
kics-control [-K] --query-kics4networks-server-certificate
```

Команда `kics-control --add-kics4networks-client-certificate`

Команда позволяет добавить или заменить ранее добавленный сертификат клиента, используемый для защиты подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks.

Синтаксис команды

```
kics-control [-K] --add-kics4networks-client-certificate <имя и путь к файлу>
```

Аргументы и ключи

<имя и путь к файлу> – имя и путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

Команда `kics-control --remove-kics4networks-client-certificate`

Команда позволяет удалить сертификат клиента, используемый для защиты подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks.

Синтаксис команды

```
kics-control [-K] --remove-kics4networks-client-certificate
```

Команда `kics-control --query-kics4networks-client-certificate`

Команда позволяет вывести информацию о сертификате клиента.

Синтаксис команды

```
kics-control [-K] --query-kics4networks-client-certificate
```

Команды управления параметрами интеграции с Kaspersky Endpoint Detection and Response Optimum

-R – префикс, указывающий, что команда принадлежит к группе команд управления параметрами интеграции с Kaspersky Endpoint Detection and Response Optimum (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response Optimum" на стр. [610](#)).

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum выполняется с помощью параметра `UseEdrOptimum` в общих параметрах приложения.

Команда `kics-control --isolation-stat`

Команда позволяет вывести в консоль текущее состояние сетевой изоляции: включена или выключена.

Синтаксис команды

```
kics-control [-R] --isolation-stat
```

Команда kics-control --isolation-off

Команда позволяет временно выключить сетевую изоляцию устройства.

Синтаксис команды

```
kics-control [-R] --isolation-off
```

Приложение 3. Конфигурационные файлы и параметры приложения по умолчанию

Для управления работой приложения Kaspersky Industrial CyberSecurity for Linux Nodes используются следующие конфигурационные файлы:

- Конфигурационные файлы, которые содержат параметры первоначальной настройки приложения:
 - конфигурационный файл `autoinstall.ini` (см. раздел "Параметры конфигурационного файла `autoinstall.ini`" на стр. [42](#)), который используется при установке приложения с помощью Kaspersky Security Center;
 - конфигурационный файл, который используется при установке приложения с помощью командной строки.
- Предустановленные конфигурационные файлы (на стр. [702](#)), которые создаются автоматически во время первоначальной настройки приложения и содержат значения параметров, заданные при первоначальной настройке. Эти параметры применяются во время работы приложения.
- Конфигурационные файлы, которые вы можете создавать с помощью команд управления Kaspersky Industrial CyberSecurity for Linux Nodes (см. раздел "Приложение 2. Команды управления Kaspersky Industrial CyberSecurity for Linux Nodes" на стр. [676](#)). Эти конфигурационные файлы могут содержать параметры задач (см. раздел "Параметры задач командной строки по умолчанию" на стр. [711](#)) и другие параметры приложения. Вы можете изменять эти файлы (см. раздел "Правила редактирования конфигурационных файлов задач приложения" на стр. [701](#)) и импортировать их в приложение, чтобы изменять соответствующие параметры.

В этом разделе

Правила редактирования конфигурационных файлов задач приложения	701
Предустановленные конфигурационные файлы	702
Параметры задач командной строки по умолчанию	711
Общие параметры приложения	721
Общие параметры проверки контейнеров	728
Параметры проверки защищенных соединений	731
Параметры расписания задач	734

Правила редактирования конфигурационных файлов задач приложения

При редактировании конфигурационного файла соблюдайте следующие правила:

- В конфигурационном файле укажите все обязательные параметры. Отдельные параметры задачи можно указать без файла, с помощью командной строки.
- Если параметр принадлежит к какой-либо секции, укажите его только в этой секции. В пределах одной секции вы можете указывать параметры в любом порядке.
- Закрывайте имена секций в квадратные скобки [].
- Вводите значения параметров в формате `<имя параметра>=<значение параметра>` (пробелы между именем параметра и его значением не обрабатываются).

Пример:

```
[ScanScope.item_0000]
AreaDesc=Home
AreaMask.item_0000=*doc
Path=/home
```

Символы "пробел" и "табуляция" игнорируются перед первой кавычкой и после последней кавычки строкового значения, а также в начале и в конце строкового значения, не заключенного в кавычки.

- Если вам нужно указать несколько значений параметра, повторите параметр столько раз, сколько значений вы хотите указать.

Пример:

```
AreaMask.item_0000=*xml
AreaMask.item_0001=*doc
```

- Соблюдайте регистр при вводе значений параметров следующих типов:
 - имена (маски) проверяемых объектов и объектов исключения;
 - названия (маски) угроз.

При вводе остальных значений параметров соблюдать регистр не требуется.

- Указывайте значения параметров булевского типа следующим образом: Yes / No.
- Закрывайте в кавычки строковые значения, содержащие символ "пробел" (например, имена файлов и директорий, пути к ним; выражения, содержащие дату и время в формате "ГГГГ-ММ-ДД ЧЧ:ММ:СС").

Остальные значения вы можете вводить как в кавычках, так и без них.

Пример:

```
AreaDesc="Проверка почтовых баз"
```

Одиночная кавычка в начале или в конце строки считается ошибкой.

Предустановленные конфигурационные файлы

После первоначальной настройки в приложении создаются следующие конфигурационные файлы:

- `/var/opt/kaspersky/kics/common/agreements.ini`
Конфигурационный файл `agreements.ini` содержит параметры, связанные с Лицензионным соглашением, Политикой конфиденциальности и Положением о Kaspersky Security Network.
- `/var/opt/kaspersky/kics/common/kics.ini`
Конфигурационный файл `kics.ini` содержит параметры, приведенные в таблице ниже.

Если требуется, вы можете изменять значения параметров (см. раздел "Правила редактирования конфигурационных файлов задач приложения" на стр. [701](#)) в этих файлах.

Изменять значения по умолчанию в этих файлах рекомендуется под руководством специалистов Службы технической поддержки по полученным от них инструкциям.

Таблица 245. Параметры конфигурационного файла *kics.ini*

Параметр	Описание	Значения
Секция [General] содержит следующие параметры:		
Locale	Языковой стандарт, используемый для локализации текстов, передаваемых приложением Kaspersky Industrial CyberSecurity for Linux Nodes в Kaspersky Security Center (события, уведомления, результаты выполнения задач и другие). Локализация графического интерфейса и командной строки приложения зависит от локализации, указанной в переменной окружения LANG. Если в переменной окружения LANG указана локализация, которую не поддерживает приложение Kaspersky Industrial CyberSecurity for Linux Nodes, то графический интерфейс и командная строка отображаются в английской локализации.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр <code>Locale</code> не указан, устанавливается язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию <code>en_US.utf8</code> .
PackageType	Формат установленного пакета приложения (см. раздел "Установка приложения с помощью командной строки" на стр. 53). Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения.	<code>rpm</code> – установлен пакет формата RPM. <code>deb</code> – установлен пакет формата DEB.
UseFanotify	Использование технологии fanotify. Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения (см. раздел "Определение типа перехватчика файловых операций" на стр. 57).	<code>true/yes</code> – операционная система поддерживает технологию fanotify. <code>false/no</code> – операционная система не поддерживает технологию fanotify.
StartupTraces	Включение создания файлов трассировки (см. раздел "О файлах трассировки приложения" на стр. 663) при запуске приложения.	<code>true/yes</code> – создавать файлы трассировки при запуске приложения. <code>false/no</code> (значение по умолчанию) – не создавать файлы трассировки при запуске приложения.

Параметр	Описание	Значения
RevealSensitiveInfoInTraces	Отображение в файлах трассировки (см. раздел "О файлах трассировки приложения" на стр. 663) информации, которая может содержать персональные данные (например, пароли).	<code>true/yes</code> – отображать информацию, которая может содержать персональные данные, в файлах трассировки приложения. <code>false/no</code> (значение по умолчанию) – не отображать информацию, которая может содержать персональные данные, в файлах трассировки.
AsyncTraces	Включение асинхронной трассировки, при которой запись информации в файлы трассировки происходит в асинхронном режиме.	<code>true/yes</code> – включить асинхронную трассировку. <code>false/no</code> (значение по умолчанию) – не включать асинхронную трассировку.

Параметр	Описание	Значения
CoreDumps	Включение создания файла дампа (см. раздел "О файлах дампа" на стр. 667) при сбое в работе приложения.	<code>true/yes</code> – создавать файл дампа при сбое в работе приложения. <code>false/no</code> (значение по умолчанию) – не создавать файл дампа при сбое в работе приложения.
CoreDumpsPath	Путь к директории, в которой хранятся файлы дампа (см. раздел "О файлах дампа" на стр. 667).	Значение по умолчанию: <code>/var/opt/kaspersky/kics/common/dumps</code> . Для доступа к директории хранения файлов дампа, заданной по умолчанию, требуются root-права.
MinFreeDiskSpace	Минимальное количество памяти на диске, которое останется после записи файла дампа, в мегабайтах.	Значение по умолчанию: 300.
ScanMemoryLimit	Ограничение на использование памяти (см. раздел "Установка ограничения на использование памяти приложением" на стр. 675) приложением в мегабайтах.	Значение по умолчанию: 8192.
MachineId	Уникальный идентификатор устройства пользователя.	Значение параметра заполняется автоматически во время установки приложения.
SocketPath	Путь к сокету для удаленного подключения, по которому подключаются, например, графический интерфейс и утилита <code>kics-control</code> .	Значение по умолчанию: <code>/var/run/bl4control</code> .
MaxInotifyWatches	Ограничение количества подписок на изменения в файлах и директориях (<code>user watches</code>), указанное в файле <code>/proc/sys/fs/inotify/max_user_watches</code> .	Значение по умолчанию: 300000.
MaxInotifyInstances	Ограничение количества подписок на изменения в файлах и директориях на одного пользователя.	Значение по умолчанию: 2048.
ExecEnvMax	Количество переменных окружения, которые приложение будет захватывать из вызова команды.	Значение по умолчанию: 50.

Параметр	Описание	Значения
ExecArgMax	Количество аргументов, которые приложение будет захватывать из вызова <code>exec</code> .	Значение по умолчанию: 50.
DisableFileAvActions	Выключение функций лечения и удаления файлов для компонентов приложения после его установки. Если функции лечения и удаления файлов выключены, в случае обнаружения угрозы приложение не пытается лечить или удалять файлы, в которых обнаружена угроза, а только информирует пользователя об обнаружении угрозы.	<code>true/yes</code> – выключить функции лечения и удаления файлов при запуске приложения после установки. <code>false/no</code> (значение по умолчанию) – не выключать функции лечения и удаления файлов при запуске приложения после установки.
AdditionalDNSLookup	Использование публичного DNS. При сбоях доступа к серверам через системный DNS приложение будет использовать публичный DNS. Это нужно для обновления баз приложения и поддержки уровня безопасности устройства. Приложение будет использовать следующие публичные DNS в порядке их обхода: • Google™ Public DNS™ (8.8.8.8). • Cloudflare® DNS (1.1.1.1). • Alibaba Cloud® DNS (223.6.6.6). • Quad9® DNS (9.9.9.9). • CleanBrowsing (185.228.168.168).	<code>true/yes</code> – использовать публичный DNS для доступа к серверам "Лаборатории Касперского". <code>false/no</code> (значение по умолчанию) – не использовать публичный DNS для доступа к серверам "Лаборатории Касперского".
Секция [Network] содержит следующие параметры:		

Запросы приложения могут содержать адреса доменов и внешний IP-адрес пользователя, так как приложение устанавливает с DNS-сервером TCP/UDP-соединение. Эти данные нужны, например, для проверки сертификата веб-ресурса при обращении по HTTPS. Если приложение использует публичный DNS-сервер, правила обработки данных регламентируются Политикой конфиденциальности этого сервиса. Если требуется запретить приложению использовать публичный DNS-сервер, обратитесь в Службу технической поддержки за приватным патчем.

Параметр	Описание	Значения
WtpFwMark	Метка в правилах утилиты iptables для перенаправления трафика в приложение для обработки компонентом Защита от веб-угроз (на стр. 378). Вам может потребоваться изменить эту метку, если на одном устройстве с установленным приложением работает другое ПО, которое использует девятый бит маски TCP-пакета, и возникает конфликт.	Значение задается десятичным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 0x100.
NtpFwMark	Метка в правилах утилиты iptables для перенаправления трафика в приложение для обработки компонентом Защита от сетевых угроз (на стр. 398). Вам может потребоваться изменить эту метку, если на одном устройстве с установленным приложением работает другое ПО, которое использует девятый бит маски TCP-пакета, и возникает конфликт.	Значение задается десятичным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 0x200.
BypassFwMark	Метка, которой маркируются пакеты, созданные или проверенные приложением, чтобы они снова не попали в приложение на проверку.	Значение задается десятичным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 0x400.
BypassNFlogMark	Метка, которой маркируются пакеты, созданные или проверенные приложением, чтобы исключить запись о них в журнал утилиты iptable.	Значение задается десятичным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 0x800.
ProxyRouteTable	Номер таблицы маршрутизации.	Значение по умолчанию: 101.
Секция [Watchdog] содержит следующие параметры:		
TimeoutAfterHeads hot	Максимальное время ожидания завершения процесса kics от момента отправки сигнала HEADSHOT Watchdog-сервером процессу kics.	Значение по умолчанию: 2 мин.
StartupTimeout	Максимальный интервал времени от момента получения сообщения REGISTER до момента получения сообщения SUCCESSFUL_STARTUP.	Значение по умолчанию: 3 мин.

Параметр	Описание	Значения
TimeoutAfterKill	Максимальное время ожидания завершения управляемого процесса от момента отправки сигнала SIGKILL Watchdog-сервером процессу kics. Если по истечении этого времени процесс kics не завершился, выполняется действие, заданное параметром --failed-kill.	Значение по умолчанию: 2 дня.
PingInterval	Периодичность, с которой приложение пытается отправить серверу сообщение PONG в ответ на принятое сообщение PING.	Значение по умолчанию: 2000 мс.
MaxRestartCount	Максимальное количество неудачных последовательных попыток запуска приложения.	Значение по умолчанию: 5.
ActivityTimeout	Максимальный интервал времени, в течение которого приложение должно отправить сообщение Watchdog-серверу. Если в течение этого интервала времени от приложения не будет сообщения, Watchdog-сервер начнет процедуру завершения процесса kics.	Значение по умолчанию: 2 мин.
ConnectTimeout	Максимальный интервал времени от момента запуска процесса kics до момента установления приложением соединения с Watchdog-сервером. Если приложение не успевает создать соединение за этот интервал времени, Watchdog-сервер начнет процедуру завершения процесса kics.	Значение по умолчанию: 3 мин.
RegisterTimeout	Максимальный интервал времени от момента соединения приложения с Watchdog-сервером до получения сервером сообщения REGISTER.	Значение по умолчанию: 500 мс.
TimeoutAfterShutdown	Максимальное время ожидания завершения процесса kics от момента отправки сигнала SHUTDOWN Watchdog-сервером процессу kics.	Значение по умолчанию: 2 мин.

Параметр	Описание	Значения
MaxMemory	Ограничение на использование резидентной памяти процесса kics. Если резидентная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения процесса kics.	off – использование резидентной памяти не ограничено. <значение>% – значение от 0 до 100 в процентах от объема памяти. <значение>MB – значение в мегабайтах. lowest/<значение>%/<значение>MB – наименьшее значение между значением в процентах и значением в мегабайтах. highest/<значение>%/<значение>MB – наибольшее значение между значением в процентах и значением в мегабайтах. auto – до 50% доступной памяти, но не менее 2ГБ и не более 16ГБ. Значение по умолчанию: auto.
MaxVirtualMemory	Ограничение на использование виртуальной памяти процесса kics. Если виртуальная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения процесса kics.	off (значение по умолчанию) – использование виртуальной памяти не ограничено. <значение>MB – значение в мегабайтах.
MaxSwapMemory	Ограничение на размер swap-файла управляемого процесса kics. Если swap-файл управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения процесса kics.	off (значение по умолчанию) – размер swap-файла не ограничен. <значение>% – значение от 0 до 100 в процентах от объема памяти. <значение>MB – значение в мегабайтах. lowest/<значение>%/<значение>MB – наименьшее значение между значением в процентах и значением в мегабайтах. highest/<значение>%/<значение>MB – наибольшее значение между значением в процентах и значением в мегабайтах.
TrackProductCrashes	Включение мониторинга стабильности работы приложения. Если мониторинг стабильности работы приложения включен, Watchdog-сервер отслеживает количество нештатных остановок приложения.	true/yes – включить мониторинг стабильности работы приложения. false/no (значение по умолчанию) – выключить мониторинг стабильности работы приложения.

Параметр	Описание	Значения
ProductHealthLogFile	Путь к файлу, с помощью которого осуществляется мониторинг стабильности приложения.	Значение по умолчанию: /var/opt/kaspersky/kics/private/kics_health.log.
WarnThreshold	Интервал времени (в секундах), за который приложение должно посчитать количество нештатных остановок, прежде чем вывести уведомление о нестабильной работе.	Значение по умолчанию: 3600 секунд.
WarnAfter_#_crash	Количество нештатных остановок приложения, необходимых для отображения уведомления о нестабильной работе приложения.	Значение по умолчанию: 10. Если указано значение 0, уведомление о нестабильной работе приложения не отображается.
WarnRemovingThreshold	Интервал времени, по истечении которого статус о нестабильной работе приложения будет снят.	Значение по умолчанию: 86400 секунд.
Секция [Environment] содержит следующие параметры:		
ExperimentalContainerdSupport	Включение поддержки среды containerd при работе компонента Мониторинг контейнеров. Этот параметр по умолчанию отсутствует в конфигурационном файле. Если вы хотите использовать среду containerd при работе компонента Мониторинг контейнеров, вам нужно вручную добавить в конфигурационный файл секцию [Environment] и добавить в нее параметр ExperimentalContainerdSupport.	true/yes – включить поддержку среды containerd в работе компонента Мониторинг контейнеров. false/no – не включать поддержку среды containerd в работе компонента Мониторинг контейнеров.

Параметры задач командной строки по умолчанию

Этот раздел содержит параметры по умолчанию всех предустановленных задач (см. раздел "Управление задачами в командной строке" на стр. [119](#)), которые предусмотрены для управления приложением Kaspersky Industrial CyberSecurity for Linux Nodes с помощью командной строки.

Задачи *Rollback* и *License* не имеют параметров.

В этом разделе

Параметры по умолчанию задачи File_Threat_Protection (ID:1)	712
Параметры по умолчанию задачи Scan_My_Computer (ID:2).....	713
Параметры по умолчанию задачи Scan_File (ID:3).....	714
Параметры по умолчанию задачи Critical_Areas_Scan (ID:4).....	715
Параметры по умолчанию задачи Update (ID:6)	716
Параметры по умолчанию задачи Backup (ID:10).....	716
Параметры по умолчанию задачи System_Integrity_Monitoring (ID:11).....	716
Параметры по умолчанию задачи Firewall_Management (ID:12)	716
Параметры по умолчанию задачи Anti_Cryptor (ID:13).....	717
Параметры по умолчанию задачи Web_Threat_Protection (ID:14)	717
Параметры по умолчанию задачи Device_Control (ID:15)	717
Параметры по умолчанию задачи Removable_Drives_Scan (ID:16)	719
Параметры по умолчанию задачи Network_Threat_Protection (ID:17).....	719
Параметры по умолчанию задач Container_Scan (ID:18) и Custom_Container_Scan (ID:19)	719
Параметры по умолчанию задачи Behavior_Detection (ID:20)	720
Параметры по умолчанию задачи Application_Control (ID: 21)	720
Параметры по умолчанию задачи Inventory_Scan (ID:22).....	720
Параметры по умолчанию задачи KICS4Networks_Integration (ID:23)	720
Параметры по умолчанию задачи Web_Control (ID:26).....	721

Параметры по умолчанию задачи File_Threat_Protection (ID:1)

ScanArchived=No

ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

SkipPlainTextFiles=No

TimeLimit=60

SizeLimit=0

FirstAction=Skip

SecondAction=Block

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
ScanByAccessType=SmartCheck
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*

Параметры по умолчанию задачи Scan_My_Computer (ID:2)

ScanFiles=Yes
ScanBootSectors=Yes
ScanComputerMemory=Yes
ScanStartupObjects=Yes
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Skip
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes

HeuristicLevel=Recommended
UseIChecker=Yes
UseGlobalExclusions=Yes
UseOASExclusions=Yes
DeviceNameMasks.item_0000=/**
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*

Параметры по умолчанию задачи Scan_File (ID:3)

ScanFiles=Yes
ScanBootSectors=No
ScanComputerMemory=No
ScanStartupObjects=No
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Skip
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes

```
UseGlobalExclusions=Yes  
UseOASExclusions=Yes  
DeviceNameMasks.item_0000=/**  
[ScanScope.item_0000]  
AreaDesc=All objects  
UseScanArea=Yes  
Path=/  
AreaMask.item_0000=*
```

Параметры по умолчанию задачи Critical_Areas_Scan (ID:4)

```
ScanFiles=No  
ScanBootSectors=Yes  
ScanComputerMemory=Yes  
ScanStartupObjects=Yes  
ScanArchived=Yes  
ScanSfxArchived=Yes  
ScanMailBases=No  
ScanPlainMail=No  
TimeLimit=0  
SizeLimit=0  
FirstAction=Skip  
SecondAction=Skip  
UseExcludeMasks=No  
UseExcludeThreats=No  
ReportCleanObjects=No  
ReportPackedObjects=No  
ReportUnprocessedObjects=No  
UseAnalyzer=Yes  
HeuristicLevel=Recommended  
UseIChecker=Yes  
UseGlobalExclusions=Yes  
UseOASExclusions=Yes
```

```
DeviceNameMasks.item_0000=/**  
[ScanScope.item_0000]  
AreaDesc=All objects  
UseScanArea=Yes  
Path=/  
AreaMask.item_0000=*
```

Параметры по умолчанию задачи Update (ID:6)

```
SourceType=KLServers  
UseKLServersWhenUnavailable=Yes  
ApplicationUpdateMode=DownloadOnly  
ConnectionTimeout=10
```

Параметры по умолчанию задачи Backup (ID:10)

```
DaysToLive=90  
BackupSizeLimit=0  
BackupFolder=/var/opt/kaspersky/kics/common/objects-backup/
```

Параметры по умолчанию задачи System_Integrity_Monitoring (ID:11)

```
UseExcludeMasks=No  
[ScanScope.item_0000]  
AreaDesc=Kaspersky internal objects  
UseScanArea=Yes  
Path=/opt/kaspersky/kics/  
AreaMask.item_0000=*
```

Параметры по умолчанию задачи Firewall_Management (ID:12)

```
DefaultIncomingAction=Allow  
DefaultIncomingPacketAction=Allow  
OpenNagentPorts=Yes  
[NetworkZonesTrusted]  
[NetworkZonesLocal]  
[NetworkZonesPublic]
```

Параметры по умолчанию задачи Anti_Cryptor (ID:13)

ActionOnDetect=Notify
BlockTime=30
UseExcludeMasks=No
[ScanScope.item_0000]
AreaDesc=All shared directories
UseScanArea=Yes
Path=AllShared
AreaMask.item_0000=*

Параметры по умолчанию задачи Web_Threat_Protection (ID:14)

UseTrustedAddresses=Yes
ActionOnDetect=Notify
CheckMalicious=Yes
CheckPhishing=Yes
UseHeuristicForPhishing=Yes
CheckAdware=No
CheckOther=No

Параметры по умолчанию задачи Device_Control (ID:15)

OperationMode=Notify
[DeviceClass]
HardDrive=DependsOnBus
RemovableDrive=DependsOnBus
Printer=DependsOnBus
FloppyDrive=DependsOnBus
OpticalDrive=DependsOnBus
Modem=DependsOnBus
TapeDrive=DependsOnBus
MultifuncDevice=DependsOnBus
SmartCardReader=DependsOnBus
PortableDevice=DependsOnBus

```
WiFiAdapter=DependsOnBus
NetworkAdapter=DependsOnBus
BluetoothDevice=DependsOnBus
ImagingDevice=DependsOnBus
SerialPortDevice=DependsOnBus
ParallelPortDevice=DependsOnBus
InputDevice=DependsOnBus
SoundAdapter=DependsOnBus
[DeviceBus]
USB=Allow
FireWire=Allow
[Schedules.item_0000]
ScheduleName=Default
DaysHours=All
[HardDrivePrincipals.item_0000]
Principal=\Everyone
[HardDrivePrincipals.item_0000.AccessRules.item_0000]
UseRule=Yes
ScheduleName=Default
Access=Allow
[RemovableDrivePrincipals.item_0000]
Principal=\Everyone
[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]
UseRule=Yes
ScheduleName=Default
Access=Allow
[FloppyDrivePrincipals.item_0000]
Principal=\Everyone
[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]
UseRule=Yes
ScheduleName=Default
Access=Allow
[OpticalDrivePrincipals.item_0000]
Principal=\Everyone
```

[OpticalDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

Параметры по умолчанию задачи Removable_Drives_Scan (ID:16)

ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No

Параметры по умолчанию задачи Network_Threat_Protection (ID:17)

ActionOnDetect=Notify

BlockAttackingHosts=Yes

BlockDurationMinutes=60

UseExcludeIPs=No

Параметры по умолчанию задач Container_Scan (ID:18) и Custom_Container_Scan (ID:19)

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Skip

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

```
UseIChecker=Yes
ScanContainers=Yes
ContainerNameMask=*
ScanImages=Yes
ImageNameMask=*
DeepScan=No
ContainerScanAction=StopContainerIfFailed
ImageAction=Skip
UseGlobalExclusions=Yes
```

Вы можете использовать параметры этого конфигурационного файла также для задачи Выборочная проверка контейнеров.

Параметры по умолчанию задачи Behavior_Detection (ID:20)

```
UseTrustedPrograms=No
TaskMode=Notify
```

Параметры по умолчанию задачи Application_Control (ID: 21)

```
AppControlMode=DenyList
AppControlRulesAction=Notify
```

Параметры по умолчанию задачи Inventory_Scan (ID:22)

```
ScanScripts=Yes
ScanBinaries=Yes
ScanAllExecutable=Yes
CreateGoldenImage=No
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/usr/bin
AreaMask.item_0000=*
```

Параметры по умолчанию задачи KICS4Networks_Integration (ID:23)

```
UseClientPinnedCertificate=No
```



```

SynchronizationPeriod=5
ConnectionTimeout=10
RequestTimeout=10
EnableTelemetry=Yes
[Endpoints.item_0000]
Address=127.0.0.1
Port=8081
[EventTransferSettings]
MaximumDataTransferTime=30
MaximumNumberOfEventsInPackage=1024
UseRequestCountLimits=Yes
MaximumNumberOfEventsInHour=3000
EventLimitExceededPercentage=15
PingPeriod=450

```

Параметры по умолчанию задачи Web_Control (ID:26)

```

WebControlDefaultAction=Allow
ComplaintRecipient=

```

Общие параметры приложения

Общие параметры приложения определяют работу приложения в целом и работу отдельных функций.

Таблица 246. Общие параметры приложения

Параметр	Описание	Значения
SambaConfigPath	Директория, в которой хранится конфигурационный файл Samba. Конфигурационный файл Samba нужен для обеспечения работы значений AllShared или Shared:SMB для параметра Path.	По умолчанию указана стандартная директория конфигурационного файла Samba. Значение по умолчанию: /etc/samba/smb.conf. После изменения значения этого параметра требуется перезапустить приложение.

Параметр	Описание	Значения
NfsExportPath	Директория, в которой хранится конфигурационный файл NFS. Конфигурационный файл NFS нужен для обеспечения работы значений AllShared или Shared:NFS для параметра Path.	По умолчанию указана стандартная директория конфигурационного файла NFS. Значение по умолчанию: /etc/exports. После изменения значения этого параметра требуется перезапустить приложение.
TraceLevel	Включение трассировки приложения (см. раздел "О файлах трассировки приложения" на стр. 663) и уровень детализации файлов трассировки.	Detailed – создавать детализированный файл трассировки. MediumDetailed – создавать файл трассировки, содержащий информационные сообщения и сообщения об ошибках. NotDetailed – создавать файл трассировки, содержащий сообщения об ошибках. None (значение по умолчанию) – не создавать файл трассировки.
TraceFolder	Директория, в которой хранятся файлы трассировки приложения (см. раздел "О файлах трассировки приложения" на стр. 663).	Значение по умолчанию: /var/log/kaspersky/kics. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, под которой работает Kaspersky Industrial CyberSecurity for Linux Nodes. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права. После изменения значения этого параметра требуется перезапустить приложение.
TraceMaxFileCount	Максимальное количество файлов трассировки приложения.	1–10000 Значение по умолчанию: 10. После изменения значения этого параметра требуется перезапустить приложение.
TraceMaxFileSize	Максимальный размер файла трассировки приложения (в мегабайтах).	1–1000 Значение по умолчанию: 500. После изменения значения этого параметра требуется перезапустить приложение.

Параметр	Описание	Значения
BlockFilesGreaterMaxFileNamePath	Блокировка доступа к файлам, длина полного пути к которым превышает заданное значение параметра (в байтах). Если длина полного пути к проверяемому файлу превышает значение этого параметра, задачи проверки пропускают такой файл во время проверки. Этот параметр недоступен для операционных систем, в которых используется технология fanotify.	4096–33554432 Значение по умолчанию: 16384. После изменения значения этого параметра требуется перезапустить задачу Защита от файловых угроз.
DetectOtherObjects	Включение обнаружения легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.	Yes – включить обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным. No (значение по умолчанию) – выключить обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
NamespaceMonitoring	Включение проверки пространств имен и контейнеров (см. раздел "Мониторинг контейнеров" на стр. 322). Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен.	Yes (значение по умолчанию) – включить проверку пространств имен и контейнеров. No – выключить проверку пространств имен и контейнеров.
FileBlockDuringScan	Включение режима перехвата файловых операций (см. раздел "Выбор режима перехвата файловых операций" на стр. 574) с блокированием доступа к файлам на время проверки. Режим перехвата файловых операций влияет на работу компонентов Защита от файловых угроз (на стр. 172) и Контроль устройств (на стр. 464).	Yes – блокировать доступ к файлам на время проверки. No (значение по умолчанию) – не блокировать доступ к файлам на время проверки. Обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.

Параметр	Описание	Значения
UseKSN	Включение использования Kaspersky Security Network. В сертифицированной версии приложения используется только KPSN. Использование KSN не допускается, так как приводит к выходу приложения из сертифицированного состояния.	Basic – включить использование Kaspersky Security Network в стандартном режиме. Extended – включить использование Kaspersky Security Network в расширенном режиме. No (значение по умолчанию) – выключить использование Kaspersky Security Network.
CloudMode	Включение облачного режима работы приложения. Облачный режим доступен, если включено использование KSN. Включение облачного режима приводит к выходу приложения из сертифицированного состояния.	Yes – включить режим работы, при котором приложение Kaspersky Industrial CyberSecurity for Linux Nodes использует облегченную версию баз вредоносного ПО. No (значение по умолчанию) – использовать полную версию баз вредоносного ПО. Облачный режим выключается автоматически, если выключено использование KSN.
UseMDR	Включение компонента Managed Detection and Response для интеграции с Kaspersky Managed Detection and Response. В сертифицированной версии приложения интеграция с Kaspersky Managed Detection and Response не поддерживается. Включение компонента Managed Detection and Response приводит к выходу приложения из сертифицированного состояния.	Yes – включить компонент Managed Detection and Response. No (значение по умолчанию) – выключить компонент Managed Detection and Response.

Параметр	Описание	Значения
UseProxy	Включение использования прокси-сервера (см. раздел "Настройка прокси-сервера" на стр. 560) компонентами приложения Kaspersky Industrial CyberSecurity for Linux Nodes. Прокси-сервер может использоваться для взаимодействия с Kaspersky Security Network, с Kaspersky Industrial CyberSecurity for Networks, для активации приложения и при обновлении баз и модулей приложения.	Yes – включить использование прокси-сервера. No (значение по умолчанию) – выключить использование прокси-сервера. Если выбрано значение Yes, интеграция с Kaspersky Industrial CyberSecurity for Networks будет выполняться через прокси-сервер.
ProxyServer	Параметры прокси-сервера в формате [<пользователь>[:<пароль>]@<адрес прокси-сервера>[:<порт>]. Для подключения через HTTP прокси рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP прокси использует незащищенное соединение, и учетная запись может быть скомпрометирована.	—
MaxEventsNumber	Максимальное количество событий, которые будет хранить приложение. При превышении заданного количества событий приложение удаляет наиболее давние события.	Значение по умолчанию: 500000. Если задано значение 0, то события не сохраняются.

Параметр	Описание	Значения
LimitNumberOfScanFileTasks	Максимальное количество задач выборочной проверки (см. раздел "Выборочная проверка файлов и директорий" на стр. 265), которые непривилегированный пользователь может одновременно запустить на устройстве. Этот параметр не ограничивает количество задач, которые может запустить пользователь с root-правами.	0–4294967295 Значение по умолчанию: 0. Если задано значение 0, непривилегированный пользователь не может запускать задачи выборочной проверки (см. раздел "Выборочная проверка файлов и директорий" на стр. 265). Если во время установки приложения вы установили пакет графического интерфейса, для параметра LimitNumberOfScanFileTasks по умолчанию используется значение 5.
UseSyslog	Включение записи информации о событиях в syslog. Для доступа к syslog требуются root-права.	Yes – включить запись информации о событиях в syslog. No (значение по умолчанию) – выключить запись информации о событиях в syslog.
SyslogFormatType	Формат записи событий в syslog в случае, если установлено значение параметра UseSyslog=yes.	cef – записывать в syslog события в формате CEF. При выборе этого формата записываются только события об обнаружениях. json (значение по умолчанию) – записывать в syslog события в формате JSON. При выборе этого формата записываются все события.
EventsStoragePath	Директория базы данных, в которой приложение сохраняет информацию о событиях. Для доступа к заданной по умолчанию базе данных событий требуются root-права.	Значение по умолчанию: /var/opt/kaspersky/kics/private/storage/events.db.

Параметр	Описание	Значения
ExcludedMountPoint.item_#	Точка монтирования, которую требуется исключить (см. раздел "Настройка глобальных исключений" на стр. 566) из области проверки. Исключение применяется в работе компонентов Защита от файловых угроз (на стр. 172) и Защита от шифрования (см. раздел "Защита от удаленного вредоносного шифрования" на стр. 404), Мониторинг контейнеров (на стр. 322) и задачи Проверка съемных дисков (на стр. 314), а также настраивается в работе задач проверки (типов ODS и ContainerScan). Вы можете указать несколько точек монтирования, которые требуется исключить из проверки. Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды mount. Параметр ExcludedMountPoint.item_# по умолчанию не указан.	AllRemoteMounted – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протоколов SMB и NFS. Mounted:NFS – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протокола NFS. Mounted:SMB – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протокола SMB. Mounted:<тип файловой системы> – исключать из перехвата файловых операций все смонтированные директории с указанным типом файловой системы. /mnt – исключать из перехвата объекты, находящиеся в точке монтирования /mnt (включая вложенные директории), используемой в качестве временной точки монтирования съемных дисков. <путь, содержащий маску /mnt/user* или /mnt/**/user_share> – исключать из перехвата объекты, находящиеся в точках монтирования, имена которых содержат указанную маску.
MemScanExcludedProgramPath.item_#	Исключение памяти процесса из проверки. Приложение не будет проверять память указанного процесса.	<полный путь к процессу> – исключать из проверки процесс в указанной локальной директории. Для указания пути вы можете использовать маски.
UseOnDemandCPULimit	Включение ограничения на использование ресурсов процессора для задач типа (см. раздел "Управление задачами в командной строке" на стр. 119) ODS, ContainerScan и InventoryScan.	Yes – включить ограничение потребления ресурсов процессора для задач типа ODS, ContainerScan и InventoryScan. No (значение по умолчанию) – выключить ограничение потребления ресурсов процессора для задач.

Параметр	Описание	Значения
OnDemandCPULimit	Максимальное значение нагрузки на все ядра процессора (в процентах) при работе задач типа (см. раздел "Управление задачами в командной строке" на стр. 119) <i>ODS</i> , <i>ContainerScan</i> и <i>InventoryScan</i> .	10–100 Значение по умолчанию: 100.
UseEdrOptimum	Включение компонента EDR Optimum для интеграции с Kaspersky Endpoint Detection and Response Optimum (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response Optimum" на стр. 610).	Yes – включить компонент EDR Optimum. No (значение по умолчанию) – выключить компонент EDR Optimum.

Общие параметры проверки контейнеров

Общие параметры проверки контейнеров используются при проверке пространств имен и контейнеров в реальном времени (см. раздел "Мониторинг контейнеров" на стр. [322](#)).

Таблица 247. Общие параметры проверки контейнеров и пространств имен

Параметр	Описание	Значения
OnAccessContainerScanAction	Действие над контейнером при обнаружении зараженного объекта. При проверке объектов внутри контейнера используются параметры задачи Защита от файловых угроз (см. раздел "Параметры задачи Защита от файловых угроз" на стр. 210). Действие над контейнером при обнаружении зараженного объекта также зависит от заданных параметров задачи Защита от файловых угроз (см. таблицу ниже).	StopContainerIfFailed – остановить контейнер, если не удалось вылечить или удалить зараженный объект. StopContainer – остановить контейнер при обнаружении зараженного объекта. Skip (значение по умолчанию) – не выполнять никаких действий над контейнерами при обнаружении зараженного объекта.
UseDocker	Использование среды Docker.	Yes (значение по умолчанию) – использовать среду Docker. No – не использовать среду Docker.
DockerSocket	Путь или URI (универсальный идентификатор ресурса) Docker-сокета.	Значение по умолчанию: /var/run/docker.sock.
UseCrio	Использование среды CRI-O.	Yes (значение по умолчанию) – использовать среду CRI-O. No – не использовать среду CRI-O.
CrioConfigFilePath	Путь к конфигурационному файлу CRI-O.	Значение по умолчанию: /etc/crio/crio.conf.
UsePodman	Использование утилиты Podman.	Yes (значение по умолчанию) – использовать утилиту Podman. No – не использовать утилиту Podman.
PodmanBinaryPath	Путь к исполняемому файлу утилиты Podman.	Значение по умолчанию: /usr/bin/podman.
PodmanRootFolder	Путь к корневой директории хранилища контейнеров.	Значение по умолчанию: /var/lib/containers/storage.
UseRunc	Использование утилиты runc.	Yes (значение по умолчанию) – использовать утилиту runc. No – не использовать утилиту runc.
RuncBinaryPath	Путь к исполняемому файлу утилиты runc.	Значение по умолчанию: /usr/bin/runc.
RuncRootFolder	Путь к корневой директории хранилища состояний контейнеров.	Значение по умолчанию: /run/runc.

Действие над контейнером при обнаружении зараженного объекта может меняться в зависимости от заданных значений параметров `FirstAction` и `SecondAction` задачи Защита от файловых угроз (см. раздел "Параметры задачи Защита от файловых угроз" на стр. [210](#)).

Таблица 248. Зависимость действия над контейнером от заданного действия при обнаружении угрозы

Значение параметра <code>FirstAction</code> / <code>SecondAction</code>	Действие, выполняемое над контейнером при выбранном действии <code>StopContainerIfFailed</code>
<code>Disinfect</code>	Остановить контейнер, если не удалось вылечить зараженный объект.
<code>Remove</code>	Остановить контейнер, если не удалось удалить зараженный объект.

Параметры проверки защищенных соединений

Таблица 249. Параметры проверки защищенных соединений

Параметр	Описание	Значения
EncryptedConnectionsScan	Включает или выключает проверку зашифрованного трафика. Для FTP-протокола проверка защищенных соединений по умолчанию выключена.	Yes (значение по умолчанию) – включить проверку защищенных соединений. No – выключить проверку защищенных соединений. Приложение не расшифровывает зашифрованный трафик.
EncryptedConnectionsScanErrorAction	Действие, выполняемое приложением при возникновении ошибки проверки защищенных соединений на веб-сайте.	AddToAutoExclusions (значение по умолчанию) – добавить домен, на котором возникла ошибка, в список доменов с ошибками проверки. Приложение не будет контролировать зашифрованный сетевой трафик при посещении этого домена. Disconnect – заблокировать сетевое соединение.
CertificateVerificationPolicy	Задаёт способ проверки сертификатов приложением Kaspersky Industrial CyberSecurity for Linux Nodes. Если сертификат является самоподписанным, приложение не выполняет дополнительную проверку.	FullCheck (значение по умолчанию) – приложение использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата. LocalCheck – приложение не использует интернет для проверки сертификата.
UntrustedCertificateAction	Действие, выполняемое приложением при обнаружении неподтвержденного сертификата.	Allow (значение по умолчанию) – разрешить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом. Block – запретить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом.
ManageExclusions	Использование исключений при проверке зашифрованного трафика.	Yes – не проверять веб-сайты, указанные в секции [Exclusions.item_#] (см. ниже). No (значение по умолчанию) – проверять все веб-сайты.

Параметр	Описание	Значения
MonitorNetworkPorts	Способ контроля сетевых портов приложением Kaspersky Industrial CyberSecurity for Linux Nodes.	Selected (значение по умолчанию) – контролировать только сетевые порты, указанные в секции [NetworkPorts.item_#] (см. ниже). All – контролировать все сетевые порты. Выбор этого значения может значительно увеличить нагрузку на операционную систему.
Секция [Exclusions.item_#] содержит домены, исключенные из проверки. Приложение не проверяет защищенные соединения, установленные при посещении указанных доменов.		
DomainName	Имя домена. Для указания домена можно использовать маски.	Значение по умолчанию не задано.
Секция [NetworkPorts.item_#] содержит сетевые порты, контролируемые приложением.		
PortName	Описание сетевого порта.	Значение по умолчанию не задано.
Port	Номера сетевых портов, контролируемые приложением.	1 – 65535 Значение по умолчанию не задано.

Параметры расписания задач

Таблица 250. Параметры расписания запуска задачи

Параметр	Описание	Значения
RuleType	Расписание запуска задачи.	Once – запускать задачу один раз. Monthly – запускать задачу каждый месяц в указанный день и в указанное время. Weekly – запускать задачу каждую неделю в указанный день и в указанное время. Daily – запускать задачу регулярно, с заданным интервалом в днях. Hourly – запускать задачу регулярно, с заданным интервалом в часах, начиная с указанных даты и времени. Minutely – запускать задачу регулярно, с заданным интервалом в минутах, начиная с указанного времени. Manual – запускать задачу вручную. PS – запускать задачу после запуска приложения. BR – запускать задачу после обновления баз приложения.
StartTime	Дата и время запуска задачи. Параметр StartTime является обязательным, если параметр RuleType принимает одно из следующих значений Once, Monthly, Weekly, Daily, Hourly, Minutely.	[<год>/<месяц>/<день месяца>] [чч]:[мм]:[сс]; [<день месяца> <день недели>]; [<периодичность запуска>]
RandomInterval	Интервал времени от 0 до указанного значения (в минутах), который будет добавлен ко времени запуска задачи, чтобы избежать одновременного запуска задач.	
RunMissedStartRules	Включение запуска пропущенной задачи после запуска приложения.	Yes – включать запуск пропущенной задачи после запуска приложения. No – не включать запуск пропущенной задачи после запуска приложения.

Приложение 4. Коды возврата командной строки

В приложении Kaspersky Industrial CyberSecurity for Linux Nodes предусмотрены следующие коды возврата командной строки:

- 0 – команда / задача выполнена успешно;
- 1 – общая ошибка в аргументах команды;
- 2 – ошибка в переданных параметрах приложения;
- 64 – приложение Kaspersky Industrial CyberSecurity for Linux Nodes не запущено;
- 66 – базы приложения не загружены (используется только командой `kics-control --app-info`);
- 67 – активация 2.0 завершилась с ошибкой из-за сетевых проблем;
- 68 – выполнение команды невозможно, так как приложение работает под политикой;
- 69 – приложение находится в инфраструктуре Amazon Paid Ami;
- 70 – попытка запуска уже запущенной задачи, удаления запущенной задачи, изменения параметров запущенной задачи, остановки остановленной задачи, приостановки приостановленной задачи или возобновления выполняющейся задачи;
- 71 – не приняты условия Положения о Kaspersky Security Network;
- 72 – при выполнении задачи Выборочная проверка или Выборочная проверка контейнеров обнаружены угрозы;
- 73 – попытка задать параметры задачи Контроль приложений, влияющие на работу приложения, без их подтверждения с помощью флага `--accept`.
- 74 – требуется перезапуск приложения Kaspersky Industrial CyberSecurity for Linux Nodes после обновления;
- 75 – требуется перезагрузка устройства;
- 76 – соединение запрещено, так как только пользователи с правами root должны иметь права на запись по указанному пути;
- 77 – указанный лицензионный ключ уже используется на устройстве;
- 128 – неизвестная ошибка;
- 65 – все остальные ошибки.

Приложение 5. Настройка совместной работы с SIEM-системами

► Чтобы настроить совместную работу приложения Kaspersky Industrial CyberSecurity for Linux Nodes с SIEM-системами:

1. Для запуска интеграции с SIEM-системами, запустите скрипт `tune_syslog_for_siem.sh`, указав параметры интеграции с SIEM-сервером: протокол, адрес SIEM-сервера и порт SIEM-сервера.

```
./tune_syslog_for_siem.sh <протокол> <адрес SIEM-сервера> <порт SIEM-сервера>
```

где:

- `<протокол>` – протокол TCP или UDP;
- `<адрес SIEM-сервера>` – IP-адрес или FQDN вашего SIEM-сервера;
- `<порт SIEM-сервера>` – TCP-порт или UDP-порт, на котором ваш SIEM-сервер ожидает подключений.

Если вы не укажете нужные параметры, отобразится сообщение о необходимости их указать.

2. Для выключения интеграции, запустите скрипт `turnoff_syslog_for_siem.sh`.

Также вы можете распространить скрипты через Kaspersky Security Center с помощью мастера создания инсталляционного пакета и задачи удаленной установки. Подробнее см. в справке Kaspersky Security Center.

Приложение 6. Значения параметров приложения в сертифицированной конфигурации

Этот раздел содержит перечень параметров приложения, влияющих на безопасное состояние приложения, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение значений (диапазонов значений) перечисленных параметров с их значений в сертифицированной конфигурации на другие значения выводит приложение из безопасного состояния.

Таблица 251. Параметры и их безопасные значения для приложения в сертифицированной

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
FirstAction	задача Защита от файловых угроз, задача Поиск вредоносного ПО, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Одно из следующих значений: • Disinfect (лечить) – приложение пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано Disinfect, рекомендуется задать второе действие в параметре SecondAction. • Remove (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. • Recommended (выполнять рекомендуемое действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе.
SecondAction	задача Защита от файловых угроз, задача Поиск вредоносного ПО, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Одно из следующих значений: • Disinfect (лечить) – приложение пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. • Remove (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. • Recommended (выполнять рекомендуемое действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Если для FirstAction выбрано Remove, то SecondAction указывать не нужно.
UseExcludeMasks	задача Защита от файловых угроз, задача Поиск вредоносного ПО, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров, задача Защита от шифрования	No – не исключать из области защиты объекты, указанные параметром ExcludeMasks. Исключение из области защиты объектов (значение Yes) допускается только для подтвержденных ложноположительных срабатываний для исключения влияния приложения на технологические процессы.

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
UseAnalyzer	задача Защита от файловых угроз, задача Поиск вредоносного ПО, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Yes – включить эвристический анализатор.
HeuristicLevel	задача Защита от файловых угроз, задача Поиск вредоносного ПО, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Одно из следующих значений: • Light – наименее тщательная проверка, минимальная загрузка системы. • Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. • Deep – наиболее тщательная проверка, максимальная загрузка системы. • Recommended – рекомендуемое значение.
ScanArchived	задача Защита от файловых угроз, задача Поиск вредоносного ПО, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Yes – проверять архивы.
ScanSfxArchived	задача Защита от файловых угроз, задача Поиск вредоносного ПО, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Yes – проверять самораспаковывающиеся архивы.
ScanMailBases	задача Защита от файловых угроз, задача Поиск вредоносного ПО, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Yes – проверять файлы почтовых баз.

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
ScanByAccessType	задача Защита от файловых угроз	Одно из следующих значений: • <code>SmartCheck</code> (значение по умолчанию) – проверять файл при попытке открытия, и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс во время своей работы многократно обращается к файлу в течение некоторого времени и изменяет его, повторно проверять файл только при последней попытке закрытия файла этим процессом. • <code>OpenAndModify</code> – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. • <code>Open</code> – проверять файл при попытке его открытия как на чтение, так и на выполнение или изменение.
SourceType	задача Обновление	Одно из следующих значений: • <code>KLServers</code> – приложение получает обновления с одного из серверов обновлений "Лаборатории Касперского". Обновления загружаются по протоколу HTTPS. • <code>SCServer</code> – приложение загружает обновления на защищаемое устройство с установленного в локальной сети Сервера администрирования. • <code>Custom</code> – приложение загружает обновления из пользовательского источника, указанного в секции <code>[CustomSources.item_#]</code>. Вы можете указать директории FTP-, HTTP- и HTTPS-серверов или директории на любом смонтированном устройстве защищаемого клиентского устройства, включая директории на удаленных устройствах, смонтированные по протоколам Samba или NFS.
ApplicationUpdateMode	задача Обновление	<code>Disabled</code> – не загружать и не устанавливать обновления приложения. Включение автоматической загрузки и установки обновлений приложения приводит к выходу приложения из сертифицированного состояния.

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
UseHostBlocker	задача Защита от шифрования	Yes – включить блокировку недоверенных компьютеров.
ActionOnDetect	задача Защита от веб-угроз	Block – запретить доступ к обнаруженному объекту, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.
OperationMode	задача Контроль устройств	Block – приложение применяет режим доступа, заданный для устройства или шины.
AppControlRules Action	задача Контроль приложений	Block – Kaspersky Industrial CyberSecurity for Linux Nodes блокирует запуск приложения, удовлетворяющего правилам.
ScanRemovable Drives	задача Проверка съемных дисков	Одно из следующих значений: - DetailedScan – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). - QuickScan – проверять только файлы определенных типов на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков).
UseKSN	общие параметры приложения	Одно из следующих значений: Basic – включить использование Kaspersky Security Network в стандартном режиме. Extended – включить использование Kaspersky Security Network в расширенном режиме. No (значение по умолчанию) – выключить использование Kaspersky Security Network. Значения Basic и Extended возможны только в случае использования KPSN. Использование KSN не допускается, так как приводит к выходу приложения из сертифицированного состояния.
CloudMode	общие параметры приложения	No – использовать полную версию баз вредоносного ПО. Включение облачного режима приводит к выходу приложения из сертифицированного состояния.

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
UseMDR	общие параметры приложения	№ – выключить Managed Detection and Response. Включение Managed Detection and Response приводит к выходу приложения из сертифицированного состояния.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 252. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь
базы приложения	базы данных признаков компьютерных вирусов (БД ПКВ)
виртуальная инфраструктура	среда функционирования
вирус; программа, представляющая угрозу; вредоносная программа	КВ, компьютерный вирус
приложение	продукт, объект оценки, программное изделие
события	данные аудита

Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Amazon является товарным знаком Amazon.com, Inc. или аффилированных лиц компании.

FireWire – товарный знак Apple Inc.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Ubuntu и LTS являются зарегистрированными товарными знаками Canonical Ltd.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Google, Google Public DNS, Chrome – товарные знаки Google LLC.

EulerOS является товарным знаком Huawei Technologies Co., Ltd.

Core – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Outlook, Visual C++ и Windows являются товарными знаками группы компаний Microsoft.

OVAL и логотип OVAL – зарегистрированные товарные знаки MITRE Corporation.

Oracle, JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Red Hat, Red Hat Enterprise Linux, CentOS – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.