kaspersky

Kaspersky Endpoint Security для Linux (исполнение ARM)

Подготовительные процедуры и руководство по эксплуатации

Версия приложения: 12.0.0.6672

kaspersky

Уважаемый пользователь!

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

Дата редакции документа: 30.11.2023

Обозначение документа: 643.46856491.00122-02 90 01

https://www.kaspersky.ru

https://help.kaspersky.com/ru

https://support.kaspersky.ru

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

kaspersky

Содержание

kaspersky

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Endpoint Security для Linux" (исполнение ARM) (далее также "Kaspersky Endpoint Security", "приложение").

Подготовительные процедуры изложены в разделах "Подготовка к установке приложения (см. стр. 26)", "Установка приложения (на стр. 29)" и "Процедура приемки (см. стр. 74)" и содержат процедуры безопасной установки и первоначальной настройки приложения, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки приложения.

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

В документе также содержатся разделы с дополнительной информацией о приложении.

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

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.

kaspersky

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 Kaspersky Endpoint Security:

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

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

На странице приложения (https://www.kaspersky.com/small-to-medium-business-security/endpoint-linux) вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

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

Страница Kaspersky Endpoint Security в Базе знаний

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

На странице приложения в Базе знаний (https://support.kaspersky.ru/kes-for-linux/12?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 Kaspersky Endpoint Security, 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, а также об окнах графического пользовательского интерфейса и окнах плагинов управления Kaspersky Endpoint Security: 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.

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

kaspersky

О приложении

Программное изделие «Kaspersky Endpoint Security для Linux» (исполнение ARM) (далее также "Kaspersky Endpoint Security", "приложение") представляет собой средство антивирусной защиты типов "Б", "В", "Г" и средство контроля подключения съемных машинных носителей информации второго класса защиты, предназначенное для применения на серверах и автоматизированных рабочих местах информационных систем, а также на автономных автоматизированных рабочих местах на аппаратных платформах arm64 и aarch64 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 Endpoint Security, являются:

- угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и / или съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ);
- угрозы, связанные с установкой на узлы информационной системы внутренними и внешними нарушителями незарегистрированного (неучтенного) потенциально вредоносного программного обеспечения;
- 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;
- управление работой ОО;
- управление параметрами ОО;
- управление установкой обновлений (актуализации) БД ПКВ ОО;
- аудит безопасности ОО;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация ОО;
- контроль целостности ОО;
- контроль подключения съемных машинных носителей информации.

В сертифицированной версии приложения не допускается использование следующих функций:

- интеграция с решением Kaspersky Managed Detection and Response;
- механизм автоматической загрузки обновлений приложения;
- работа в режиме KESL-контейнера.

kaspersky

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

1. Установка, конфигурирование и управление приложением должны осуществляться в соответствии с эксплуатационной документацией.
2. Приложение должно эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделах "Аппаратные требования (на стр. 20)" и "Программные требования (на стр. 20)".
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 контролируемыми 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 Endpoint Security имеет следующие аппаратные требования:

Минимальные аппаратные требования для архитектуры Arm:

- процессор Armv8.2-A Kunpeng 920 или Armv8-A Baikal-M (BE-M1000) или платформа m-TrusT Терминал;
- раздел подкачки не менее 1 ГБ;
- 2 ГБ оперативной памяти;
- 3 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов;
- если используется графический пользовательский интерфейс, разрешение монитора не менее 1930x1010.

Использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред не поддерживается на операционных системах для архитектуры Arm.

Программные требования

Для установки Kaspersky Endpoint Security на устройстве должна быть установлена одна из следующих операционных систем:

- 64-битные операционные системы для архитектуры Arm:
  - Операционная система специального назначения «Astra Linux Special Edition»[1,2] РУСБ.10152-02 (очередное обновление 4.7).
  - CentOS Stream 9.
  - EulerOS 2.0 SP8.
  - SUSE Linux Enterprise Server 15 SP4.

[1] Включая режим замкнутой программной среды и мандатный режим

[2] В режиме «Мобильный» не поддерживается работа локального графического интерфейса

- Ubuntu 22.04 LTS.
- Альт СП Рабочая станция релиз 10;
- Альт СП Сервер релиз 10;
- Альт Рабочая станция 10;
- Альт Сервер 10;
- РЕД ОС 7.3.

На устройствах с операционными системами для архитектуры Arm не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

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 Security Center

Приложение Kaspersky Endpoint Security совместимо с приложением Kaspersky Security Center следующих версий:

- Kaspersky Security Center 13.2. Поддерживается управление приложением Kaspersky Endpoint Security через Консоль администрирования с помощью mmc-плагина управления (см. раздел "Об mmc-плагине управления Kaspersky Endpoint Security" на стр. 48).
- Kaspersky Security Center 14. Поддерживается управление приложением Kaspersky Endpoint Security через Консоль администрирования с помощью mmc-плагина управления (см. раздел "Об mmc-плагине управления Kaspersky Endpoint Security" на стр. 48) и через Kaspersky Security Center Web Console с помощью веб-плагина управления (см. раздел "О веб-плагине управления Kaspersky Endpoint Security" на стр. 49).
- Kaspersky Security Center 14 Linux. Поддерживается управление приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console с помощью веб-плагина управления (см. раздел "О веб-плагине управления Kaspersky Endpoint Security" на стр. 49).

  Kaspersky Security Center на базе Linux имеет в составе версию Сервера администрирования, предназначенную для установки на устройство с операционной системой Linux. Взаимодействие с Сервером администрирования Kaspersky Security Center Linux осуществляется с помощью Kaspersky Security Center Web Console. Подробнее о Kaspersky Security Center Linux см. в документации Kaspersky Security Center Linux.

  В Kaspersky Security Center 14 Linux недоступны некоторые функциональные возможности Kaspersky Security Center 14, например, функции, связанные с использованием Kaspersky Security Network. Вы можете управлять использованием Kaspersky Security Network с помощью Kaspersky Security Center на базе Windows.

- Kaspersky Security Center 14.2. Поддерживается управление приложением Kaspersky Endpoint Security через Консоль администрирования с помощью mmc-плагина управления (см. раздел "Об mmc-плагине управления Kaspersky Endpoint Security" на стр. 48) и через Kaspersky Security Center Web Console с помощью веб-плагина управления (см. раздел "О веб-плагине управления Kaspersky Endpoint Security" на стр. 49).
- Kaspersky Security Center 14.2 Linux. Поддерживается управление приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console с помощью веб-плагина управления (см. раздел "О веб-плагине управления Kaspersky Endpoint Security" на стр. 49).
- Kaspersky Security Center 15 Linux. Поддерживается управление приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console с помощью веб-плагина управления (см. раздел "О веб-плагине управления Kaspersky Endpoint Security" на стр. 49).

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23) для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент), для управления приложением рекомендуется использовать Kaspersky Security Center следующих версий:

- Kaspersky Security Center 14.2.
- Kaspersky Security Center 15 Linux.

Для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center требуется Агент администрирования Kaspersky Security Center.

Агент администрирования Kaspersky Security Center не входит в приложение Kaspersky Endpoint Security и поставляется отдельно в составе приложения Kaspersky Security Center.

kaspersky

О режимах использования приложения Kaspersky Endpoint Security

Вы можете использовать Kaspersky Endpoint Security в одном из следующих режимов:

- В автономном режиме. Kaspersky Endpoint Security используется как автономное приложение для защиты устройств под управлением операционных систем Linux.
- В режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/index.htm). Kaspersky Endpoint Security используется как компонент Легкий агент решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.

  Режим Легкого агента для защиты виртуальных сред доступен только в составе решения Kaspersky Security для виртуальных сред Легкий агент. Для использования этого режима требуется отдельная лицензия.

По умолчанию приложение используется в автономном режиме.

Если вы хотите использовать приложение в режиме Легкого агента, вам нужно выполнить следующие действия:

1. Установить (см. раздел "Установка приложения" на стр. 29) Kaspersky Endpoint Security на каждой виртуальной машине, которую требуется защищать с помощью решения Kaspersky Security для виртуальных сред Легкий агент. Вы также можете установить приложение на шаблоне виртуальных машин.

   В ходе установки вам нужно указать одним из следующих способов, что приложение будет использоваться в режиме Легкого агента:

   - во время первоначальной настройки приложения в интерактивном (см. раздел "Первоначальная настройка приложения" на стр. 33) или автоматическом режиме (см. раздел "Автоматический режим первоначальной настройки приложения" на стр. 41) (в случае установки с помощью командной строки);
   - в конфигурационном файле autoinstall.ini (см. раздел "Параметры конфигурационного файла autoinstall.ini" на стр. 57), который включается в инсталляционный пакет приложения (в случае установки с помощью Kaspersky Security Center).

   После установки Kaspersky Endpoint Security изменить режим использования приложения невозможно.

   При выборе режима Легкого агента вы также можете настроить следующие параметры работы Kaspersky Endpoint Security в режиме Легкого агента:

   - Роль виртуальной машины, которую вы хотите защищать, в виртуальной инфраструктуре: сервер или рабочай станция. Роль виртуальной машины определяет, по какой лицензии будет использоваться приложение на этой виртуальной машине, и объем доступной функциональности.

- Режим защиты инфраструктуры VDI. Рекомендуется включить этот режим, если вы устанавливаете приложение на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах.

2. Настроить параметры подключения Легкого агента к SVM и параметры подключения Легкого агента к Серверу интеграции.

Компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент. Осуществляет взаимодействие между компонентами Kaspersky Endpoint Security и виртуальной инфраструктурой.

Secure virtual machine – специальная виртуальная машина, на которой установлена служба scanserver (Сервер защиты, компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент).

Kaspersky Endpoint Security в режиме Легкого агента взаимодействует с другими компонентами решения Kaspersky Security для виртуальных сред Легкий агент: Сервером интеграции и Сервером защиты, установленным на SVM (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254032.htm). Для взаимодействия с Сервером защиты Kaspersky Endpoint Security устанавливает и поддерживает подключение к SVM, на которой установлен этот Сервер защиты.

Подключение к Серверу интеграции требуется, если вы хотите, чтобы Легкие агенты получали информацию об SVM через Сервер интеграции, или если вы хотите защищать соединение между Сервером защиты и Легким агентом.

Вы можете настроить параметры подключения в политике Kaspersky Endpoint Security с помощью Консоли администрирования Kaspersky Security Center (см. раздел "Режим Легкого агента" на стр. 345) или с помощью Kaspersky Security Center Web Console (см. раздел "Режим Легкого агента" на стр. 462).

Информацию о параметрах работы приложения в режиме Легкого агента, о подключении к Серверу интеграции и к SVM вы можете получить с помощью команд приложения:--ksvla-info, --viis-info и --svm-info.

Информация о режиме использования приложения отображается в Kaspersky Security Center в свойствах приложения Kaspersky Endpoint Security на управляемом устройстве в разделе **Компоненты**. Информация отображается в строке **Режим Легкого агента для защиты виртуальных сред** следущим образом:

- статус *выполняется* означает, что приложение используется в режиме Легкого агента;
- статус *не установлено* означает, что приложение используется в автономном режиме.

Об активации приложения в режиме Легкого агента

Если Kaspersky Endpoint Security используется в режиме Легкого агента, отдельно активировать приложение не требуется. Вы активируете решение Kaspersky Security для виртуальных сред Легкий агент, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионного ключа на SVM. См. подробнее в справке Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/74253.htm.

После активации решения и подключения Легкого агента к SVM компонент Сервер защиты передает информацию о лицензии Легкому агенту. При выборе SVM для подключения Легкий агент учитывает среди прочих параметров тип лицензионного ключа, добавленного на SVM. Легкий агент не подключается к SVM, если тип ключа, добавленного на SVM, не соответствует роли защищенной виртуальной машины в виртуальной инфраструктуре (сервер или рабочая станция). См. подробнее в справке Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254867.htm.

Информацию о лицензии, которую использует Легкий агент для Linux, вы можете посмотреть на защищенной виртуальной машине с Легким агентом с помощью команды -L --query.

Не поддерживается управление лицензионными ключами с помощью задачи Kaspersky Endpoint Security *Добавление ключа* и с помощью команд Kaspersky Endpoint Security для добавления и удаления лицензионных ключей.

Об обновлении баз и модулей приложения в режиме Легкого агента

Kaspersky Endpoint Security в режиме Легкого агента использует базы вредоносного ПО, необходимые для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Kaspersky Endpoint Security получает от Сервера защиты обновления баз и программных модулей. См. подробнее в справке Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/255465.htm.

Допускается устанавливать только обновления модулей приложения, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу приложения из сертифицированного состояния.

Обновление баз на защищенных виртуальных машинах выполняется с помощью специальной локальной задачи приложения Kaspersky Endpoint Security *Обновление*, в которой в качестве источника обновлений указана папка на SVM. Задача обновления запускается автоматически. Вы не можете удалять эту задачу и изменять ее параметры.

Не поддерживается обновление из источников, отличных от папки на SVM, и использование групповых задач обновления.

Откат последнего обновления баз также выполняется на стороне Сервера защиты. После отката обновления баз на SVM на защищенной виртуальной машине автоматически запускается специальная локальная задача *Обновление*. В результате выполнения задачи Легкий агент возвращается к использованию предыдущего набора баз.

Не поддерживается использование локальной и групповой задачи приложения Kaspersky Endpoint Security *Откат обновления баз*.

Другие особенности использования приложения в режиме Легкого агента

Если Kaspersky Endpoint Security используется в режиме Легкого агента:

- Недоступно управление приложением с помощью графического пользовательского интерфейса.
- При проверке и защите не используется технология iChecker. Оптимизация проверки реализована средствами Сервера защиты.
- Не поддерживается использование облачных баз.
- Kaspersky Endpoint Security может взаимодействовать с серверами KSN с помощью прокси-сервера KSN. Взаимодействие с KSN напрямую на поддерживается.
- Использование прокси-сервера не поддерживается при подключении к Серверу интеграции, к SVM и к серверам KSN.

kaspersky

Подготовка к установке приложения

Общие действия

Перед началом установки приложения Kaspersky Endpoint Security вам нужно выполнить следующие действия:

- Убедиться в том, что программные и аппаратные ресурсы устройства, на который будет произведена установка, удовлетворяют требованиям (см. раздел "Требования" на стр. 19).
- Убедиться в том, что для операционной системы и программных средств, необходимых для установки (если таковые имеются), установлены самые последние пакеты обновлений, выпускаемые производителями операционной системы и программного обеспечения.
- 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.
- На устройствах с операционными системами, не поддерживающими технологию fanotify, убедиться в том, что установлены:
  - пакеты для компиляции программ и запуска задач (gcc, binutils, glibc, glibc-devel, make);
  - пакет с заголовочными файлами ядра операционной системы для компиляции модулей Kaspersky Endpoint Security.
- 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 Endpoint Security. Для корректной работы Kaspersky Endpoint Security 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**).
- Если на вашем устройстве используется ядро Linux ниже 3.16, то для корректной работы задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA) нужно убедиться, что служба auditd не запущена или не установлена.

- Для работы задач Управление сетевым экраном и Защита от веб-угроз (см. раздел "Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)" на стр. 206) требуется установить на вашем устройстве пакет утилит iptables.
- Для работы плагина управления Kaspersky Endpoint Security на устройстве, где установлен Сервер администрирования Kaspersky Security Center требуется установить Microsoft® Visual C++® 2015 Redistributable Update 3 RC (см. https://www.microsoft.com/ru-ru/download/details.aspx?id=52685 https://www.microsoft.com/ru-ru/download/details.aspx?id=52685).
- Для запуска 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.

Дополнительные действия перед установкой Kaspersky Endpoint Security в режиме Легкого агента

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент), вам нужно выполнить дополнительно следующие действия перед началом установки приложения Kaspersky Endpoint Security:

- Убедиться в том, что на виртуальных машинах, которые вы хотите защищать, установлены следующие пакеты, в зависимости от виртуальной инфраструктуры, в которой развернуто решение Kaspersky Security для виртуальных сред Легкий агент:
  - В инфраструктуре Microsoft Hyper-V на виртуальных машинах должен быть установлен пакет служб интеграции (Integration Services).
  - В инфраструктуре VMware vSphere на виртуальных машинах должен быть установлен пакет VMware Tools.
  - В инфраструктуре Citrix Hypervisor на виртуальных машинах должна быть установлена программа XenTools.
  - В инфраструктуре HUAWEI FusionSphere на виртуальных машинах должен быть установлен пакет HUAWEI Tools.
  - В инфраструктуре KVM, Облачная платформа ТИОНИКС, OpenStack, Astra Linux и Альт Сервер Виртуализации на виртуальных машинах должен быть установлен QEMU Guest Agent.
- Убедиться в том, что в настройках сетевого оборудования или программного обеспечения, обеспечивающего контроль трафика между виртуальными машинами, разрешено прохождение сетевого трафика через порты, которые используются для взаимодействия приложения Kaspersky Endpoint Security в режиме Легкого агента с другими компонентами решения Kaspersky Security для виртуальных сред Легкий агент. Подробнее о компонентах решения см. в справке Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254032.htm.

Таблица 1. Порты, используемые в работе Легкого агента

Порт и протокол	Направление	Назначение и описание
7271 TCP	От Легкого агента к Серверу интеграции.	Для взаимодействия Легкого агента и Сервера интеграции.
8000 UDP	От SVM к Легкому агенту.	Для передачи Легким агентам информации о доступных SVM с использованием списка адресов SVM.
8000 UDP	От Легкого агента к SVM.	Для получения Легким агентом информации о состоянии SVM.
11111 TCP	От Легкого агента к SVM.	Для передачи служебных запросов (например, на получение информации о лицензии) от Легкого агента Серверу защиты при незащищенном соединении.
11112 TCP	От Легкого агента к SVM.	Для передачи служебных запросов (например, на получение информации о лицензии) от Легкого агента Серверу защиты при защищенном соединении.
9876 TCP	От Легкого агента к SVM.	Для передачи запросов на проверку файлов от Легкого агента Серверу защиты при незащищенном соединении.
9877 TCP	От Легкого агента к SVM.	Для передачи запросов на проверку файлов от Легкого агента Серверу защиты при защищенном соединении.
80 TCP	От Легкого агента к SVM.	Для обновления баз и программных модулей решения на Легком агенте.
15000 UDP	От Kaspersky Security Center к SVM.	Для управления Сервером защиты через Kaspersky Security Center.
15000 UDP	От Kaspersky Security Center к Легким агентам.	Для управления Легким агентом через Kaspersky Security Center.
13000 TCP	От Легкого агента к Kaspersky Security Center.	Для управления Легким агентом через Kaspersky Security Center при защищенном соединении.
14000 TCP	От Легкого агента к Kaspersky Security Center.	Для управления Легким агентом через Kaspersky Security Center при незащищенном соединении.

kaspersky

Установка приложения

Перед началом установки приложения Kaspersky Endpoint Security требуется выполнить подготовку к установке.

Сценарии ниже описывают установку и первоначальную настройку приложения Kaspersky Endpoint Security, а также установку и настройку Агента администрирования Kaspersky Security Center и установку плагинов управления Kaspersky Endpoint Security. Сценарий установки зависит от режима (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), в котором вы планируете использовать приложение Kaspersky Endpoint Security.

Автономный режим

Если вы планируете использовать приложение Kaspersky Endpoint Security в автономном режиме, установка и первоначальная настройка Kaspersky Endpoint Security состоит из следующих этапов:

a. **Установка и первоначальная настройка Агента администрирования**

   Если вы планируете управлять приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, установите на защищаемом устройстве Агент администрирования Kaspersky Security Center и настройте его параметры (см. раздел "Установка и настройка Агента администрирования Kaspersky Security Center" на стр. 46).

b. **Установка плагина управления Kaspersky Endpoint Security**

   Если вы планируете управлять приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, установите плагин управления Kaspersky Endpoint Security (см. раздел "Установка плагинов управления Kaspersky Endpoint Security" на стр. 48). В зависимости от консоли управления Kaspersky Security Center используются следующие плагины управления:

   - Mmc-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Консоль администрирования Kaspersky Security Center. Mmc-плагин устанавливается на устройстве, где установлена Консоль администрирования Kaspersky Security Center.
   - Веб-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console.

     Веб-плагин устанавливается на устройство с установленным приложением Kaspersky Security Center Web Console.

c. **Установка пакетов приложения и графического пользовательского интерфейса**

   Kaspersky Endpoint Security и графический пользовательский интерфейс распространяются в пакетах форматов DEB и RPM. Установите Kaspersky Endpoint Security и, если требуется, графический пользовательский интерфейс из пакетов требуемого формата.

   Вы можете выполнить установку с помощью командной строки (см. раздел "Установка приложения с помощью командной строки" на стр. 32) или через Kaspersky Security Center (см. раздел "Развертывание приложения с помощью Kaspersky Security Center" на стр. 50), используя Консоль администрирования или Kaspersky Security Center Web Console.

d. **Первоначальная настройка Kaspersky Endpoint Security**

   Выполнение первоначальной настройки требуется для включения защиты клиентского устройства.

   Если вы установили приложение Kaspersky Endpoint Security с помощью командной строки, запустите скрипт первоначальной настройки (см. раздел "Первоначальная настройка приложения" на стр. 33) или выполните первоначальную настройку в автоматическом режиме (см. раздел "Автоматический режим первоначальной настройки приложения" на стр. 41).

Если вы установили приложение Kaspersky Endpoint Security с помощью Kaspersky Security Center, выполните подготовку приложения к работе (см. раздел "Подготовка приложения к работе через Kaspersky Security Center" на стр. 62).

Режим Легкого агента

> Не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред на операционных системах для архитектуры Arm.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, установка и первоначальная настройка Kaspersky Endpoint Security состоит из следующих этапов:

a. **Установка и первоначальная настройка Агента администрирования**

   Установите на виртуальные машины и шаблоны виртуальных машин Агент администрирования Kaspersky Security Center и настройте его параметры (см. раздел "Установка и настройка Агента администрирования Kaspersky Security Center" на стр. 46).

   Если вы устанавливаете Агент администрирования на шаблон, из которого будут создаваться временные виртуальные машины, рекомендуется настроить параметры, которые позволяют оптимизировать работу на временных виртуальных машинах. Подробнее об установке на шаблон виртуальных машин см. в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/98763.htm.

b. **Установка плагина управления Kaspersky Endpoint Security**

   Установите плагин управления Kaspersky Endpoint Security (см. раздел "Установка плагинов управления Kaspersky Endpoint Security" на стр. 48). В зависимости от консоли управления Kaspersky Security Center используются следующие плагины управления:

   - Mmc-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Консоль администрирования Kaspersky Security Center. Mmc-плагин устанавливается на устройстве, где установлена Консоль администрирования Kaspersky Security Center.
   - Веб-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console. Веб-плагин устанавливается на устройство с установленным приложением Kaspersky Security Center Web Console.

c. **Установка пакетов приложения**

   Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM. Установите Kaspersky Endpoint Security из пакета требуемого формата.

   > Графический пользовательский интерфейс не поддерживается, если Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

   Вы можете выполнить установку с помощью командной строки (см. раздел "Установка приложения с помощью командной строки" на стр. 32) или через Kaspersky Security Center (см. раздел "Развертывание приложения с помощью Kaspersky Security Center" на стр. 50), используя Консоль администрирования или Kaspersky Security Center Web Console.

   В случае установки через Kaspersky Security Center вам нужно выбрать режим Легкого агента в файле autoinslall.ini (`KSVLA_MODE=yes`) и включить этот файл в инсталляционный пакет, используемый при установке приложения. Если вы устанавливаете Kaspersky Endpoint Security на

шаблон, из которого будут создаваться временные виртуальные машины, в файле autoinslall.ini рекомендуется также настроить параметр `VDI_MODE=yes`, который позволяет оптимизировать работу на временных виртуальных машинах.

d. Первоначальная настройка Kaspersky Endpoint Security

Выполнение первоначальной настройки требуется для включения защиты клиентского устройства.

- Если вы установили приложение Kaspersky Endpoint Security с помощью командной строки, запустите скрипт первоначальной настройки (см. раздел "Первоначальная настройка приложения" на стр. 33) или выполните первоначальную настройку в автоматическом режиме (см. раздел "Автоматический режим первоначальной настройки приложения" на стр. 41). Вам нужно выбрать режим Легкого агента одним из следующих способов:
  - Ввести `yes` на шаге `Specifying the application usage` скрипта первоначальной настройки.
  - Задать в конфигурационном файле первоначальной настройки параметр `KSVLA_MODE=yes`.

  Если вы устанавливаете Kaspersky Endpoint Security на шаблон, из которого будут создаваться временные виртуальные машины, рекомендуется также настроить параметр, который позволяет оптимизировать работу на временных виртуальных машинах. Подробнее об установке на шаблон виртуальных машин см. в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/98763.htm.
- Если вы установили приложение Kaspersky Endpoint Security с помощью Kaspersky Security Center, выполните подготовку приложения к работе (см. раздел "Подготовка приложения к работе через Kaspersky Security Center" на стр. 62).

В этом разделе

Развертывание приложения с помощью командной строки

Приложение Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM. Предусмотрены отдельные пакеты для приложения и графического пользовательского интерфейса.

Вы можете выполнить следующие действия при установке приложения:

- Установить пакет приложения без графического пользовательского интерфейса.
- Установить пакет графического пользовательского интерфейса.

Невозможно установить пакет графического пользовательского интерфейса на клиентское устройство, на котором не установлен пакет приложения.
Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент), графический пользовательский интерфейс не поддерживается. Вам нужно установить пакет приложения без графического пользовательского интерфейса.

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 с помощью командной строки требуется выполнить первоначальную настройку приложения путем запуска скрипта первоначальной настройки (см. раздел "Первоначальная настройка приложения" на стр. 33) или в автоматическом режиме (см. раздел "Автоматический режим первоначальной настройки приложения" на стр. 41).

В этом разделе

Установка приложения с помощью командной строки

Установка пакета приложения без графического пользовательского интерфейса

► *Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 64-битную операционную систему для архитектуры Arm, выполните следующую команду:*

```
# rpm -i kesl-12.0-<номер сборки>.aarch64.rpm
```

► *Чтобы установить Kaspersky Endpoint Security из пакета формата DEB на 64-битную операционную систему для архитектуры Arm, выполните следующую команду:*

```
# apt-get install ./kesl_12.0-<номер сборки>_arm64.deb
```

Установка пакета графического интерфейса

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

```
# rpm -i kesl-gui-12.0-<номер сборки>.aarch64.rpm
```

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

```
# apt-get install ./kesl-gui_12.0-<номер сборки>_arm64.deb
```

Первоначальная настройка приложения

После установки приложения Kaspersky Endpoint Security с помощью командной строки требуется выполнить первоначальную настройку приложения, запустив скрипт первоначальной настройки. Скрипт первоначальной настройки входит в пакет Kaspersky Endpoint Security.

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

► *Чтобы запустить скрипт первоначальной настройки Kaspersky Endpoint Security, выполните следующую команду:*

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

Скрипт первоначальной настройки требуется запускать с root-правами после завершения установки пакета Kaspersky Endpoint Security. Скрипт пошагово запрашивает значения параметров Kaspersky Endpoint Security. 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

В этом разделе

Выбор режима использования приложения

На этом шаге выберите режим использования приложения Kaspersky Endpoint Security (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23):

- Введите `yes`, если вы хотите использовать Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.
- Введите `no`, если вы хотите использовать Kaspersky Endpoint Security в автономном режиме.

После завершения первоначальной настройки изменить режим использования приложения невозможно.

Определение роли виртуальной машины

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

На этом шаге укажите роль виртуальной машины (сервер или рабочая станция), на которую вы устанавливаете приложение Kaspersky Endpoint Security:

- Введите `yes`, если вы используете виртуальную машину как сервер.
- Введите `no`, если вы используете виртуальную машину как рабочую станцию.

Включение режима защиты инфраструктуры VDI

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

На этом шаге вы можете включить режим защиты инфраструктуры VDI. Этот режим позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. Если режим защиты инфраструктуры VDI включен, то обновления, требующие перезагрузки виртуальной машины, не устанавливаются. При получении обновлений, требующих перезагрузки, Легкий агент, установленный на виртуальной машине, отправляет в Kaspersky Security Center сообщение о необходимости обновить шаблон защищенных виртуальных машин.

Введите `yes`, если вы хотите включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки Kaspersky Endpoint Security на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины.

Введите `no`, если не требуется включать режим защиты инфраструктуры VDI. Рекомендуется в случае установки Kaspersky Endpoint Security на постоянную виртуальную машину или на шаблон виртуальных машин, из которого будут создаваться постоянные виртуальные машины.

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 Endpoint Security 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.

kaspersky

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 Endpoint Security 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 Endpoint Security 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 ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network находится в директории /opt/kaspersky/kesl/doc/.

Введите одно из следующих значений:

- `yes` (или `y`), если вы принимаете условия Положения о Kaspersky Security Network. Будет включен расширенный режим KSN (см. раздел "Использование Kaspersky Security Network" на стр. 260).
- `no` (или `n`), если вы не принимаете условия Положения о Kaspersky Security Network.

Отказ от использования Kaspersky Security Network не прерывает процесс установки приложения Kaspersky Endpoint Security. Вы можете в любой момент включить, выключить или изменить режим Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network с помощью командной строки" на стр. 262).

Если приложение Kaspersky Endpoint Security используется в автономном режиме и вы включили использование Kaspersky Security Network, автоматически включается облачный режим работы приложения (см. раздел "Использование Kaspersky Security Network" на стр. 260), при котором Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО. В режиме Легкого агента для защиты виртуальных сред работа с облегченными базами вредоносного ПО не поддерживается.

Включение облачного режима приводит к выходу приложения из сертифицированного состояния.

Удаление пользователей из привилегированных групп

Этот шаг отображается, только если обнаружены пользователи в группе kesladmin и/или в группе keslaudit.

На этом шаге укажите, следует ли удалить пользователей из привилегированных групп kesladmin и keslaudit. Пользователи, включенные в группы kesladmin и keslaudit, получают привилегированный доступ к функциям приложения (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. 88).

Введите `yes`, чтобы удалить всех обнаруженных пользователей из группы kesladmin и/или keslaudit. Пользователи, для которых группа kesladmin или keslaudit 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. 88) администратора (admin).

Введите имя пользователя, которому вы хотите назначить роль администратора.

Вы можете назначить пользователю роль (см. раздел "Назначение роли пользователю" на стр. 89) 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 Endpoint Security 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 Endpoint Security.

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 Endpoint Security.

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. 67) для работы с приложение позже, после завершения первоначальной настройки приложения Kaspersky Endpoint Security.

Настройка источника обновлений

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в автономном режиме. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает обновления баз и программных модулей Легкого агента от Сервера защиты.

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.

kaspersky

Настройка параметров прокси-сервера

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в автономном режиме.

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. 39) 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, без использования скрипта первоначальной настройки.

Запуск обновления баз приложения

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в автономном режиме. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает обновления баз и программных модулей Легкого агента от Сервера защиты.

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 Endpoint Security обеспечивает защиту устройства только после обновления баз приложения.

Вы можете запустить задачу обновления (см. раздел "Запуск и остановка задачи" на стр. 123) без использования скрипта первоначальной настройки.

Включение автоматического обновления баз приложения

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в автономном режиме. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает обновления баз и программных модулей Легкого агента от Сервера защиты.

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.

Активация приложения

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в автономном режиме. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает информацию о лицензии от Сервера защиты, отдельно активировать Kaspersky Endpoint Security не требуется.

На этом шаге вам нужно активировать приложение с помощью файла ключа (см. раздел "О лицензионном ключе" на стр. 77).

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

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

Вы можете активировать приложение позже, (см. раздел "Задача Лицензирование (License, ID:9)" на стр. 177) без использования скрипта первоначальной настройки.

kaspersky

Автоматический режим первоначальной настройки приложения

Вы можете выполнить первоначальную настройку приложения в автоматическом режиме.

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

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

где <конфигурационный файл первоначальной настройки> – путь к конфигурационному файлу, который содержит параметры первоначальной настройки (см. раздел "Параметры конфигурационного файла первоначальной настройки" на стр. 41). Вы можете создать этот файл или скопировать структуру для него из конфигурационного файла autoinstall.ini (см. раздел "Параметры конфигурационного файла autoinstall.ini" на стр. 57), который используется для удаленной установки приложения с помощью Консоли администрирования.

Завершение работы скрипта 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.

Для корректного обновления модулей приложения после завершения работы скрипта может потребоваться перезапустить приложение. Проверьте состояние обновлений для приложения с помощью команды kesl-control --app-info (см. раздел "Просмотр информации о приложении" на стр. 95).

Параметры конфигурационного файла первоначальной настройки

В конфигурационном файле первоначальной настройки вы можете задавать параметры, приведенные в таблице ниже. Набор применимых параметров зависит от режима использования приложения.

Таблица 2. Параметры конфигурационного файла первоначальной настройки

Параметр	Описание	Значения
KSVLA_MODE	Режим использования Kaspersky Endpoint Security (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23).	yes – Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент). no – Kaspersky Endpoint Security используется в автономном режиме.

Параметр	Описание	Значения
SERVER_MODE	Роль защищаемой виртуальной машины (см. раздел "Определение роли виртуальной машины" на стр. 34) (сервер или рабочая станция). Параметр применяется, только если приложение используется в режиме Легкого агента.	`yes` – защищаемая виртуальная машина используется как сервер. `no` – защищаемая виртуальная машина используется как рабочая станция.
VDI_MODE	Включение режима защиты инфраструктуры VDI (см. раздел "Включение режима защиты инфраструктуры VDI" на стр. 35) для оптимизации работы приложения на временных виртуальных машинах. Параметр применяется, только если приложение используется в режиме Легкого агента.	`yes` – включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки Kaspersky Endpoint Security на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. `no` – не включать режим защиты инфраструктуры VDI.

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 приложение Kaspersky Endpoint Security используется в автономном режиме и вы включили использование KSN, автоматически включается облачный режим работы приложения (см. раздел "Использование Kaspersky Security Network" на стр. 260). Включение облачного режима приводит к выходу приложения из сертифицированного состояния.

Параметр	Описание	Значения
GROUP_CLEAN	Обязательный параметр. Удаление пользователей из привилегированных групп kesladmin и keslaudit.	`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	Файл ключа. Параметр применяется, только если приложение используется в автономном режиме.	
UPDATER_SOURCE	Источник обновлений. Параметр применяется, только если приложение используется в автономном режиме.	`SCServer` – использовать в качестве источника обновлений Сервер администрирования Kaspersky Security Center. `KLServers` – использовать в качестве источника обновлений серверы "Лаборатории Касперского". Адрес источника обновлений.

Параметр	Описание	Значения
PROXY_SERVER	Адрес прокси-сервера, используемого для подключения к интернету. Параметр применяется, только если приложение используется в автономном режиме.	Адрес прокси-сервера.
UPDATE_EXECUTE	Запуск задачи обновления баз приложения во время процедуры настройки. Параметр применяется, только если приложение используется в автономном режиме.	`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 назначается роль администратора (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. 88) (admin).	
CONFIGURE_SELINUX	Автоматическая настройка SELinux для работы с приложением Kaspersky Endpoint Security.	`yes` – выполнить автоматическую настройку SELinux для работы с Kaspersky Endpoint Security. `no` – не выполнять автоматическую настройку SELinux для работы с Kaspersky Endpoint Security.

Параметр	Описание	Значения
DISABLE_PROTECTION	Выключение компонентов защиты и задач проверки приложения после его установки. Установка с выключенными компонентами защиты может быть удобна, например, для воспроизведения проблемы в работе приложения с целью создания файла трассировки. Если после установки приложения с параметром `DISABLE_PROTECTION=yes` вы включите нужные компоненты и задачи, то после перезапуска приложения включенные компоненты и задачи продолжат работу.	`yes` – выключить компоненты защиты и задачи проверки при запуске приложения после установки. `no` – не выключать компоненты защиты и задачи проверки 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).

Установка и настройка Агента администрирования Kaspersky Security Center

Установка Агента администрирования требуется для управления приложением Kaspersky Endpoint Security 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 (см. раздел "Установка Агента администрирования с помощью командной строки" на стр. 47) и первоначальную настройку (см. раздел "Первоначальная настройка Агента администрирования с помощью командной строки" на стр. 47) Агента администрирования с помощью командной строки. Установка и настройка Агента администрирования также может быть выполнена удаленно с помощью Kaspersky Security Center (см. подробнее в документации Kaspersky Security Center https://support.kaspersky.com/KSC/14/ru-RU/5022.htm).

В этом разделе

kaspersky

Установка Агента администрирования с помощью командной строки

Процесс установки Агента администрирования требуется запускать с root-правами.

► *Чтобы установить Агент администрирования из пакета формата RPM на 64-битную операционную систему для архитектуры Arm, выполните следующую команду:*

```
# rpm -i klnagent64-<номер сборки>.aarch64.rpm
```

► *Чтобы установить Агент администрирования из пакета формата DEB на 64-битную операционную систему для архитектуры Arm, выполните следующую команду:*

```
# apt-get install ./klnagent64_<номер сборки>_arm64.deb
```

После установки пакета выполните первоначальную настройку Агента администрирования. (см. раздел "Первоначальная настройка Агента администрирования с помощью командной строки" на стр. 47)

Первоначальная настройка Агента администрирования с помощью командной строки

► *Чтобы настроить параметры Агента администрирования:*

1. Выполните команду:
   - 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
     ```

2. Примите условия Лицензионного соглашения.
3. Укажите DNS-имя или IP-адрес Сервера администрирования.
4. Укажите номер порта Сервера администрирования.

   По умолчанию используется порт 14000.
5. Если вы хотите использовать SSL-соединение, укажите номер SSL-порта Сервера администрирования.

   По умолчанию используется порт 13000.
6. Выполните одно из следующих действий:
   - Введите `yes`, чтобы использовать SSL-соединение.
   - Введите `no`, чтобы не использовать SSL-соединение.

   По умолчанию SSL-соединение включено.
7. Если требуется, укажите режим использования шлюза соединений:

- 1 – не настраивать шлюз соединений.
- 2 – не использовать шлюз соединений.
- 3 – подключаться к Серверу администрирования через шлюз соединений.
- 4 – использовать Агент администрирования в качестве шлюза соединений.

По умолчанию используется вариант 1.

Для получения подробной информации о настройке Агента администрирования обратитесь к документации Kaspersky Security Center https://support.kaspersky.com/KSC/14/ru-RU/5022.htm.

Установка плагинов управления Kaspersky Endpoint Security

Для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center используются следующие плагины управления Kaspersky Endpoint Security:

- mmc-плагин (см. раздел "Об mmc-плагине управления Kaspersky Endpoint Security" на стр. 48) управления Kaspersky Endpoint Security позволяет управлять работой приложением через Консоль администрирования Kaspersky Security Center;
- веб-плагин (см. раздел "О веб-плагине управления Kaspersky Endpoint Security" на стр. 49) управления Kaspersky Endpoint Security позволяет управлять работой приложения через Kaspersky Security Center Web Console.

Вы можете одновременно установить плагины управления для разных версий приложения Kaspersky Endpoint Security. Таким образом вы сможете управлять приложением, используя политики, созданные с помощью разных версий плагина управления. Вы можете также конвертировать политики и задачи, созданные с помощью предыдущих версий плагина управления, в новые версии.

В этом разделе

Об mmc-плагине управления Kaspersky Endpoint Security

Mmc-плагин управления Kaspersky Endpoint Security (далее также *mmc-плагин*) обеспечивает взаимодействие приложения Kaspersky Endpoint Security с Kaspersky Security Center через Консоль администрирования. Mmc-плагин позволяет управлять приложением Kaspersky Endpoint Security с помощью политик и задач.

Mmc-плагин требуется установить на том же клиентском устройстве, на котором установлена Консоль администрирования Kaspersky Security Center.

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

Дополнительная информация о плагинах управления приведена в документации Kaspersky Security Center https://support.kaspersky.com/KSC/14/ru-RU/5022.htm.

О веб-плагине управления Kaspersky Endpoint Security

Веб-плагин управления Kaspersky Endpoint Security (далее также *веб-плагин*) обеспечивает взаимодействие приложения Kaspersky Endpoint Security с Kaspersky Security Center через Kaspersky Security Center Web Console. Веб-плагин позволяет управлять приложением Kaspersky Endpoint Security с помощью политик и задач.

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

Вы можете просмотреть список установленных веб-плагинов в интерфейсе Kaspersky Security Center Web Console: **Параметры Консоли** → **Веб-плагины**. Дополнительная информация о совместимости версий веб-плагина и Kaspersky Security Center Web Console приведена в документации Kaspersky Security Center https://support.kaspersky.com/KSC/14/ru-RU/5022.htm.

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

Установка веб-плагина

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 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 документации Kaspersky Security Center.

- Из списка доступных дистрибутивов в Kaspersky Security Center Web Console.

  Для установки веб-плагина выберите дистрибутив веб-плагина в интерфейсе Web Console: **Параметры Консоли** → **Веб-плагины**. Список доступных дистрибутивов обновляется автоматически после выпуска новых версий приложений "Лаборатории Касперского".

- Загрузить дистрибутив в Kaspersky Security Center Web Console из стороннего источника.

  Для установки веб-плагина добавьте ZIP-архив дистрибутива веб-плагина в интерфейсе Web Console: **Параметры Консоли** → **Веб-плагины**. Дистрибутив веб-плагина можно загрузить, например, на веб-сайте "Лаборатории Касперского". Для локальной версии приложения вам также нужно загрузить текстовый файл, содержащий сигнатуру.

Обновление веб-плагина

При появлении новой версии веб-плагина Kaspersky Security Center Web Console отобразит уведомление *Доступны обновления для используемых плагинов*. Вы можете перейти к обновлению версии веб-плагина

из уведомления Web Console. Также вы можете проверить наличие обновлений веб-плагина вручную в интерфейсе Web Console (**Параметры Консоли** → **Веб-плагины**). Предыдущая версия веб-плагина будет автоматически удалена во время обновления.

При обновлении веб-плагина сохраняются уже существующие элементы (например, политики или задачи). Новые параметры элементов, реализующие новые функции приложения Kaspersky Endpoint Security, появятся в существующих элементах и будут иметь значения по умолчанию.

Вы можете обновить веб-плагин следующими способами:

- В списке веб-плагинов в онлайн-режиме.

  Для обновления веб-плагина требуется выбрать дистрибутив веб-плагина Kaspersky Endpoint Security в интерфейсе Kaspersky Security Center Web Console и запустить обновление (**Параметры Консоли** → **Веб-плагины**). Web Console проверит наличие обновлений на серверах "Лаборатории Касперского" и загрузит необходимые обновления.

- Из файла.

  Для обновления веб-плагина требуется выбрать ZIP-архив дистрибутива веб-плагина Kaspersky Endpoint Security в интерфейсе Kaspersky Security Center Web Console: **Параметры Консоли** → **Веб-плагины**. Дистрибутив веб-плагина можно загрузить, например, на веб-сайте "Лаборатории Касперского". Для локальной версии приложения вам также нужно загрузить текстовый файл, содержащий сигнатуру.

  Вы можете обновить веб-плагин только до более новой версии. Обновить веб-плагин до более старой версии невозможно.

При открытии любого элемента (например, политики или задачи) веб-плагин проверяет информацию о совместимости. Если версия веб-плагина равна или выше версии, указанной в информации о совместимости, то вы можете изменять параметры этого элемента. В противном случае изменение параметров выбранного элемента с помощью веб-плагина недоступно. Рекомендуется обновить веб-плагин.

Развертывание приложения с помощью Kaspersky Security Center

Вы можете установить приложение Kaspersky Endpoint Security на клиентское устройство удаленно с рабочего места администратора с помощью Консоли администрирования Kaspersky Security Center или с помощью Kaspersky Security Center Web Console.

Для удаленной установки используется инсталляционный пакет приложения Kaspersky Endpoint Security. *Инсталляционный пакет* – это набор файлов, формируемый для удаленной установки приложений "Лаборатории Касперского" с помощью Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки приложения и обеспечения его работоспособности сразу после установки. Значения параметров соответствуют значениям параметров приложения по умолчанию. Инсталляционный пакет создается на основании файла с расширением kud, входящего в состав дистрибутива приложения. Инсталляционный пакет приложения Kaspersky Endpoint Security является общим для всех поддерживаемых операционных систем и типов архитектуры процессора.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23) (в составе решения Kaspersky Security для виртуальных сред Легкий агент), вам нужно настроить параметры в конфигурационном файле autoinstall.ini (см. раздел "Параметры конфигурационного файла autoinstall.ini" на стр. 57) и включить этот файл в инсталляционный пакет.

Вы можете развернуть приложение Kaspersky Endpoint Security на устройствах в сети организации несколькими способами.

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.

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.

Описание процедур развертывания см. в справке Kaspersky Security Center https://support.kaspersky.com/KSC/14/ru-RU/5022.htm.

При необходимости вы можете просмотреть журнал удаленной установки приложения в Web Console в свойствах управляемого устройства на закладке **Дополнительно** в разделе **Удаленная диагностика** (см. раздел "**Настройка удаленной диагностики клиентских устройств**" на стр. 499) или в Консоли администрирования с помощью утилиты удаленной диагностики (см. раздел "Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center" на стр. 389).

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), не поддерживается активация приложения во время установки и автоматическое распространение лицензионных ключей. Kaspersky Endpoint Security получает информацию о лицензии от Сервера защиты после подключения к SVM, отдельно активировать Kaspersky Endpoint Security не требуется.

Чтобы управлять с помощью Kaspersky Security Center работой приложения Kaspersky Endpoint Security, установленного на клиентских устройствах, вам нужно поместить эти устройства в группы администрирования. Перед началом установки приложения Kaspersky Endpoint Security 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).

kaspersky

В этом разделе

Создание инсталляционного пакета в Консоли администрирования Kaspersky Security Center

Перед тем, как создать инсталляционный пакет приложения Kaspersky Endpoint Security, вам нужно подготовить файлы, которые будут включены в пакет.

► *Чтобы подготовить файлы для создания инсталляционного пакета:*

1. Скачайте архив kesl.zip на странице загрузки приложений https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint?utm_content=downloads в разделе **Kaspersky Endpoint Security для Linux** (**Дополнительный дистрибутив -> Files for Product remote installation**).
2. Распакуйте архив kesl.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 Endpoint Security:
     - kesl-12.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
     - kesl_12.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)
   - для установки графического интерфейса:
     - kesl-gui-12.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
     - kesl-gui_12.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)

   Если вы не хотите устанавливать графический пользовательский интерфейс, не используйте эти файлы, тогда размер инсталляционного пакета будет меньше.
   Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, графический пользовательский интерфейс не поддерживается.

   Обратите внимание, что если графический пользовательский интерфейс не будет использоваться, то вам нужно установить значение параметра `USE_GUI=No` 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.

3. Если вы планируете использовать приложение Kaspersky Endpoint Security в автономном режиме и хотите использовать предварительно скачанные базы, в конфигурационном файле autoinstall.ini (см. раздел "Параметры конфигурационного файла autoinstall.ini" на стр. 57) вам нужно установить значение параметра `UPDATE_EXECUTE=no`.

4. Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред или вы хотите настроить параметры установки приложения, откройте конфигурационный файл autoinstall.ini (см. раздел "Параметры конфигурационного файла autoinstall.ini" на стр. 57) и внесите необходимые изменения. Файл autoinstall.ini находится в папке, в которую вы распаковали архив kesl.zip.

   Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, в конфигурационном файле autoinstall.ini вам нужно установить значение параметра `KSVLA_MODE=yes`.

► *Чтобы создать инсталляционный пакет Kaspersky Endpoint Security в Консоли администрирования Kaspersky Security Center:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
3. Нажмите на кнопку **Создать инсталляционный пакет**.

   Запустится мастер создания инсталляционного пакета.
4. В открывшемся окне мастера нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
5. Введите имя нового инсталляционного пакета и перейдите к следующему шагу.
6. Выберите дистрибутив приложения Kaspersky Endpoint Security. Для этого откройте стандартное окно Windows с помощью кнопки **Обзор** и укажите путь к файлу kesl.kud. Файл находится в папке, в которую вы распаковали архив kesl.zip.

   В окне отобразится название приложения.

   Перейдите к следующему шагу.
7. 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.
8. Мастер загружает файлы, необходимые для установки приложения, на Сервер администрирования Kaspersky Security Center. Дождитесь окончания загрузки.
9. 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.

Создание инсталляционного пакета в Kaspersky Security Center 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".

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред или хотите настроить дополнительные параметры установки приложения, вам нужно подготовить файлы, которые будут включены в инсталляционный пакет и создать пакет из архивного файла.

Если вы планируете использовать приложение Kaspersky Endpoint Security в автономном режиме и вам не требуется настройка дополнительных параметров установки, вы можете создать инсталляционный пакет из дистрибутива, размещенного на серверах "Лаборатории Касперского".

► *Чтобы подготовить архивный файл для создания инсталляционного пакета:*

1. Скачайте архив kesl.zip на странице загрузки приложений https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint?utm_content=downloads в разделе **Kaspersky Endpoint Security для Linux** (**Дополнительный дистрибутив -> Files for Product remote installation**).
2. Распакуйте архив kesl.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 Endpoint Security:
     - kesl-12.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
     - kesl_12.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)
   - для установки графического интерфейса:
     - kesl-gui-12.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
     - kesl-gui_12.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)

     Если вы не хотите устанавливать графический пользовательский интерфейс, не используйте эти файлы, тогда размер инсталляционного пакета будет меньше.
     Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, графический пользовательский интерфейс не поддерживается.

Обратите внимание, что если графический пользовательский интерфейс не будет использоваться, то вам нужно установить значение параметра `USE_GUI=No` 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.

3. Если вы планируете использовать приложение Kaspersky Endpoint Security в автономном режиме и хотите использовать предварительно скачанные базы, в конфигурационном файле autoinstall.ini (см. раздел "Параметры конфигурационного файла autoinstall.ini" на стр. 57) вам нужно установить значение параметра `UPDATE_EXECUTE=no`.
4. Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред или вы хотите настроить параметры установки приложения, откройте конфигурационный файл autoinstall.ini (см. раздел "Параметры конфигурационного файла autoinstall.ini" на стр. 57) и внесите необходимые изменения. Файл autoinstall.ini находится в папке, в которую вы распаковали архив kesl.zip.

   Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, в конфигурационном файле autoinstall.ini вам нужно установить значение параметра `KSVLA_MODE=yes`.

5. Поместите все подготовленные файлы в архив формата ZIP, CAB, TAR или TAR.GZ с произвольным именем.

► *Чтобы создать инсталляционный пакет Kaspersky Endpoint Security 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. Вам нужно выбрать этот вариант, если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.
   - **Создать инсталляционный пакет для программы "Лаборатории Касперского"**. Инсталляционный пакет будет создан из .дистрибутива, размещенного на серверах "Лаборатории Касперского".

Kaspersky Security Center Cloud Console не поддерживает создание инсталляционных пакетов из файла.

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 Endpoint Security. 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 Endpoint Security 12.0 для Linux 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. 57).

Таблица 3. 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 программу	Установите флажок, чтобы активировать приложение. Вы также можете активировать приложение после установки (см. раздел "Активация приложения через Kaspersky Security Center" на стр. 64). Параметр применяется, только если приложение используется в автономном режиме.

Раздел	Описание
Выберите источник обновлений	Укажите источник обновлений: • **Серверы обновлений "Лаборатории Касперского"**. • **Сервер администрирования Kaspersky Security Center**. • **Другие источники в локальной или глобальной сети**. Параметр применяется, только если приложение используется в автономном режиме.
Запустить задачу обновления баз после установки	Установите флажок, чтобы запустить задачу обновления после установки приложения. Параметр применяется, только если приложение используется в автономном режиме.
Указать параметры прокси-сервера	Установите флажок, чтобы указать адрес прокси-сервера, используемого для подключения к интернету. Параметр применяется, только если приложение используется в автономном режиме.
Установить исходный код ядра	Установите флажок, чтобы автоматически начать компиляцию модулей ядра.
Использовать графический пользовательский интерфейс	Установите флажок, чтобы включить использование графического пользовательского интерфейса. Параметр применяется, только если приложение используется в автономном режиме.
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. 88) (admin).
Выполнить автоматическую настройку SELinux	Установите флажок, чтобы выполнить автоматическую настройку SELinux для работы с Kaspersky Endpoint Security.

Параметры конфигурационного файла autoinstall.ini

В конфигурационном файле autoinstall.ini вы можете задавать параметры, приведенные в таблице ниже. Набор применимых параметров зависит от режима использования приложения.

Таблица 4. Параметры конфигурационного файла autoinstall.ini

Параметр	Описание	Значения
KSVLA_MODE	Режим использования Kaspersky Endpoint Security (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23).	`yes` – Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент). `no` (значение по умолчанию) – Kaspersky Endpoint Security используется в автономном режиме.
SERVER_MODE	Роль защищаемой виртуальной машины (см. раздел "Определение роли виртуальной машины" на стр. 34) (сервер или рабочая станция). Параметр применяется, только если приложение используется в режиме Легкого агента.	`yes` (значение по умолчанию) – защищаемая виртуальна машина используется как сервер. `no` – защищаемая виртуальна машина используется как рабочая станция.
VDI_MODE	Включение режима защиты инфраструктуры VDI (см. раздел "Включение режима защиты инфраструктуры VDI" на стр. 35) для оптимизации работы приложения на временных виртуальных машинах. Параметр применяется, только если приложение используется в режиме Легкого агента.	`yes` – включить режим защиты инфраструктуры VDI. Рекомендуется в случае устанавки Kaspersky Endpoint Security на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. `no` (значение по умолчанию) – не включать режим защиты инфраструктуры VDI.
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.

Параметр	Описание	Значения
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. 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` (значение по умолчанию) – не принимать условия Положения о Kaspersky Security Network. Если приложение Kaspersky Endpoint Security используется в автономном режиме и вы включили использование KSN, автоматически включается облачный режим работы приложения (см. раздел "Использование Kaspersky Security Network" на стр. 260). Включение облачного режима приводит к выходу приложения из сертифицированного состояния.
GROUP_CLEAN	Обязательный параметр. Удаление пользователей из привилегированных групп kesladmin и keslaudit.	`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 `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	Файл ключа. Параметр применяется, только если приложение используется в автономном режиме.	
UPDATER_SOURCE	Источник обновлений. Параметр применяется, только если приложение используется в автономном режиме.	`SCServer` – использовать в качестве источника обновлений Сервер администрирования Kaspersky Security Center. `KLServers` – 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. Параметр применяется, только если приложение используется в автономном режиме.	Адрес прокси-сервера.

Параметр	Описание	Значения
UPDATE_EXECUTE	Запуск задачи обновления баз приложения во время процедуры настройки. Параметр применяется, только если приложение используется в автономном режиме.	`yes` (значение по умолчанию) – запускать задачу обновления. `no` – не запускать задачу обновления.
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра.	`yes` (значение по умолчанию) – компилировать модуль ядра. `no` – не компилировать модуль ядра.
USE_GUI	Использование графического пользовательского интерфейса. Параметр применяется, только если приложение используется в автономном режиме.	`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. 88) (admin).	Нет
CONFIGURE_SELINUX	Автоматическая настройка SELinux для работы с приложением Kaspersky Endpoint Security.	`yes` (значение по умолчанию) – выполнить автоматическую настройку SELinux для работы с Kaspersky Endpoint Security. `no` – не выполнять автоматическую настройку SELinux для работы с Kaspersky Endpoint Security.

Параметр	Описание	Значения
DISABLE_PROTECTION	Выключение компонентов защиты и задач проверки приложения после его установки. Установка с выключенными компонентами защиты может быть удобна, например, для воспроизведения проблемы в работе приложения с целью создания файла трассировки. Если после установки приложения с параметром `DISABLE_PROTECTION=yes` вы включите нужные компоненты и задачи, то после перезапуска приложения включенные компоненты и задачи продолжат работу.	`yes` – выключить компоненты защиты и задачи проверки при запуске приложения после установки. `no` – не выключать компоненты защиты и задачи проверки 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 через Kaspersky Security Center

После развертывания приложения Kaspersky Endpoint Security через Kaspersky Security Center требуется подготовить приложение к работе. Действия, которые необходимо выполнить, зависят от режима (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), в котором вы планируете использовать приложение Kaspersky Endpoint Security.

Автономный режим

Если вы планируете использовать приложение Kaspersky Endpoint Security в автономном режиме, после развертывания приложения вам нужно выполнить следующие действия:

- Активировать приложение. Вы можете создать и выполнить задачу активации через Консоль администрирования (см. раздел "Добавление ключа" на стр. 356) или через Kaspersky Security Center Web Console (см. раздел "Добавление ключа" на стр. 471), а также распространить на устройства лицензионный ключ из хранилища ключей Kaspersky Security Center (см. раздел "Активация приложения через Kaspersky Security Center" на стр. 64).
- Обновить базы и модули приложения через Консоль администрирования или через Kaspersky Security Center Web Console. Вы можете использовать задачу *Обновление*, которая создана автоматически мастером первоначальной настройки Kaspersky Security Center после установки mmc-плагина управления или веб-плагина управления Kaspersky Endpoint Security.
- Настроить политику для централизованного управления работой приложенияс помощью Консоли администрирования Kaspersky Security Center или Web Console. Вы можете использовать политику,

которая создана автоматически мастером первоначальной настройки Kaspersky Security Center после установки mmc-плагина управления или веб-плагина управления Kaspersky Endpoint Security.

Также вы можете настроить задачи управления приложением с помощью Консоли администрирования или Web Console.

Режим Легкого агента

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, после развертывания приложения вам нужно выполнить следующие действия:

1. Настроить параметры обнаружения SVM Легкими агентами. Для этого вам нужно создать и настроить политику для централизованного управления работой приложения на клиентских устройствах. Для работы с политиками вы можете использовать Консоль администрирования или Web Console.

   В политике вам нужно настроить следующие параметры:

   - Параметры подключения Легких агентов к Серверу интеграции.
   - Параметры подключения Легких агентов к SVM.

2. Убедиться в том, что установлено подключение Легких агентов к SVM и к Серверу интеграции.

   Вы можете получить информацию о подключении с помощью команд Kaspersky Endpoint Security на защищенной виртуальной машине:

   - Информацию о подключении к SVM вы можете посмотреть с помощью команды `kesl-control [-V] --viis-info`.
   - Информацию о подключении к Серверу интеграции вы можете посмотреть с помощью команды `kesl-control [-V] --svm-info`.

3. Убедиться в том, что приложение Kaspersky Endpoint Security, используемое в качестве Легкого агента, получает информацию о лицензии, по которой активировано решение Kaspersky Security для виртуальных сред Легкий агент.

   После активации решения на SVM и подключения Легких агентов к SVM компонент Сервер защиты передает информацию о лицензии Легким агентам. Информацию о лицензии, которую использует приложение Kaspersky Endpoint Security в составе решения, вы можете посмотреть на защищенной виртуальной машине с помощью команды `kesl-control -L --query`.

4. Убедиться в том, что на защищенных виртуальных машинах установлены обновления баз, необходимых для работы Легкого агента.

   Обновление баз на защищенных виртуальных машинах выполняется с помощью специальной задачи *Обновление*, в которой в качестве источника обновлений указана папка на SVM. Задача обновления запускается автоматически.

   Вы можете проверить актуальность баз на защищенной виртуальной машине с Легким агентом с помощью команды (см. раздел "Просмотр информации о приложении" на стр. 95) `kesl-control --app-info`.

   Также вы можете настроить задачи управления приложением с помощью Консоли администрирования или Web Console.

kaspersky

Активация приложения через Kaspersky Security Center

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, отдельно активировать приложение после установки не требуется. Вы активируете решение Kaspersky Security для виртуальных сред Легкий агент, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент).

Активация – это процедура введения в действие приложения в рамках лицензии, дающей право на использование полнофункциональной версии приложения в течение срока действия лицензии. Процедура активации приложения заключается в добавлении лицензионного ключа.

Вы можете активировать приложение дистанционно через Kaspersky Security Center следующими способами:

- С помощью задачи активации приложения.

  Этот способ позволяет добавить лицензионный ключ на конкретное устройство или устройства, входящие в группу администрирования. Вы можете создать и выполнить задачу активации через Консоль администрирования (см. раздел "Добавление ключа" на стр. 356) или через Kaspersky Security Center Web Console (см. раздел "Добавление ключа" на стр. 471).

- 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.

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

Активация в Kaspersky Security Center Web Console

Перед созданием задачи активации 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** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне выберите **Добавить файл ключа**, чтобы добавить ключ с помощью файла ключа.
4. Нажмите на кнопку **Выберите файл ключа** и в открывшемся окне выберите файл с расширением key.
5. Нажмите на кнопку **Закрыть**.

Добавленный ключ отобразится в списке ключей.

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

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите название приложения Kaspersky Endpoint Security.

   b. В раскрывающемся списке **Тип задачи** выберите **Добавление ключа**.

   c. В поле **Название задачи** введите короткое описание, например, `Активация Kaspersky Endpoint Security`.

   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 **Добавить файл ключа**, чтобы добавить ключ с помощью файла ключа.

   b. 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 **Закрыть**.

   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 по кнопке **Готово**.

   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.

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

1. В главном окне Web Console выберите **Операции** → **Лицензирование** → **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 ключей в инфраструктуре организации (**Мониторинг и отчеты** → **Отчеты**).
- Просмотреть статусы управляемых устройств (**Устройства** → **Управляемые устройства**). Если приложение не активировано, то для устройства будет отображаться статус  и описание статуса **Защита выключена**.
- Просмотреть свойства ключа (**Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**).

Запуск приложения в 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/digsig/digsig_initramfs.conf:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Установите пакет совместимости:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Создайте директорию для ключа приложения:

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

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

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/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/digsig/digsig_initramfs.conf:

   ```
   DIGSIG_LOAD_KEYS=1
   DIGSIG_ENFORCE=1
   ```

2. Создайте директорию для ключа приложения:

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

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

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/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.

Настройка разрешающих правил в системе SELinux

Если во время первоначальной настройки приложению Kaspersky Endpoint Security не удалось настроить систему SELinux автоматически (см. раздел "Включение автоматической настройки SELinux" на стр. 38) или вы отказались от автоматической настройки, вы можете вручную настроить систему SELinux для работы с приложением Kaspersky Endpoint Security.

► *Чтобы 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 policycoreutils-python или policycoreutils-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 следующих исходных исполняемых файлов приложения Kaspersky Endpoint Security в соответствии с используемой политикой SELinux:
   - /var/opt/kaspersky/kesl/12.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/libexec/kesl

- /var/opt/kaspersky/kesl/12.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/bin/kesl-control
- /var/opt/kaspersky/kesl/12.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/libexec/kesl-gui
- /var/opt/kaspersky/kesl/12.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/shared/kesl

4. Запустите следующие задачи:
   - задачу Защита от файловых угроз:

     ```
     kesl-control --start-task 1
     ```

   - задачу Проверка важных областей:

     ```
     kesl-control --start-task 4 -W
     ```

   Рекомендуется запустить все задачи, которые вы планируете запускать при использовании приложения Kaspersky Endpoint Security.
5. Запустите графический пользовательский интерфейс, если вы планируете его использовать.
6. Убедитесь, что в файле audit.log нет ошибок:

   ```
   grep kesl /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 Endpoint Security.

   В случае появления новых audit-сообщений, связанных с Kaspersky Endpoint Security, 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 Endpoint Security (выполните шаги 1, 3–8).

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

kaspersky

Удаление приложения

Вы можете удалить приложение Kaspersky Endpoint Security локально (см. раздел "Удаление приложения с помощью командной строки" на стр. 69) или через Kaspersky Security Center (см. раздел "Удаление приложения с помощью Консоли администрирования" на стр. 71) или Kaspersky Security Center Web Console (см. раздел "Удаление приложения с помощью Kaspersky Security Center Web Console" на стр. 71).

В процессе удаления приложения все задачи Kaspersky Endpoint Security будут остановлены.

Вы можете выполнить следующие действия при удалении приложения:

- одновременно удалить пакет приложения и пакет графического пользовательского интерфейса;
- удалить только пакет приложения, если пакет графического пользовательского интерфейса не установлен;

  Невозможно удалить только пакет приложения, если установлен пакет графического пользовательского интерфейса.

- удалить только пакет графического пользовательского интерфейса.

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

Удаление приложения с помощью командной строки

Приложение автоматически выполняет процедуру удаления. После завершения процедуры удаления приложение выводит сообщение о результатах удаления.

Удаление пакета приложения и пакета графического интерфейса

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

```
# rpm -e kesl kesl-gui
```

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

```
# apt-get purge kesl kesl-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 kesl
```

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

```
# apt-get purge kesl
```

Удаление пакета графического интерфейса

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

```
# rpm -e kesl-gui
```

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

```
# apt-get purge kesl-gui
```

Удаление Агента администрирования

- *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
```

kaspersky

Удаление приложения с помощью Консоли администрирования

Вы можете удалить приложение Kaspersky Endpoint Security через Консоль администрирования Kaspersky Security Center. Для этого вам нужно создать и запустить в Kaspersky Security Center задачу удаленной деинсталляции программы.

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. 57) и запустить задачу удаленной установки приложений.

Подробнее о создании и запуске задач удаленной деинсталляции и удаленной установки приложений см. в справке Kaspersky Security Center.

Удаление приложения с помощью Kaspersky Security Center Web Console

Вы можете удалить приложение дистанционно через Kaspersky Security Center Web Console с помощью задачи удаленной деинсталляция программы. При выполнении задачи приложение Kaspersky Endpoint Security загрузит на устройство пользователя утилиту для удаления приложения. После завершения удаления приложения, утилита будет автоматически удалена.

► *Чтобы удалить приложение:*

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Следуйте указаниям мастера создания задачи.

Шаг 1. Настройка основных параметров задачи

На этом шаге настройте основные параметры задачи:

1. В раскрывающемся списке **Программа** выберите **Kaspersky Security Center <номер версии>**.
2. В раскрывающемся списке **Тип задачи** выберите **Удаленная деинсталляция программы**.
3. В поле **Название задачи** введите короткое описание, например, `Удаление Kaspersky Endpoint Security на устройствах Службы технической поддержки`.
4. В разделе **Выбор устройств, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Выбор устройств для удаления приложения

На этом шаге выберите устройства, на которых будет удалено приложение Kaspersky Endpoint Security, в соответствии с выбранным вариантом области действия задачи.

Шаг 3. Настройка параметров удаления приложения

На этом шаге настройте параметры удаления приложения:

1. Выберите **Удалить управляемую программу**.
2. В раскрывающемся списке **Программа для деинсталляции** выберите инсталляционный пакет приложения Kaspersky Endpoint Security.
3. В разделе **Принудительно загрузить утилиту деинсталляции** выберите способ доставки утилиты:
   - **С помощью Агента администрирования**. Если на клиентском устройстве не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее приложение Kaspersky Endpoint Security будет удалено средствами Агента администрирования.
   - **Средствами операционной системы с помощью Сервера администрирования**. Доставка утилиты на клиентские устройства будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.
   - **Средствами операционной системы с помощью точек распространения**. Утилита передается на клиентские устройства средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о точках распространения см. в документации Kaspersky Security Center.
4. В поле **Максимальное количество одновременных загрузок** установите ограничение количества запросов к Серверу администрирования для загрузки утилиты для удаления приложения. Ограничение запросов позволит избежать перегрузки сети.
5. В поле **Максимальное количество попыток деинсталляции** установите ограничение количества попыток удалить приложение. Если удаление приложения завершается с ошибкой, задача автоматически запускает удаление повторно.
6. Если требуется, снимите флажок **Предварительно поверять тип операционной системы перед загрузкой**. Это позволит избежать загрузки утилиты деинсталляции, если операционная система клиентского устройства не соответствует программным требованиям. Если вы уверены, что операционная система устройства соответствует программным требованиям, проверку можно пропустить.

Шаг 4. Выбор действия приложения при необходимости перезагрузки операционной системы

На этом шаге вы можете выбрать действие, которое будет выполнять приложение, если в ходе удаления потребуется перезагрузка операционной системы.

Шаг 5. Выбор учетной записи для доступа к клиентским устройствам

На этом шаге выберите учетную запись для удаления приложения средствами операционной системы. В этом случае для доступа к клиентскому устройству требуются права администратора. Вы можете добавить несколько учетных записей. Если у одной учетной записи нет необходимых прав, мастер удаления будет использовать следующую учетную запись. Для удаления приложения Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 6. Завершение создания задачи

Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача.

Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**. Удаление приложения будет выполнено в фоновом режиме. После завершения удаления приложения отобразится запрос на перезагрузку клиентского устройства.

kaspersky

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

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

- Приложение активировано: добавлен лицензионный ключ.
- Обновлены базы приложения.
- KSN выключен или используется KPSN.
- Настроена и запущена задача Защита от файловых угроз (см. раздел "Задача Защита от файловых угроз (File_Threat_Protection, ID:1)" на стр. 133).
- Параметры приложения находятся в рамках допустимых значений, приведенных в Приложении 4 (см. раздел "Приложение 4. Значения параметров приложения в сертифицированной конфигурации" на стр. 542) 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 4 (см. раздел "Приложение 4. Значения параметров приложения в сертифицированной конфигурации" на стр. 542) к этому документу.
2. Убедитесь, что приложение активировано и базы приложения обновлены, выполнив следующую команду:

   ```
   kesl-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:

   ```
   kesl-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:

   ```
   kesl-control --stop-task 1
   ```

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

   ```
   kesl-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:

   ```
   kesl-control --start-task 1
   ```

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

   ```
   kesl-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:

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

kaspersky

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Endpoint Security.

В этом разделе

О Лицензионном соглашении

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

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки приложения Kaspersky Endpoint Security (см. раздел "Установка приложения" на стр. 29).
- Прочитав текст файла license.<ID языка>. Этот файл включен в комплект поставки приложения.

Вы принимаете условия Лицензионного соглашения (см. раздел "Принятие Лицензионного соглашения" на стр. 36), подтверждая свое согласие с текстом Лицензионного соглашения во время первоначальной настройки приложения (см. раздел "Первоначальная настройка приложения" на стр. 33). Если вы не согласны с условиями Лицензионного соглашения, вы не должны использовать приложение.

О лицензии

Лицензия – это ограниченное по времени право на использование приложения Kaspersky Endpoint Security, 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 Endpoint Security 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 Endpoint Security 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*. Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

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 конфигурациии. 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.

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 или коммерческой лицензии. В приложении не может быть больше одного активного лицензионного ключа.

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.

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

kaspersky

Предоставление данных

Этот раздел содержит информацию о данных, которые приложение Kaspersky Endpoint Security может сохранять на устройстве и передавать 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. 76), Положении о Kaspersky Security Network (см. раздел "Использование Kaspersky Security Network" на стр. 260) и Политике конфиденциальности на веб-сайте "Лаборатории Касперского" https://www.kaspersky.ru/products-and-services-privacy-policy. Файлы license.<ID языка> и ksn_license.<ID 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"

Если приложение Kaspersky Endpoint Security используется в автономной режиме и 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.

kaspersky

Данные, передаваемые при использовании приложения в режиме Легкого агента

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред в составе решения Kaspersky Security для виртуальных сред Легкий агент, во время работы приложение сохраняет и передает другим компонентам решения следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Для активации Kaspersky Endpoint Security передает Серверу защиты следующие данные: тип ОС защищенной виртуальной машины, срок действия тикета; время запроса тикета (в формате UTC); идентификатор (BIOS ID) защищенной виртуальной машины.
- Для обновления баз Легкого агента Kaspersky Endpoint Security передает Серверу защиты следующие данные: идентификатор ПО, полученный из лицензии; полную версию ПО; идентификатор лицензии ПО; идентификатор установки ПО (PCID); обрабатываемый веб-адрес; тип установленной лицензии; идентификатор запуска обновления.
- Для обеспечения защиты и в ходе выполнения задач проверки Kaspersky Endpoint Security передает Серверу защиты информацию, необходимую для выполнения проверки объектов. В том числе могут передаваться имена файлов и пути к ним в файловой системе, хеши файлов, веб-адреса, а также проверяемые объекты или их фрагменты.
- В инфраструктуре под управлением VMware vCenter Server и VMware NSX Manager Kaspersky Endpoint Security может передавать Серверу интеграции информацию о тегах безопасности (Security Tags), которые назначаются защищенной виртуальной машине при обнаружении вирусов, вредоносных программ и активности, характерной для сетевых атак. В том числе передаются идентификаторы защищенных виртуальных машин.
- Для получения информации, которая используется при выборе SVM для подключения, Kaspersky Endpoint Security передает идентификатор защищенной виртуальной машины Серверу интеграции и Серверу защиты.
- При использовании решения Kaspersky Security для виртуальных сред Легкий агент в режиме мультитенантности информация, необходимая для формирования отчетов о защите тенантов, может передаваться от Kaspersky Endpoint Security Серверу защиты. В том числе могут передаваться: идентификатор защищенной виртуальной машины; тип и версия гостевой операционной системы на защищенной виртуальной машине; периоды времени, когда приложение Kaspersky Endpoint Security было подключено к SVM.
- Для получения статистики Kaspersky Endpoint Security передает Серверу защиты следующую информацию: информацию о версии ОС защищенной виртуальной машины; локализацию приложения Kaspersky Endpoint Security; названия активных компонентов приложения Kaspersky Endpoint Security; идентификатор (BIOS ID) защищенной виртуальной машины.

Указанная информация, кроме информации, необходимой для выполнения проверки объектов, и информации, которая используется при выборе SVM, передается по зашифрованным каналам передачи данных. Соединение между Kaspersky Endpoint Security и Серверами защиты по умолчанию не защищено. Вы можете включить шифрование канала передачи данных между Легкими агентами и Серверами защиты в параметрах приложения Kaspersky Endpoint Security.

Данные, передаваемые приложению Kaspersky Security Center

Во время работы приложение Kaspersky Endpoint Security 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;
  - дополнительную информацию в случае использования приложения по подписке (признак подписки, дату истечения периода подписки и количество дней, доступных для продления подписки, веб-адрес провайдера подписки, текущий статус и причину перехода в этот статус), дату и время активации приложения на устройстве;
  - 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 приложения;
  - веб-адрес для загрузки плагина управления приложения;
  - 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.
- 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, класс, производитель, описание, серийный номер и VID/PID).
- Информацию о резервных копиях файлов, помещенных в 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 Хранилище, действия над объектом в 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 и метод 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 состояния 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 SHA-256);
- информацию о внешних системах, входящих в состав корпоративных программных решений (адрес сервера интеграции);
- информацию о включении и выключении сетевой изоляции для устройства;
- информацию о работе в режиме Легкого агента: имя шаблона виртуальной машины, адрес Сервера интеграции.
- имя устройства, для которого включена или выключена сетевая изоляция.

- 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, обнаруженных на клиентском устройстве (имя, путь, тип и хеш файла; список категорий, к которым отнесено приложение; группу доверия, к которой отнесено

приложение; первое время запуска файла; имя 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; имя группы HIPS, имя группы KSN).

Данные, предоставляемые при переходе по ссылкам из интерфейса приложения

При переходе по ссылкам из интерфейса приложения Kaspersky Endpoint Security вы соглашаетесь предоставлять 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 (см. раздел "Использование Kaspersky Security Network" на стр. 260). 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, предоставляемые при использовании решения Kaspersky Anti Targeted Attack Platform

При интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Anti Targeted Attack Platform приложение Kaspersky Endpoint Security сохраняет и может передавать приложению Kaspersky Security Center следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Служебные данные:
  - адреса серверов KATA;
  - открытый ключ сертификата сервера для интеграции с компонентом EDR (KATA);
  - криптоконтейнер с сертификатом клиента для интеграции с компонентом EDR (KATA);
  - учетные данные для авторизации на прокси-сервере;
  - параметры частоты синхронизации с сервером KATA и параметры передачи данных на сервер KATA;

- статус соединения с сервером KATA и сведения об ошибках сертификата клиента и сертификата сервера.

При интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Anti Targeted Attack Platform приложение Kaspersky Endpoint Security сохраняет и может передавать серверу KATA следующие данные:

- Данные из запросов на синхронизацию к компоненту EDR (KATA):
  - Уникальный идентификатор.
  - Базовую часть веб-адреса сервера.
  - Имя устройства.
  - IP-адрес устройства.
  - MAC-адрес устройства.
  - Локальное время на устройстве.
  - Название и версию операционной системы, установленной на устройстве.
  - Версию Kaspersky Endpoint Security.
  - Версии параметров приложения и параметров задач.
  - Состояние задач (идентификаторы задач, статусы выполнения, коды ошибок).
- Данные из запросов к компоненту EDR (KATA) в отчетах о результатах выполнения задач:
  - IP-адрес устройства.
  - Ошибки выполнения задач и коды возврата.
  - Статусы, с которыми завершались задачи.
  - Время завершения выполнения задач.
  - Версии параметров, с которыми выполнялись задачи.
  - Информацию о процессах, запущенных или остановленных на устройстве по запросу сервера: PID и UniquePID, код ошибки, хеш-суммы MD5 и SHA-256 объектов.
  - Файлы, запрошенные сервером.
  - Пакеты телеметрии.
  - Данные о запущенных процессах:
    - имя исполняемого файла, включая полный путь и расширение;
    - параметры запуска процесса;
    - идентификатор процесса;
    - код сеанса входа в систему;
    - имя сеанса входа в систему;
    - дата и время запуска процесса;
    - хеш-суммы MD5 и SHA-256 объекта.
  - Данные о файлах:
    - Путь к файлу.
    - Имя файла.

        - Размер файла.
        - Атрибуты файла.
        - Дата и время создания файла.
        - Дата и время последнего изменения файла.
        - хеш-суммы MD5 и SHA-256 объекта.
    - Данные в ошибках получения информации об объектах:
        - Полное имя объекта, при обработке которого возникла ошибка.
        - Код ошибки.
- Данные из запросов от сервера KATA к встроенному агенту Kaspersky Endpoint Security (параметры задач):
    - Типы задач.
    - Параметры расписания запуска задач.
    - Имена и пароли учетных записей, от имени которых требуется запускать задачи.
    - Версии параметров.
    - Пути к объектам.
    - Хеш-суммы MD5 и SHA-256 объектов.
    - Командную строку запуска процесса с аргументами.
    - Наименование служб.
    - Тип запуска служб.
- Параметры ответных запросов (response), которые сервер KATA отправляет встроенному агенту Kaspersky Endpoint Security:
    - Задача Получить файл (Get file task):
        - Полный путь к файлу или директории.
        - Алгоритм расчет хеша. Возможные значения: MD5 и/или SHA-256.
        - Хеш-суммы MD5 и SHA-256 файла.
    - Задача Удалить файл (Delete file task):
        - подтверждение удаления или произошедшая ошибка.
    - Задача Запустить процесс (Run process):
        - Полный путь к исполняемому файлу, из которого запущен процесс.
        - Командную строку процесса.
        - Полный путь к рабочей директории процесса.
    - Задача Завершить процесс (Terminate process):
        - Уникальный PID процесса.
        - Системный PID процесса.
        - Код ошибки завершения процесса (0, если процесс успешно завершен).
    - Задача Поиск IOC (IOC Scan task):

- Результаты поиска (сработал или не сработал каждый индикатор, найденные объекты и информация о том, какая ветка индикатора сработала).

  Для объектов, вызвавших срабатывания, возвращаются разные значения в зависимости от типа:

  - ArpEntry: IP-адрес из ARP-таблицы (в том числе ipv6), физический адрес из ARP-таблицы.
  - File: MD5-хеш файла, SHA-256-хеш файла, полное имя файла (включая путь), размер файла.
  - Port: удаленный IP-адрес и порт, с которым в момент проверки, установлено соединение; IP-адрес и порт локального адаптера; тип протокола (TCP, UDP, IP, RAWIP).
  - Process: имя процесса; аргументы процесса; путь к файлу процесса; системный PID процесса; системный PID родительского процесса; имя пользователя, от которого запущен процесс; дата и время запуска процесса.
  - SystemInfo: имя ОС, версия ОС, сетевое имя компьютера без домена, домен или рабочая группа.
  - User: имя пользователя

- Сетевая изоляция:
  - Статус применения сетевой изоляции.

kaspersky

Разделение доступа к функциям приложения по пользовательским ролям

Доступ к функциям приложения Kaspersky Endpoint Security предоставляется пользователю в соответствии с его ролью. *Роль* – это набор прав и разрешений на управление приложением.

В операционной системе создаются четыре группы пользователей системы: *kesladmin*, *kesluser*, *keslaudit* и *nokesl*. Когда роль в приложении назначается пользователю (см. раздел "Назначение роли пользователю" на стр. 89) 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. 89) 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:

- kesladmin соответствует роли Администратор;
- kesluser соответствует роли Пользователь;
- keslaudit соответствует роли Аудитор;
- nokesl назначается пользователю, если не назначена ни одна из ролей. В этом случае пользователь относится к отдельной группе *пользователи без прав*.

В таблице ниже описаны роли в приложении и их права.

Таблица 5. Роли пользователей

Название роли	Роль в приложении	Пользователь ОС	Права
Администратор	admin	kesladmin	Управление параметрами всех приложений и 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	kesluser	Управление только задачами Scan_File. Запуск и остановка задач обновления. Просмотр отчетов для созданных пользователем задач. Просмотр особых событий, общих для всех пользователей приложения.

Название роли	Роль в приложении	Пользователь ОС	Права
Аудитор	audit	keslaudit	Просмотр параметров приложения. Просмотр статуса приложения. Просмотр всех задач, их параметров и расписания запуска. Просмотр всех событий. Просмотр всех объектов в Хранилище.
—	—	nokesl	Роль в приложении не назначена, права отсутствуют.

В этом разделе

Просмотр списка пользователей и ролей

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

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

Назначение роли пользователю

► *Чтобы назначить роль определенному пользователю, выполните следующую команду:*

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

Пример:

Назначить роль audit пользователю test15:

```
kesl-control --grant-role audit test15
```

Отзыв роли у пользователя

► *Чтобы отозвать роль у определенного пользователя, выполните следующую команду:*

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

Пример:

Отозвать роль audit у пользователя test15:

```
kesl-control --revoke-role audit test15
```

kaspersky

Интерфейсы управления приложением

Вы можете управлять приложением Kaspersky Endpoint Security следующими способами:

- С помощью команд управления из командной строки (см. раздел "Управление приложением с помощью командной строки" на стр. 92).
- С помощью Консоли администрирования Kaspersky Security Center (см. раздел "Управление приложением с помощью Консоли администрирования" на стр. 271).
- С помощью Kaspersky Security Center Web Console (см. раздел "Управление приложением с помощью Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console" на стр. 390).
- С помощью графического пользовательского интерфейса (см. раздел "Управление приложением с помощью графического пользовательского интерфейса" на стр. 500).

> Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, недоступно управление приложением с помощью Kaspersky Security Center Cloud Console и графического пользовательского интерфейса.

kaspersky

Управление приложением с помощью командной строки

Вы можете управлять приложением Kaspersky Endpoint Security с помощью командной строки. Из командной строки доступны все действия, включая управление задачами (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118) и настройку параметров приложения.

В этом разделе

Запуск и остановка приложения

По умолчанию приложение Kaspersky Endpoint Security запускается автоматически при запуске операционной системы (на уровнях выполнения по умолчанию, принятых для каждой операционной системы). Приложение запускает все служебные задачи, а также пользовательские задачи, в параметрах расписания которых задан режим запуска `PS`.

Если вы остановите приложение, все выполняющиеся задачи будут прерваны. После повторного запуска приложения прерванные пользовательские задачи автоматически не возобновляются. Будут запущены снова только те пользовательские задачи, в параметрах расписания которых задан режим запуска `PS`.

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 Endpoint Security

- *Чтобы запустить приложение в systemd-системе, выполните следующую команду:*

  ```
  systemctl start kesl
  ```

- *Чтобы остановить приложение в systemd-системе, выполните следующую команду:*

  ```
  systemctl stop kesl
  ```

- *Чтобы перезапустить приложение в systemd-системе, выполните следующую команду:*

  ```
  systemctl restart kesl
  ```

- *Чтобы запустить приложение в системе без systemd, выполните следующую команду:*

  ```
  /etc/init.d/kesl start
  ```

- *Чтобы остановить приложение в системе без systemd, выполните следующую команду:*

  ```
  /etc/init.d/kesl stop
  ```

- *Чтобы перезапустить приложение в системе без systemd, выполните следующую команду:*

  ```
  /etc/init.d/kesl restart
  ```

Мониторинг статуса приложения Kaspersky Endpoint Security

Мониторинг статуса приложения Kaspersky Endpoint Security выполняется с помощью контрольной службы. Контрольная служба автоматически запускается при запуске приложения.

В случае сбоя приложения создается файл дампа, и приложение автоматически перезапускается.

- *Чтобы вывести статус приложения в systemd-системе, выполните следующую команду:*

  ```
  systemctl status kesl
  ```

- *Чтобы вывести статус приложения в системе без systemd, выполните следующую команду:*

  ```
  /etc/init.d/kesl status
  ```

Вывод справки о командах

Команда `kesl-control --help <набор команд приложения>` возвращает справку по командам приложения.

Синтаксис команды

```
kesl-control --help [<набор команд приложения>]
```

<набор команд приложения>

Доступные значения:

`-T` – команды управления задачами (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118) и общими параметрами приложения (см. раздел "Изменение общих параметров приложения" на стр. 113).

`-C` – команды управления общими параметрами проверки контейнеров (см. раздел "Изменение общих параметров проверки контейнеров" на стр. 116).

`-N` – команды управления параметрами проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 129).

`-L` – команды управления лицензионными ключами (см. раздел "Задача Лицензирование (License, ID:9)" на стр. 177) и интеграцией приложения Kaspersky Endpoint Security с Kaspersky Managed Detection and Response.

`-E` – команды управления событиями приложения (см. раздел "Просмотр событий" на стр. 267).

`-B` – команды управления задачей Управление Хранилищем (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 179).

`-F` – команды управления задачей Управление сетевым экраном.

`-H` – команды управления задачей Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 200).

`-D` – команды управления задачей Контроль устройств (см. раздел "Задача Контроль устройств (Device_Control, ID:15)" на стр. 209).

`-A` – команды управления задачей Контроль приложений (см. раздел "Задача Контроль приложений (Application_Control, ID:21)" на стр. 243).

`-U` – команды управления пользователями и ролями пользователей (см. раздел "Разделение доступа к функциям приложения по пользовательским ролям" на стр. 88).

`-S` – команды статистики (см. раздел "Просмотр информации о приложении" на стр. 95).

`-W` – вывод событий (см. раздел "Включение вывода событий" на стр. 95).

`-R` – команды управления параметрами интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA).

`-V` – команды приложения в режиме Легкого агента (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23) для защиты виртуальных сред.

Включение автоматического дополнения команды kesl-control (bash completion)

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

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

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

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

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

Включение вывода событий

Команда `kesl-control -W` включает вывод текущих событий приложения. Команда возвращает название события и дополнительную информацию о событии.

Эту команду можно использовать либо отдельно для вывода всех текущих событий приложения, либо совместно с командой `kesl-control --start-task` для вывода событий, связанных только с запущенной задачей.

Кроме того, вы можете использовать команду `kesl-control -W` с флагом `--query`, чтобы указать условия фильтра (см. раздел "Использование фильтра для ограничения результатов запроса" на стр. 103) для вывода определенных событий.

Синтаксис команды

```
kesl-control -W
```

Примеры:

Включить режим вывода текущих событий приложения:

```
kesl-control -W
```

Включить вывод текущих событий задачи с ID=1:

```
kesl-control --start-task 1 -W
```

Включить вывод текущих событий TaskStateChanged:

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

Просмотр информации о приложении

Команда `kesl-control --app-info` выводит информацию о приложении.

Синтаксис команды

```
kesl-control [-S] --app-info [--json]
```

Результат выполнения команды:

- **Название**. Название приложения.
- **Версия**. Текущая версия приложения.
- **Политика**. Отображается, применяется ли политика Kaspersky Security Center.
- **Информация о лицензии**. Информация о лицензии или статус лицензионного ключа.

- **Статус подписки**. Статус подписки. Это поле отображается, если приложение используется по подписке.
- **Дата окончания срока действия лицензии**. Дата и время окончания срока действия лицензии (см. раздел "О лицензии" на стр. 76) в формате UTC.
- **Статус файла MDR BLOB**. Статус конфигурационного файла BLOB для интеграции с 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 Хранилища**. Состояние Хранилища (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 179).
- **Использование Хранилища**. Размер Хранилища (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 179).
- **Дата последнего запуска задачи Scan_My_Computer**. Время последнего запуска задачи Поиск вредоносного ПО (см. раздел "Задача Поиск вредоносного ПО (Scan_My_Computer, ID:2)" на стр. 148).
- **Дата последнего выпуска баз приложения**. Время последнего выпуска баз приложения (см. раздел "Задача Обновление (Update, ID:6)" на стр. 172).
- **Базы приложения загружены**. Отображается, загружены ли базы приложения (см. раздел "Задача Обновление (Update, ID:6)" на стр. 172).
- **Использование Kaspersky Security Network**. Информация об использовании Kaspersky Security Network (см. раздел "Использование Kaspersky Security Network" на стр. 260): `Расширенный режим KSN`, `Стандартный режим KSN` или `Выключен`.
- **Инфраструктура Kaspersky Security Network**. Информация об инфраструктурном решении (см. раздел "Использование Kaspersky Security Network" на стр. 260), которое используется для работы с репутационными базами "Лаборатории Касперского": `Kaspersky Security Network` или `Kaspersky Private Security Network`.
- **Состояние Managed Detection and Response**. Состояние Managed Detection and Response: `активный`, `неактивный`.
- **Защита от файловых угроз**. Состояние задачи Защита от файловых угроз (см. раздел "Задача Защита от файловых угроз (File_Threat_Protection, ID:1)" на стр. 133).
- **Мониторинг контейнеров**. Отображается информация о параметрах проверки контейнеров (см. раздел "Описание общих параметров проверки контейнеров" на стр. 114).
- **Контроль целостности системы**. Состояние задачи Контроль целостности системы (см. раздел "Задача Контроль целостности системы (System_Integrity_Monitoring, ID:11)" на стр. 182).
- **Управление сетевым экраном**. Состояние задачи Управление сетевым экраном.
- **Защита от шифрования**. Состояние задачи Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 200).
- **Защита от веб-угроз**. Состояние задачи Защита от веб-угроз (см. раздел "Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)" на стр. 206).
- **Контроль устройств**. Состояние задачи Контроль устройств (см. раздел "Параметры задачи Контроль устройств" на стр. 211).
- **Проверка съемных дисков**. Состояние задачи Проверка съемных дисков (см. раздел "Задача Проверка съемных дисков (Removable_Drives_Scan, ID:16)" на стр. 220).

- **Защита от сетевых угроз**. Состояние задачи Защита от сетевых угроз (см. раздел "Задача Защита от сетевых угроз (Network_Threat_Protection, ID:17)" на стр. 222).
- **Анализ поведения**. Состояние задачи Анализ поведения (см. раздел "Задача Анализ поведения (Behavior_Detection, ID:20)" на стр. 242).
- **Контроль приложений**. Состояние задачи Контроль приложений (см. раздел "Задача Контроль приложений (Application_Control, ID:21)" на стр. 243).
- **Интеграция с Endpoint Detection and Response (KATA)**. Состояние задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA).
- **Состояние обновления для приложения**. Отображаются действия по обновлению приложения и действия, которые требуется выполнить пользователю.
- **Приложение работает нестабильно**. Отображается информация о сбое в работе приложения и создании файла дампа. Это поле отображается, если при предыдущем запуске приложения произошел сбой.

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.

Описание команд приложения

Вывод справки о командах приложения

--help – выводит справку о командах приложения (см. раздел "Вывод справки о командах" на стр. 93).

Вывод событий приложения

-W – включает вывод событий приложения (см. раздел "Включение вывода событий" на стр. 95).

Команды статистики

-S – префикс указывающий, что команда принадлежит к группе команд статистики.

[-S] --app-info – выводит информацию о приложении (см. раздел "Просмотр информации о приложении" на стр. 95).

[-S] --omsinfo --file <имя и путь к файлу> – создает файл в формате JSON для интеграции с Microsoft Operations Management Suite.

Команды управления параметрами и задачами приложения

-T – префикс, указывающий, что команда принадлежит к группе команд управления параметрами / задачами приложения.

[-T] --get-app-settings --file <имя и путь к файлу> – выводит общие параметры приложения (см. раздел "Изменение общих параметров приложения" на стр. 113).

[-T] --set-app-settings --file <имя и путь к файлу> – устанавливает общие параметры приложения (см. раздел "Изменение общих параметров приложения" на стр. 113).

[-T] --set-app-settings <параметр>=<значение параметра> – устанавливает значение для указанного общего параметра приложения (см. раздел "Описание общих параметров приложения" на стр. 106).

[-T] --export-settings --file <полный путь к конфигурационному файлу> – экспортирует параметры приложения в конфигурационный файл.

[-T] --import-settings --file <полный путь к конфигурационному файлу> – импортирует параметры приложения из конфигурационного файла.

[-T] --update-application – обновляет приложение.

[-T] --get-task-list – выводит список существующих задач приложения (см. раздел "Просмотр списка задач" на стр. 120).

[-T] --get-task-state <ID задачи>|<название задачи> – выводит состояние указанной задачи.

[-T] --create-task <название задачи> --type <тип задачи> --file <имя и путь к файлу> – создает задачу (см. раздел "Создание задачи" на стр. 121) указанного типа, импортирует в задачу параметры из указанного конфигурационного файла.

[-T] --delete-task <ID задачи>|<название задачи> – удаляет задачу (см. раздел "Удаление задачи" на стр. 129).

[-T] --start-task <ID задачи>|<название задачи> [-W] [--progress] – запускает задачу (см. раздел "Запуск и остановка задачи" на стр. 123).

[-T] --stop-task <ID задачи>|<название задачи> – останавливает задачу (см. раздел "Запуск и остановка задачи" на стр. 123).

[-T] --suspend-task <ID задачи>|<название задачи> – приостанавливает задачу. Приостановить задачу обновления невозможно.

[-T] --resume-task <ID задачи>|<название задачи> – возобновляет задачу. Возобновить задачу обновления невозможно.

[-T] --scan-file <путь к файлу или директории> [--action <действие>] – создает и запускает временную задачу Выборочная проверка (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 156) (Scan_File), которой присваивается новый идентификатор. Секции `[ScanScope.item_#]` и `[ExcludedFromScanScope.item_#]` в параметрах этой задачи не наследуются из исходной задачи с ID=3. Если параметр `--action <действие>` не указан, выполняется действие `Recommended`. После завершения проверки временная задача автоматически удаляется.

[-T] --scan-container <контейнер|образ[:тег]> – создает временную задачу Выборочная проверка контейнеров (см. раздел "Задача Выборочная проверка контейнеров (Custom_Container_Scan, ID:19)" на стр. 234) (Custom_Container_Scan). После завершения проверки временная задача автоматически удаляется.

[-T] --get-settings <ID задачи>|<название задачи> --file <имя и директория файла> – выводит параметры задачи.

[-T] --set-settings <ID задачи>|<название задачи> [<параметры>] [--file <имя и директория файла>] [--add-path <путь>] [--del-path <путь>] [--add-exclusion <исключение>] [--del-exclusion <исключение>] – устанавливает параметры задачи.

[-T] --set-settings [<ID задачи>|<название задачи>] set-to-default – восстанавливает значения по умолчанию (см. раздел "Восстановление заданных по умолчанию параметров задачи" на стр. 123) для параметров задачи.

[-T] --set-schedule <ID задачи>|<название задачи> --file <имя и путь к файлу> – устанавливает параметры расписания задачи или импортирует их в задачу из конфигурационного файла.

[-T] --get-schedule <ID задачи>|<название задачи> --file <имя и путь к файлу> – выводит параметры расписания задачи или сохраняет их в конфигурационный файл.

Команды управления параметрами проверки контейнеров

-C – префикс, указывающий, что команда принадлежит к группе команд управления параметрами проверки контейнеров.

[-C] --get-container-settings --file <имя и путь к файлу> – выводит общие параметры проверки контейнеров (см. раздел "Изменение общих параметров проверки контейнеров" на стр. 116).

[-C] --set-container-settings --file <имя и путь к файлу> – устанавливает общие параметры проверки контейнеров (см. раздел "Изменение общих параметров проверки контейнеров" на стр. 116).

Команды управления параметрами проверки зашифрованных соединений

-N – префикс, указывающий, что команда принадлежит к группе команд управления параметрами проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 129).

-N --query user – выводит список исключений из проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 129), добавленных пользователем.

-N --query auto – выводит список исключений из проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 129), добавленных приложением.

-N --query kl – выводит список исключений из проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 129), полученных из баз "Лаборатории Касперского".

-N --clear-web-auto-excluded – очищает список доменов, которые приложение автоматически исключило из проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 129).

[-N] --get-net-settings [--file <имя и путь к файлу>] – выводит параметры проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 129) в файл формата INI.

[-N] --set-net-settings [--file <имя и путь к файлу>] – устанавливает параметры проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 129).

[-N] --add-certificate <путь к файлу сертификата> – добавляет сертификат в список доверенных сертификатов (см. раздел "Управление доверенными сертификатами" на стр. 132).

[-N] --remove-certificate <субъект сертификата> – удаляет сертификат из списка доверенных сертификатов (см. раздел "Управление доверенными сертификатами" на стр. 132).

[-N] --list-certificates – выводит список доверенных сертификатов (см. раздел "Управление доверенными сертификатами" на стр. 132).

Команды управления пользователями и ролями

-U – префикс, указывающий, что команда принадлежит к группе команд управления пользователями и ролями.

[-U] --get-user-list – выводит список пользователей и ролей (см. раздел "Просмотр списка пользователей и ролей" на стр. 89).

[-U] --grant-role <роль> <пользователь> – присваивает роль (см. раздел "Назначение роли пользователю" на стр. 89) определенному пользователю.

[-U] --revoke-role <роль> <пользователь> – отзывает роль (см. раздел "Отзыв роли у пользователя" на стр. 89) у определенного пользователя.

Команды лицензирования

-L – префикс, указывающий, что команда принадлежит к группе команд управления лицензионными ключами.

[-L] --add-active-key <код активации>|<файл ключа> – добавляет активный ключ.

[-L] --add-reserve-key <код активации>|<файл ключа> – добавляет резервный ключ.

[-L] --remove-active-key – удаляет активный ключ.

[-L] --remove-reserve-key – удаляет резервный ключ.

-L --query – выводит информацию о лицензионном ключе.

> Команды добавления и удаления лицензионных ключей могут быть выполнены, только если приложение используется в автономном режиме (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23). В режиме Легкого агента для защиты виртуальных сред эти команды завершаются с ошибкой.

Команды управления задачей Управление сетевым экраном

-F – префикс, указывающий, что команда принадлежит к группе команд управления задачей Управление сетевым экраном.

[-F] --add-rule [--name <строка>] [--action <действие>] [--protocol <протокол>] [--direction <директория>] [--remote <удаленная>] [--local <локальная>] [--at <индекс>] – добавляет новое правило (см. раздел "Добавление сетевого пакетного правила" на стр. 197).

[-F] --del-rule [--name <строка>] [--index <индекс>] – удаляет правило (см. раздел "Удаление сетевого пакетного правила" на стр. 198).

[-F] --move-rule [--name <строка>] [--index <индекс>] [--at <индекс>] – изменяет приоритет выполнения правила (см. раздел "Изменение приоритета выполнения сетевого пакетного правила" на стр. 198).

[-F] --add-zone [--zone <зона>] [--address <адрес>] – добавляет в зону IP-адрес (см. раздел "Добавление сетевого адреса в секцию зоны" на стр. 199).

[-F] --del-zone [--zone <зона>] [--address <адрес>] [--index <индекс>] – удаляет из зоны IP-адрес (см. раздел "Удаление сетевого адреса из секции зоны" на стр. 199).

-F --query – выводит информацию о задаче.

Команды управления задачей Защита от шифрования

-H –префикс, указывающий, что команда принадлежит к группе команд управления задачей Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 200).

[-H] --get-blocked-hosts – отображает список заблокированных устройств (см. раздел "Просмотр списка заблокированных устройств" на стр. 204).

[-H] --allow-hosts – разблокирует недоверенные устройства (см. раздел "Разблокировка заблокированных устройств" на стр. 205).

Команды управления задачей Контроль устройств

-D – префикс, указывающий, что команда принадлежит к группе команд Контроля устройств (см. раздел "Задача Контроль устройств (Device_Control, ID:15)" на стр. 209).

[-D] --get-device-list – отображает список устройств, подключенных к клиентскому устройству (см. раздел "Просмотр списка подключенных устройств" на стр. 219).

Команды управления задачей Контроль приложений

-A – префикс, указывающий, что команда принадлежит к группе команд Контроля приложений (см. раздел "Задача Контроль приложений (Application_Control, ID:21)" на стр. 243).

[-A] --get-app-list – отображает список приложений (см. раздел "Просмотр списка обнаруженных приложений" на стр. 253), обнаруженных на клиентском устройстве во время выполнения задачи Инвентаризация (см. раздел "Задача Инвентаризация (Inventory_Scan, ID:22)" на стр. 251).

[-A] --get-categories – отображает список созданных категорий (см. раздел "Просмотр списка созданных категорий" на стр. 249) Контроля приложений.

Команды управления Хранилищем

-B – префикс, указывающий, что команда принадлежит к группе команд управления Хранилищем (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 179).

[-B] --mass-remove --query – очищает Хранилище (см. раздел "Удаление объектов из Хранилища" на стр. 181), полностью или выборочно.

-B --query <фильтр> – выводит информацию об объектах в Хранилище, соответствующих условиям фильтра (см. раздел "Использование фильтра для ограничения результатов запроса" на стр. 103).

[-B] --restore <ID объекта> --file <имя и путь к файлу> – восстанавливает объект (см. раздел "Восстановление объектов из Хранилища" на стр. 180) из Хранилища.

Команды управления журналом событий

-E – префикс, указывающий, что команда принадлежит к группе команд управления журналом событий (см. раздел "Просмотр событий" на стр. 267).

-E --query <фильтр> --db <файл базы данных> -n <количество> --file <имя и путь к файлу> [--json] – выводит информацию о событиях, соответствующих условиям фильтра (см. раздел "Использование фильтра для ограничения результатов запроса" на стр. 103), из базы данных журнала событий в указанный файл, где:

<количество> – количество последних событий из выборки (то есть количество записей от конца выборки), которые нужно вывести;

<фильтр> – условия фильтра для ограничения результатов запроса (см. раздел "Использование фильтра для ограничения результатов запроса" на стр. 103);

<имя и путь к файлу> – имя файла, в который вы хотите вывести события, и путь к нему;

<файл базы данных> – имя файла базы данных журнала событий и путь к нему.

Команды управления параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA)

-R – префикс, указывающий, что команда принадлежит к группе команд управления параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA).

[-R] --add-kataedr-server-certificate <имя и путь к файлу> – добавляет или заменяет ранее добавленный сертификат сервера KATA.

[-R] --remove-kataedr-server-certificate – удаляет сертификат сервера KATA.

[-R] --query-kataedr-server-certificate – выводит информацию о сертификате сервера KATA.

[-R] --add-kataedr-client-certificate <имя и путь к файлу> – добавляет или заменяет ранее добавленный сертификат клиента, используемый для защиты подключения к серверу KATA.

[-R] --remove-kataedr-client-certificate – удаляет сертификат клиента, используемый для защиты подключения к серверу KATA.

[-R] --query-kataedr-client-certificate – выводит информацию о сертификате клиента.

[-R] --isolation-stat – выводит в консоль текущее состояние сетевой изоляции: включена или выключена.

[-R] --isolation-off – выключить сетевую изоляцию устройства (команда выполняется синхронно, то есть, управление не вернется пока задача не завершится). Эту команду рекомендуется использовать в случае потери связи с сервером KATA после включения сетевой изоляции.

Команды приложения в режиме Легкого агента для защиты виртуальных сред

Команды могут быть выполнены, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

-V – префикс, указывающий, что команда принадлежит к группе команд приложения Kaspersky Endpoint Security, используемого в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23) (в составе решения Kaspersky Security для виртуальных сред Легкий агент).

[-V] --ksvla-info – выводит информацию об использовании приложения в режиме Легкого агента для защиты виртуальных сред:

- Режим Легкого агента для защиты виртуальных сред: включен / выключен.

  Если режим Легкого агента включен, приложение используется в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент. Если режим Легкого агента выключен, приложение используется в автономном режиме.

- Режим защиты инфраструктуры VDI: включен / выключен.

  Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. Если режим защиты инфраструктуры VDI включен, то обновления, требующие перезагрузки защищенной виртуальной машины, не устанавливаются на временных виртуальных машинах. При получении обновлений, требующих перезагрузки, Легкий агент, установленный на временной виртуальной машине, отправляет в Kaspersky Security Center сообщение о необходимости обновления шаблона защищенных виртуальных машин.

- Роль виртуальной машины в виртуальной инфраструктуре: сервер или рабочая станция.

- Идентификатор (UUID) защищенной виртуальной машины.

[-V] --viis-info – выводит информацию о подключении Легкого агента (приложения Kaspersky Endpoint Security, используемого в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент), к Серверу интеграции:

- Адрес и порт Сервера интеграции, к которому подключается Легкий агент.

- Статус подключения к Серверу интеграции.

- Дата и время последнего соединения Легкого агента с Сервером интеграции.

[-V] --svm-info – выводит информацию о подключении Легкого агента (приложения Kaspersky Endpoint Security, используемого в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент), к SVM:

- Адрес SVM, к которой подключен Легкий агент.
- Способ обнаружения SVM Легким агентом: с помощью Сервера интеграции или с использованием списка адресов SVM, заданных вручную.
- Список адресов SVM, если в качестве способа обнаружения SVM выбрано использование списка адресов SVM.
- Тег для подключения Легкого агента к SVM.
- Алгоритм выбора SVM: стандартный или расширенный.
- Тип расположения SVM в виртуальной инфраструктуре, который учитывается при выборе SVM для подключения, если применяется расширенный алгоритм выбора SVM.
- Наличие защиты соединения между Легким агентом и Сервером защиты.

Информацию о параметрах подключения Легких агентов к Серверу интеграции и SVM см. в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254032.htm.

Использование фильтра для ограничения результатов запроса

Вы можете использовать фильтр, чтобы ограничить результаты запроса для следующих команд:

- Получение информации о событиях приложения:

  ```
  kesl-control -E --query "<логическое выражение>"
  ```

- Получение информации об объектах (см. раздел "Просмотр идентификаторов объектов в Хранилище" на стр. 180) в Хранилище:

  ```
  kesl-control -B --query "<логическое выражение>"
  ```

- Удаление выбранных объектов (см. раздел "Удаление объектов из Хранилища" на стр. 181) из Хранилища:

  ```
  kesl-control -B --mass-remove --query "<логическое выражение>"
  ```

Для указания фильтра вы можете использовать несколько логических выражений, комбинируя их с помощью логического оператора **and**. Логические выражения требуется заключать в кавычки.

Синтаксис

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

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

Таблица 6. Операции сравнения

Операция сравнения	Описание
>	Больше
<	Меньше
like	Соответствует указанному значению (при указании значения можно использовать маски %, см. пример ниже)
==	Равно
!=	Не равно
>=	Больше или равно
<=	Меньше или равно

Примеры:

Вывести информацию о файлах в Хранилище, имеющих высокий (High) уровень важности:

```
kesl-control -B --query "DangerLevel == 'High'"
```

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

```
kesl-control -E --query "FileName like '%etc%'"
```

Вывести события с типом ThreatDetected (обнаружена угроза):

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

Вывести события с типом ThreatDetected, сформированные задачами с типом ODS:

```
kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

Вывести события, сформированные после даты, указанной в системе отметок времени UNIX™ (количество секунд, прошедших с 00:00:00 (UTC), 1 января 1970 года):

```
kesl-control -E --query "Date > '1583425000'"
```

Вывести события, сформированные после даты, указанной в формате YYYY-MM-DD hh:mm:ss:

```
kesl-control -E --query "Date > '2022-12-22 18:52:45'"
```

Экспорт и импорт параметров приложения

Kaspersky Endpoint Security 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 `kesl-control --export-settings`.

Синтаксис команды

```
kesl-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 `kesl-control --import-settings`.

Если вы управляете приложением через Kaspersky Security Center, импорт параметров недоступен.

Синтаксис команды

```
kesl-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 (на стр. 260), требуется указать `UseKSN=Basic` или `UseKSN=Extended`.

После импорта параметров приложения внутренние идентификаторы задач могут измениться. Для управления ими рекомендуется использовать названия задач.

kaspersky

Установка ограничения на использование памяти приложением

Вы можете задать ограничение на использование памяти приложением Kaspersky Endpoint Security во время выполнения задач проверки (типов ODS и OAS), в мегабайтах.

Параметр ограничивает только количество памяти, которое используется при проверке файлов, то есть общий размер памяти, потребляемый приложением, может быть больше значения, заданного этим параметром.

Минимальное значение параметра: 2 МБ. Значение по умолчанию: 8192 МБ. Если указанное значение меньше 2 МБ, приложение будет использовать минимальное значение (2 МБ). Если указанное значение превышает размер оперативной памяти, приложение будет использовать до 25% оперативной памяти. Это значение изменить невозможно.

► *Чтобы указать ограничение на использование памяти при проверке файлов:*

1. Остановите Kaspersky Endpoint Security (см. раздел "Запуск и остановка приложения" на стр. 92).
2. Откройте файл /var/opt/kaspersky/kesl/common/kesl.ini на редактирование.
3. Добавьте следующий параметр в секцию **[General]**:

   ```
   ScanMemoryLimit=<количество памяти в мегабайтах>
   ```

4. Запустите Kaspersky Endpoint Security (см. раздел "Запуск и остановка приложения" на стр. 92).

Ограничение на использование памяти при проверке файлов изменится при запуске приложения.

Общие параметры приложения

Этот раздел содержит информацию о командах управления общими параметрами приложения и параметрами проверки контейнеров.

В этом разделе

Описание общих параметров приложения

В этом разделе описаны значения общих параметров конфигурационного файла приложения Kaspersky Endpoint Security (см. таблицу ниже).

Таблица 7. 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.
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 создания и уровень детализации файла трассировки (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 514).	`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. В файлах трассировки (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 514) содержится информация об операционной системе, а также могут содержаться персональные данные (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 514).	Значение по умолчанию: /var/log/kaspersky/kesl. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, с правами которой работает Kaspersky Endpoint Security. 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.

Параметр	Описание	Значения
TraceMaxFileSize	Максимальный размер файла трассировки приложения (в мегабайтах).	1–1000 Значение по умолчанию: 500. После изменения значения этого параметра требуется перезапустить приложение.
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 программ, которые могут быть использованы злоумышленником для нанесения вреда устройству или данным пользователя.	`Yes` – включить обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда устройству или данным пользователя. `No` (значение по умолчанию) – выключить обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда устройству или данным пользователя.
NamespaceMonitoring	Включение проверки пространств имен и контейнеров. Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен. При этом при просмотре информации о приложении (см. раздел "Просмотр информации о приложении" на стр. 95) в строке **Мониторинг контейнеров** отображается “Задача доступна и не выполняется”.	`Yes` (значение по умолчанию) – включить проверку пространств имен и контейнеров. `No` – выключить проверку пространств имен и контейнеров.

Параметр	Описание	Значения
InterceptorProtectionMode	Режим работы файлового перехватчика при выполнении задач, использующих перехватчик файловых операций (Защита от файловых угроз, Защита от шифрования, Контроль устройств и Проверка съемных дисков. Этот параметр влияет на режим работы задач Защита от файловых угроз и Контроль устройств.	`Block` (значение по умолчанию) – блокировать файлы на время проверки задачей, использующей файловый перехватчик. Обращение к любому файлу ожидает результатов проверки. При обнаружении зараженных объектов приложение выполняет действия, указанные в параметрах `FirstAction` и `SecondAction` задачи Защита от файловых угроз. `Notify` – не блокировать файлы на время проверки задачей, использующей файловый перехватчик. Обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме. При обнаружении зараженных объектов приложение лишь записывает событие в журнал событий. Действия, указанные в параметрах `FirstAction` и `SecondAction` задачи Защита от файловых угроз, не выполняются. Если выбрано значение `Notify`, включается информирующий режим работы компонентов Защита от файловых угроз и Контроль устройств. Выбор значения `Notify` снижает уровень защиты вашего устройства.
UseKSN	Включение использования Kaspersky Security Network (см. раздел "Использование Kaspersky Security Network" на стр. 260). 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.

Параметр	Описание	Значения
CloudMode	Включение облачного режима работы приложения (см. раздел "Использование Kaspersky Security Network" на стр. 260). Облачный режим доступен, если включено использование KSN. Если вы планируете использовать облачный режим, убедитесь, что KSN доступен на устройстве. Включение облачного режима приводит к выходу приложения из сертифицированного состояния.	Yes – включить режим работы, при котором приложение Kaspersky Endpoint Security 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 Managed Detection and Response. В сертифицированной версии приложения интеграция с Kaspersky Managed Detection and Response не поддерживается. Включение Managed Detection and Response приводит к выходу приложения из сертифицированного состояния.	Yes – включить Managed Detection and Response. No (значение по умолчанию) – выключить Managed Detection and Response.
UseProxy	Включение использования прокси-сервера компонентами приложения Kaspersky Endpoint Security. Прокси-сервер может использоваться для взаимодействия с Kaspersky Security Network, с Kaspersky Endpoint Detection and Response (KATA), для активации приложения и при обновлении баз и модулей приложения. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование прокси-сервера для подключения к Kaspersky Security Network, к SVM и к Серверу интеграции.	Yes – включить использование прокси-сервера. No (значение по умолчанию) – выключить использование прокси-сервера.

Параметр	Описание	Значения
ProxyServer	Параметры прокси-сервера в формате [пользователь[:пароль]@]узел[: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.
LimitNumberOfScanFileTasks	Максимальное количество задач типа Scan_File, 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 типа Scan_File. Если во время установки приложения вы также 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.
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/kesl/private/storage/events.db.

Параметр	Описание	Значения
ExcludedMountPoint.item_#	Точка монтирования, которую требуется исключить из области проверки для задач, использующих перехватчик файловых операций (Защита от файловых угроз и Защита от шифрования). 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 с типом ODS, ContainerScan и InventoryScan.	`Yes` – включить ограничение потребления ресурсов процессора для задач с типом ODS, ContainerScan и InventoryScan. `No` (значение по умолчанию) – выключить ограничение потребления ресурсов процессора для задач с типом ODS, ContainerScan и InventoryScan.

Параметр	Описание	Значения
OnDemandCPULimit	Максимальное значение нагрузки на все ядра процессора (в процентах) при работе задач с типом ODS, ContainerScan и InventoryScan.	10–100 Значение по умолчанию: 100.

Изменение общих параметров приложения

Для изменения параметров приложения требуется наличие root-прав.

► *Чтобы изменить общие параметры приложения:*

1. Сохраните общие параметры приложения в конфигурационном файле с помощью команды --get-app-settings:

   `kesl-control [-T] --get-app-settings --file <путь к конфигурационному файлу>`

2. Откройте созданный конфигурационный файл, измените нужные параметры приложения и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в приложение с помощью команды --set-app-settings:

   `kesl-control [-T] --set-app-settings --file <путь к конфигурационному файлу>`

   Для включения использования Kaspersky Security Network требуется запускать команду `kesl-control --set-settings` с флагом `--accept-ksn`: `kesl-control --set-app-settings UseKSN=Basic|Extended --accept-ksn`.

Приложение Kaspersky Endpoint Security применит новые значения параметров после перезапуска (см. раздел "Запуск и остановка приложения" на стр. 92).

Вы можете использовать созданный конфигурационный файл для импорта параметров в приложение, установленное на другом устройстве.

Команда kesl-control --get-app-settings

Команда `kesl-control --get-app-settings` выводит общие параметры приложения. Используя эту команду, вы также можете экспортировать общие параметры приложения в конфигурационный файл.

Синтаксис команды

`kesl-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 сохранены параметры приложения. Если вы укажете имя файла, не указав пути 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, конфигурационный файл не будет создан. Если вы не укажете ключ --file, общие параметры приложения будут выведены в консоль.

`--json` – формат конфигурационного файла, в который будут сохранены параметры приложения. Если вы не укажете формат файла, экспорт будет выполнен в файл формата INI. При невозможности импорта отображается ошибка.

Пример:

Экспортировать общие параметры приложения в файл с именем kesl_config.ini. Сохранить созданный файл в текущей директории:

```
kesl-control --get-app-settings --file kesl_config.ini
```

Команда kesl-control --set-app-settings

Команда `kesl-control --set-app-settings` устанавливает с помощью ключей команды или импортирует из указанного конфигурационного файла общие параметры приложения.

Синтаксис команды

```
kesl-control [-T] --set-app-settings <название параметра>=<значение параметра> <название параметра>=<значение параметра>
```

```
kesl-control [-T] --set-app-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` – формат конфигурационного файла, параметры из которого будут импортированы в приложение. Если вы не укажете формат файла, приложение попытается выполнить импорт из файла формата INI.

Примеры:

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

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

Установить низкий уровень детализации файла трассировки:

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

Добавить точку монтирования, которую требуется исключить из области проверки для задач, использующих перехват файловых операций (Защита от файловых угроз и Защита от шифрования):

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

Описание общих параметров проверки контейнеров

В этом разделе описаны значения общих параметров проверки контейнеров и пространств имен (см. таблицу ниже). Поддерживается интеграция с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Приложение не проверяет пространства имен и контейнеры, если в операционной системе не

установлены компоненты для работы с контейнерами и пространствами имен. При этом при просмотре информации о приложении (см. раздел "Просмотр информации о приложении" на стр. 95) в строке **Мониторинг контейнеров** отображается “Задача доступна и не выполняется”. Включение проверки пространств имен и контейнеров выполняется с помощью параметра `NamespaceMonitoring`, описанного в общих параметрах приложения (см. раздел "Описание общих параметров приложения" на стр. 106).

Таблица 8. Общие параметры проверки контейнеров и пространств имен

Параметр	Описание	Значения
OnAccessContainerScanAction	Действие над контейнером при обнаружении зараженного объекта. Этот параметр доступен при использовании приложения по лицензии, которая включает эту функцию. При проверке используются параметры задачи Защита от файловых угроз. Действие над контейнером при обнаружении зараженного объекта также зависит от заданных параметров задачи Защита от файловых угроз (см. таблицу ниже).	`StopContainerIfFailed` (значение по умолчанию) – остановить контейнер, если не удалось вылечить или удалить зараженный объект. `StopContainer` – остановить контейнер при обнаружении зараженного объекта. `Skip` – 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.

Параметр	Описание	Значения
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.
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. 134) и от значения параметра `InterceptorProtectionMode`, указанного в общих параметрах приложения (см. раздел "Описание общих параметров приложения" на стр. 106) (см. таблицу ниже).

Таблица 9. Зависимость действия над контейнером от заданного действия при обнаружении угрозы

Значение параметра FirstAction / SecondAction или InterceptorProtectionMode	Действие, выполняемое над контейнером при выбранном действии StopContainerIfFailed
`Disinfect`	Остановить контейнер, если не удалось вылечить зараженный объект.
`Remove`	Остановить контейнер, если не удалось удалить зараженный объект.
`Block` или `Notify`	Не выполнять никаких действий над контейнерами при обнаружении зараженного объекта.

Изменение общих параметров проверки контейнеров

Изменение общих параметров проверки контейнеров

Для изменения параметров приложения требуется наличие root-прав.

► *Чтобы изменить общие параметры проверки контейнеров:*

1. Сохраните общие параметры проверки контейнеров в конфигурационном файле с помощью команды --get-container-settings:

   `kesl-control [-C] --get-container-settings --file <имя конфигурационного файла>`

2. Откройте созданный конфигурационный файл, измените нужные параметры проверки контейнеров и сохраните изменения.
3. Импортируйте параметры проверки контейнеров из конфигурационного файла в приложение с помощью команды --set-container-settings:

   `kesl-control [-C] --set-container-settings --file <имя конфигурационного файла>`

Kaspersky Endpoint Security применит новые значения параметров после перезапуска (см. раздел "Запуск и остановка приложения" на стр. 92).

Команда kesl-control --get-container-settings

Команда `kesl-control --get-container-settings` выводит общие параметры проверки контейнеров. Используя эту команду, вы также можете экспортировать общие параметры проверки контейнеров в конфигурационный файл.

Синтаксис команды

`kesl-control [-C] --get-container-settings [--file <имя конфигурационного файла>]`

Аргументы и ключи

`--file <имя конфигурационного файла>` – имя конфигурационного файла, в который будут сохранены параметры проверки контейнеров.

Если вы укажете имя файла, не указав пути 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, конфигурационный файл не будет создан.

Команда kesl-control --set-container-settings

Команда `kesl-control --set-container-settings` устанавливает с помощью ключей команды или импортирует из указанного конфигурационного файла общие параметры проверки контейнеров.

Синтаксис команды

`kesl-control [-C] --set-container-settings --file <имя конфигурационного файла>`

`kesl-control [-C] --set-container-settings <имя параметра>=<значение параметра> <название параметра>=<значение параметра>`

Аргументы и ключи

`--file <имя конфигурационного файла>` – имя конфигурационного файла, из которого параметры проверки контейнеров будут импортированы в приложение; включает полный путь к файлу.

kaspersky

Управление задачами приложения с помощью командной строки

Вы можете управлять работой приложения с помощью задач как локально на устройстве (с помощью командной строки или конфигурационных файлов), так и с помощью Консоли администрирования или Kaspersky Security Center Web Console.

Для работы с приложением предусмотрено два типа задач:

- *Предустановленная задача* – задача, которая создается во время установки приложения. Вы не можете удалять предустановленные задачи, но можете изменять параметры этих задач.

  Если приложение используется в режиме Легкого агента для защиты виртуальных сред, параметры предустановленной задачи типа Update недоступны для изменения.

- *Пользовательская задача* – задача, которую вы можете создавать или удалять самостоятельно. В зависимости от режима использования приложения (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23) вы можете создавать задачи следующих типов:
  - автономный режим: ODS, Update (см. раздел "Задача Обновление (Update, ID:6)" на стр. 172), Rollback (см. раздел "Задача Откат обновления баз (Rollback, ID:7)" на стр. 176), ODFIM (см. раздел "Контроль целостности системы по требованию (ODFIM)" на стр. 183), ContainerScan и InventoryScan (см. раздел "Задача Инвентаризация (Inventory_Scan, ID:22)" на стр. 251);
  - режим Легкого агента для защиты виртуальных сред: ODS, ODFIM (см. раздел "Контроль целостности системы по требованию (ODFIM)" на стр. 183), ContainerScan и InventoryScan (см. раздел "Задача Инвентаризация (Inventory_Scan, ID:22)" на стр. 251).

Идентификатор (ID) задачи – номер задачи, который приложение присваивает задаче при ее создании. Идентификаторы пользовательских задач начинаются с 100. Все задачи, включая удаленные, имеют уникальные идентификаторы. Приложение не использует повторно идентификаторы удаленных задач. Идентификатор новой задачи представляет собой номер, следующий по порядку за идентификатором последней созданной задачи.

Названия задач не чувствительны к регистру.

Предустановленные задачи приложения перечислены в таблице.

Таблица 10. Задачи приложения

Задача	Название задачи в командной строке	ID задачи	Тип задачи
Защита от файловых угроз	File_Threat_Protection	1	OAS
Поиск вредоносного ПО	Scan_My_Computer	2	ODS
Выборочная проверка	Scan_File	3	ODS
Проверка важных областей	Critical_Areas_Scan	4	ODS
Обновление	Update	6	Update
Откат обновления баз	Rollback	7	Rollback
Лицензирование	License	9	License
Управление Хранилищем	Backup	10	Backup

Задача	Название задачи в командной строке	ID задачи	Тип задачи
Контроль целостности системы	System_Integrity_Monitoring	11	OAFIM
Управление сетевым экраном	Firewall_Management	12	Firewall
Защита от шифрования	Anti_Cryptor	13	AntiCryptor
Защита от веб-угроз	Web_Threat_Protection	14	WTP
Контроль устройств	Device_Control	15	DeviceControl
Проверка съемных дисков	Removable_Drives_Scan	16	RDS
Защита от сетевых угроз	Network_Threat_Protection	17	NTP
Проверка контейнеров	Container_Scan	18	ContainerScan
Выборочная проверка контейнеров	Custom_Container_Scan	19	ContainerScan
Анализ поведения	Behavior_Detection	20	BehaviorDetection
Контроль приложений	Application_Control	21	AppControl
Инвентаризация	Inventory_Scan	22	InventoryScan
Интеграция с Kaspersky Endpoint Detection and Response (KATA)	KATAEDR	24	KATAEDR

Вы можете выполнять следующие действия над задачами:

- запускать и останавливать задачи (см. раздел "Запуск и остановка задачи" на стр. 123);
- создавать (см. раздел "Создание задачи" на стр. 121) и удалять (см. раздел "Удаление задачи" на стр. 129) пользовательские задачи;
- изменять параметры задач.

Набор доступных действий для задачи зависит от типа задачи и от режима использования приложения (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23).

kaspersky

В этом разделе

Просмотр списка задач

► *Чтобы просмотреть список задач приложения, выполните следующую команду:*

```
kesl-control [-T] --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 Endpoint Security.

Для каждой задачи отображается следующая информация:

- `Name`. Название задачи (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118).
- `ID`. Идентификатор задачи (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118).
- `Type`. Тип задачи (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118).
- `State`. Текущее состояние 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.

kaspersky

Создание задачи

Если приложение используется в автономном режиме, вы можете создавать задачи следующих типов: ODS, Update, Rollback, ODFIM, ContainerScan и InventoryScan. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, вы можете создавать задачи следующих типов: ODS, 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:*

```
kesl-control [-T] --create-task <название задачи> --type <тип задачи>
```

где:

- <название задачи> – название, которое вы задаете для новой задачи;
- <тип задачи> – тип задачи (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118).

Задача указанного типа создается с параметрами по умолчанию.

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

```
kesl-control [-T] --create-task <название задачи> --type <тип задачи> --file
<путь к файлу> [--json]
```

где:

- <название задачи> – название, которое вы задаете для новой задачи;
- <тип задачи> – тип задачи (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118);
- <путь к файлу> – полный путь к конфигурационному файлу (см. раздел "Приложение 2. Конфигурационные файлы приложения" на стр. 522).

Задача указанного типа создается с параметрами, указанными в конфигурационном файле.

Изменение параметров задачи с помощью конфигурационного файла

Если приложение используется в режиме Легкого агента для защиты виртуальных сред, параметры задачи типа Update недоступны для изменения.

► *Чтобы изменить параметры задачи путем изменения конфигурационного файла:*

1. Сохраните параметры задачи в конфигурационный файл:

```
kesl-control --get-settings <ID задачи>|<название задачи> --file <полный путь к файлу> [--json]
```

2. Откройте созданный конфигурационный файл для редактирования.
3. Измените нужный параметр в конфигурационном файле.
4. Сохраните изменения в конфигурационном файле.
5. Импортируйте в задачу параметры из конфигурационного файла:

```
kesl-control --set-settings <ID задачи>|<название задачи> --file <полный путь к файлу> [--json]
```

Параметры задачи обновятся.

В случае, если в параметрах задачи Контроль приложений вы меняете разрешающий список или запрещаете запуск всех приложений и/или приложений, влияющих на работу приложения Kaspersky Endpoint Security, требуется запускать команду `--set-settings` с флагом `--accept`.

Изменение параметров задачи с помощью командной строки

Если приложение используется в режиме Легкого агента для защиты виртуальных сред, параметры задачи типа Update недоступны для изменения.

► *Чтобы изменить параметры задачи с помощью командной строки:*

1. Укажите нужное значение параметра:

```
kesl-control --set-settings <ID задачи>|<название задачи> <параметр=значение> [<параметр=значение>]
```

Приложение изменит указанный параметр.

В случае, если в параметрах задачи Контроль приложений вы меняете разрешающий список или запрещаете запуск всех приложений и / или приложений, влияющих на работу приложения Kaspersky Endpoint Security, требуется запускать команду `--set-settings` с флагом `--accept`.

2. Убедитесь, что значение параметра изменено в конфигурационном файле задачи:

```
kesl-control --get-settings <ID задачи>|<название задачи>
```

Если вы добавили новую область проверки или область исключения без указания всех параметров, область будет добавлена в конфигурационный файл с параметрами по умолчанию.

Пример:

Чтобы указать новую область проверки, выполните следующую команду:

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

В конфигурационный файл будет добавлен новый раздел с описанием области проверки для задачи с ID=100:

```
[ScanScope.item_0001]

AreaDesc=

UseScanArea=Yes

Path=/home

AreaMask.item_0000=*
```

Восстановление заданных по умолчанию параметров задачи

Приложение Kaspersky Endpoint Security позволяет восстановить заданные по умолчанию параметры задачи из командной строки.

Восстановление заданных по умолчанию параметров недоступно для задач Backup и Rollback.

► *Чтобы восстановить заданные по умолчанию параметры задачи из командной строки:*

1. Выполните следующую команду:

   ```
   kesl-control --set-settings <ID задачи>|<название задачи> --set-to-default
   ```

   Приложение изменит значения параметров на заданные по умолчанию.

2. Убедитесь, что значения параметров изменены в конфигурационном файле задачи:

   ```
   kesl-control --get-settings <ID задачи>|<название задачи> --file <имя конфигурационного файла>
   ```

   Конфигурационный файл задачи содержит значения всех параметров, заданные по умолчанию.

Запуск и остановка задачи

По умолчанию при запуске приложения автоматически запускаются задачи Защита от файловых угроз (см. раздел "Задача Защита от файловых угроз (File_Threat_Protection, ID:1)" на стр. 133), Контроль устройств (см. раздел "Задача Контроль устройств (Device_Control, ID:15)" на стр. 209) и Анализ поведения (см. раздел "Задача Анализ поведения (Behavior_Detection, ID:20)" на стр. 242). Остальные задачи остановлены (имеют статус *Stopped*).

Вы можете запустить задачу в любой момент.

Вы не можете запускать и останавливать задачи с типами Backup и License.

► *Чтобы запустить задачу, выполните следующую команду:*

```
kesl-control --start-task <ID задачи>|<название задачи>
```

► *Чтобы остановить задачу, выполните следующую команду:*

```
kesl-control --stop-task <ID задачи>|<название задачи>
```

Просмотр состояния задачи

► *Чтобы просмотреть состояние задачи, выполните следующую команду:*

```
kesl-control --get-task-state <ID задачи>|<название задачи>
```

где:

- `<ID задачи>` – идентификатор задачи, который приложение присвоило задаче в момент создания.

Задачи приложения могут находиться в одном из следующих состояний:

- `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.

Задачи типов Backup (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 179) и License (см. раздел "Задача Лицензирование (License, ID:9)" на стр. 177) нельзя запускать, приостанавливать и останавливать. Они могут находиться только в состоянии `Started`.

Настройка расписания задачи

Если приложение используется в автономном режиме, вы можете просмотреть и настроить параметры расписания запуска задач следующих типов: ODS, Update, Rollback, ODFIM, ContainerScan и InventoryScan. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, вы можете просмотреть и настроить параметры расписания запуска задач следующих типов: ODS, ODFIM, ContainerScan и InventoryScan.

Изменение параметров расписания задачи

► *Чтобы настроить параметры расписания задачи:*

1. Сохраните параметры расписания задачи в конфигурационный файл с помощью следующей команды:

   `kesl-control --get-schedule <ID задачи>|<название задачи> --file <имя конфигурационного файла> [--json]`

2. Откройте конфигурационный файл для редактирования.
3. Задайте параметры расписания.
4. Сохраните изменения в конфигурационном файле.
5. Импортируйте параметры расписания из конфигурационного файла расписания в задачу с помощью следующей команды:

   `kesl-control --set-schedule <ID задачи>|<название задачи> --file <имя конфигурационного файла> [--json]`

Приложение применит новые значения параметров расписания немедленно.

Параметры расписания задачи

В приложении предусмотрены следующие параметры для настройки расписания запуска задачи:

`RuleType=Once|Monthly|Weekly|Daily|Hourly|Minutely|Manual|PS|BR`

где:

Manual – запускать задачу вручную.

PS – запускать задачу после запуска приложения.

BR – запускать задачу после обновления баз приложения.

`StartTime=[<год>/<месяц>/<день месяца>] [чч]:[мм]:[сс]; [<день месяца>|<день недели>]; [<периодичность запуска>]` – время запуска задачи. Параметр `StartTime` является обязательным, если значение параметра RuleType=Once|Monthly|Weekly|Daily|Hourly|Minutely.

`RandomInterval=<мин.>` – 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.

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
```

Команда kesl-control --get-schedule

Команда `kesl-control --get-schedule` выводит параметры расписания задачи или сохраняет их в указанный конфигурационный файл.

Синтаксис команды

```
kesl-control [-T] --get-schedule <ID задачи>|<название задачи> [--file <имя конфигурационного файла>] [--json]
```

Аргументы и ключи

<ID задачи> – идентификационный номер задачи в приложении.

<название задачи> – название задачи.

--file <имя конфигурационного файла> – имя конфигурационного файла, в который будут сохранены параметры расписания. Если вы укажете имя файла, не указав пути 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, конфигурационный файл не будет создан.

Примеры:

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

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

Вывести расписание задачи обновления:

```
kesl-control --get-schedule 6
```

Команда kesl-control --set-schedule

Команда kesl-control --set-schedule задает параметры расписания задачи с помощью ключей команды или импортирует параметры расписания задачи из указанного конфигурационного файла.

Синтаксис команды

```
kesl-control --set-schedule <ID задачи>|<название задачи> --file <имя конфигурационного файла> [--json]
```

```
kesl-control --set-schedule <ID задачи>|<название задачи> <название параметра>=<значение параметра> <название параметра>=<значение параметра>
```

Аргументы и ключи

<ID задачи> – идентификационный номер задачи в приложении.

<название задачи> – название задачи.

--file <имя конфигурационного файла> – имя конфигурационного файла, параметры расписания из которого будут импортированы в задачу; включает полный путь к файлу.

Пример:

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

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

kaspersky

Управление областями проверки из командной строки

Вы можете добавить или удалить область проверки с указанным параметром `Path` для задач OAS, ODS, OAFIM, ODFIM и AntiCryptor из командной строки.

► *Чтобы добавить новую область проверки, выполните следующую команду:*

```
kesl-control --set-settings <ID задачи>|<название задачи> --add-path <путь>
```

В конфигурационный файл будет добавлена новая секция `[ScanScope.item_#]`. Приложение будет проверять объекты в директории, указанной параметром `Path`.

Если для указанного параметра `Path` уже существует секция `[ScanScope.item_#]`, дублирующая секция не добавляется в конфигурационный файл. Если для параметра `UseScanArea` установлено значение `No`, после выполнения этой команды значение изменится на `Yes` и будет выполняться проверка объектов, расположенных в этой директории.

► *Чтобы удалить область проверки, выполните следующую команду:*

```
kesl-control --set-settings <ID задачи>|<название задачи> --del-path <путь>
```

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

Управление областями исключения из командной строки

Вы можете добавить или удалить область исключения с указанным параметром `Path` для задач OAS, ODS, OAFIM, ODFIM и AntiCryptor из командной строки.

► *Чтобы добавить новую область исключения, выполните следующую команду:*

```
kesl-control --set-settings <ID задачи>|<название задачи> --add-exclusion
<путь>
```

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 в качестве пути для исключения вы можете указать `/.snapshots/*/snapshot/`.

В конфигурационный файл будет добавлена новая секция `[ExcludedFromScanScope.item_#]`. Приложение будет исключать из проверки объекты в директории, указанной параметром `Path`.

Если для указанного параметра `Path` уже существует секция `[ExcludedFromScanScope.item_#]`, дублирующая секция не добавляется в конфигурационный файл. 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, выполните следующую команду:*

```
kesl-control --set-settings <ID задачи>|<название задачи> --del-exclusion
<путь>
```

Секция `[ExcludedFromScanScope.item_#]`, содержащая указанный путь, будет удалена из конфигурационного файла задачи. Приложение не будет исключать из проверки объекты в директории, указанной параметром `Path`.

Удаление задачи

Вы можете удалять только те задачи, которые вы создали. Предустановленные задачи недоступны для удаления.

Если приложение используется в режиме Легкого агента для защиты виртуальных сред, задача типа Update недоступна для удаления.

► *Чтобы удалить задачу, выполните следующую команду:*

```
kesl-control --delete-task <ID задачи>|<название задачи>
```

Проверка зашифрованных соединений

Вы можете настраивать параметры проверки зашифрованных соединений, которые используются в задаче Защита от веб-угроз (см. раздел "Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)" на стр. 206).

Также вы можете настраивать список доверенных сертификатов (см. раздел "Управление доверенными сертификатами" на стр. 132), который используется при проверке зашифрованных соединений.

В этом разделе

Параметры проверки зашифрованных соединений

В таблице описаны все доступные значения и значения по умолчанию для каждого параметра.

При изменении параметров проверки зашифрованных соединений приложение записывает в журнал событие *NetworkSettingsChanged*.

Таблица 11. Параметры проверки зашифрованных соединений

Параметр	Описание	Значения
EncryptedConnectionsScan	Включает или выключает проверку зашифрованного трафика. Для FTP-протокола проверка зашифрованных соединений по умолчанию выключена.	`Yes` (значение по умолчанию) – включить проверку зашифрованных соединений. `No` – выключить проверку зашифрованных соединений. Приложение не расшифровывает зашифрованный трафик.
EncryptedConnectionsScanErrorAction	Действие, выполняемое приложением при возникновении ошибки проверки зашифрованных 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	Задает способ проверки сертификатов приложением Kaspersky Endpoint Security. Если сертификат является самозаверяющим, 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 возникновении ошибки проверки зашифрованных соединений на веб-сайте.	`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	Включает или выключает использование исключений при проверке зашифрованного трафика.	`Yes` – не проверять веб-сайты, указанные в разделе `[Exclusions.item_#]`. `No` (значение по умолчанию) – проверять все веб-сайты.
MonitorNetworkPorts	Способ контроля сетевых портов приложением Kaspersky Endpoint Security.	`Selected` (значение по умолчанию) – контролировать только сетевые порты, указанные в разделе `[NetworkPorts.item_#]` (см. ниже). `All` – контролировать все сетевые порты. Выбор этого значения может значительно увеличить нагрузку на операционную систему.

Параметр	Описание	Значения
Секция [Exclusions.item_#] содержит домены, исключенные из проверки. Приложение не проверяет зашифрованные 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.

Управление параметрами проверки зашифрованных соединений

Вы можете управлять параметрами проверки зашифрованных соединений из командной строки.

- *Чтобы просмотреть список исключений из проверки зашифрованных соединений, добавленных пользователем, выполните следующую команду:*

  ```
  kesl-control -N --query user
  ```

- *Чтобы просмотреть список исключений из проверки зашифрованных соединений, добавленных приложением, выполните следующую команду:*

  ```
  kesl-control -N --query auto
  ```

- *Чтобы просмотреть список исключений из проверки зашифрованных соединений, полученных из баз приложения, выполните следующую команду:*

  ```
  kesl-control -N --query kl
  ```

- *Чтобы очистить список доменов, которые приложение автоматически исключила из проверки, выполните следующую команду:*

  ```
  kesl-control -N --clear-web-auto-excluded
  ```

- *Чтобы просмотреть значения параметров проверки зашифрованных соединений, выполните следующую команду:*

  ```
  kesl-control [-N] --get-net-settings [--file <имя и путь к файлу>]
  ```

  Выходной файл имеет формат INI.

- *Чтобы установить значения параметров проверки зашифрованных соединений, выполните следующую команду:*

  ```
  kesl-control [-N] --set-net-settings [--file <имя и путь к файлу>]
  ```

kaspersky

Управление доверенными сертификатами

Вы можете задать список сертификатов, которые приложение будет считать доверенными. Список доверенных сертификатов используется при проверке зашифрованных соединений.

Вы можете управлять списком доверенных сертификатов из командной строки.

► *Чтобы добавить сертификат в список доверенных сертификатов, выполните следующую команду:*

```
kesl-control [-N] --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:*

```
kesl-control [-N] --remove-certificate <субъект сертификата>
```

► *Чтобы просмотреть список доверенных сертификатов, выполните следующую команду:*

```
kesl-control [-N] --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 SHA-256.

kaspersky

Задача Защита от файловых угроз (File_Threat_Protection, ID:1)

Защита от файловых угроз позволяет избежать заражения файловой системы устройства. Задача Защита от файловых угроз создается автоматически с параметрами по умолчанию при установке приложения Kaspersky Endpoint Security на устройство. По умолчанию задача Защита от файловых угроз запускается автоматически при запуске приложения. Задача постоянно находится в оперативной памяти устройства и проверяет все открываемые, сохраняемые и запускаемые файлы.

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. 88).

При обнаружении вредоносного ПО приложение Kaspersky Endpoint Security может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

Во время работы задачи Защита от файловых угроз приложение выполняет проверку всех пространств имен и контейнеров во всех поддерживаемых операционных системах, если в общих параметрах приложения (см. раздел "Описание общих параметров приложения" на стр. 106) для параметра `NamespaceMonitoring` задано значение `Yes`. Дополнительно для операционной системы Astra Linux пользовательская задача выборочной проверки (Scan_File) позволяет проверять файлы из других пространств имен (в рамках обязательной проверки). Вы можете отдельно настроить общие параметры проверки контейнеров (см. раздел "Описание общих параметров проверки контейнеров" на стр. 114) и пространств имен.

Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен. При этом при просмотре информации о приложении (см. раздел "Просмотр информации о приложении" на стр. 95) в строке **Мониторинг контейнеров** отображается “Задача доступна и не выполняется”.

Вы не можете создавать пользовательские задачи Защита от файловых угроз. Вы можете изменить параметры задачи Защита от файловых угроз (на стр. 134), созданной по умолчанию.

Если в общих параметрах приложения (см. раздел "Описание общих параметров приложения" на стр. 106) для параметра `InterceptorProtectionMode` задано значение `Notify`, то при обнаружении зараженных объектов приложение не выполняет действия, указанные в параметрах (см. раздел "Параметры задачи Защита от файловых угроз" на стр. 134) `FirstAction` и `SecondAction` задачи Защита от файловых угроз.

kaspersky

В этом разделе

Особенности проверки символических и жестких ссылок

Приложение Kaspersky Endpoint Security 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 защиты задачи Защита от файловых угроз.

Если файл, обращение к которому происходит по символической ссылке, не входит в область задачи 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 рекомендуемое действие** (Perform recommended action), приложение автоматически подбирает и выполняет действие над объектом на основе данных об опасности обнаруженной в объекте угрозы и возможности его лечения.
- Если выбрано действие **Удалять** (Remove), приложение удаляет обрабатываемую жесткую ссылку. Остальные жесткие ссылки на этот файл обработаны не будут.
- Если выбрано действие **Лечить** (Disinfect), 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 Хранилища, приложение создает копию исходного файла с именем жесткой ссылки, которая была помещена в Хранилище. Связи с остальными жесткими ссылками на исходный файл восстановлены не будут.

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 12. 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. Перед тем как выполнить над объектом выбранное вами действие, Kaspersky Endpoint Security блокирует доступ к этому объекту для приложений, которые к нему обращаются. Если в общих параметрах приложения для параметра `InterceptorProtectionMode` задано значение `Notify`, то при обнаружении зараженных объектов приложение не выполняет действие, указанное параметром `FirstAction`.	`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. Например, Kaspersky Endpoint Security сразу удаляет троянские программы, 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. Значение по умолчанию: `Recommended`.

Параметр	Описание	Значения
SecondAction	Выбор второго действия, которое приложение будет выполнять над зараженными объектами.Приложение выполняет второе действие, если не удалось выполнить первое действие. Если в общих параметрах приложения для параметра InterceptorProtectionMode задано значение Notify, то при обнаружении зараженных объектов приложение не выполняет действие, указанное параметром SecondAction.	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=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_#.

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 веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

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.

Параметр	Описание	Значения
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. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.	`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.

Параметр	Описание	Значения
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`.
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. 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,	<путь к локальной директории> – проверять объекты в указанной директории. Для указания пути вы можете использовать маски и теги. 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.

Параметр	Описание	Значения
	/dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.	
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).

Path	Путь к директории с исключаемыми объектами. 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,	<путь к локальной директории> – исключать из проверки объекты в указанной директории. Для указания пути вы можете использовать маски и теги. 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.

Параметр	Описание	Значения
	включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.	
Секция **[ExcludedForProgram.item_#]** содержит следующие параметры:		
ProgramPath	Путь к исключаемому процессу.	<полный путь к процессу> – исключать из проверки процесс в указанной локальной директории.
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.
AreaDesc	Описание области исключения процессов.	Значение по умолчанию: All objects.
UseExcludedForProgram	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.
AreaMask.item_#	Ограничение области исключения процессов. В области исключения процессов приложение не проверяет только файлы, указанные помощью масок в формате shell. Если параметр не указан, приложение исключает из проверки все объекты в области исключения процессов. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (исключать из проверки все объекты).

Параметр	Описание	Значения
Path	Путь к директории с файлами, которые изменяет процесс. 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.	<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.

Формирование области исключения

Вы можете указать область исключения для задачи Защита от файловых угроз. Файлы в области исключения исключаются из области защиты.

► *Чтобы создать область исключения:*

1. Сохраните параметры задачи Защита от файловых угроз в файл с помощью следующей команды:

   ```
   kesl-control --get-settings 1 --file <полный путь к конфигурационному файлу>
   ```

2. Добавьте в созданный файл секцию [ExcludedFromScanScope.item_#]. Эта секция содержит следующие параметры:

- `AreaDesc` – описание области исключения, содержащее дополнительную информацию об области исключения.
- `Path` – путь к файлам или директориям, которые вы хотите исключить из области защиты.
- `AreaMask.item_#` – маска имени файла для файлов, которые вы хотите исключить из области защиты.

Пример:

```
[ExcludedFromScanScope.item_0000]
AreaDesc=
UseScanArea=Yes
Path=/tmp/notchecked
AreaMask.item_0000=*
```

3. Импортируйте параметры из конфигурационного файла в задачу Защита от файловых угроз с помощью следующей команды:

   `kesl-control --set-settings 1 --file <полный путь к конфигурационному файлу>`

Вы также можете управлять областями исключения из командной строки (см. раздел "Управление областями исключения из командной строки" на стр. 128).

Оптимизация проверки сетевых директорий

Для оптимизации работы задачи 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 из проверки для утилиты, предназначенной для копирования из сетевых директорий (например, для утилиты `cp`).

► *Чтобы настроить исключение сетевых директорий из проверки:*

1. Сохраните параметры задачи Защита от файловых угроз в файл с помощью следующей команды:

   `kesl-control --get-settings 1 --file <полный путь к конфигурационному файлу>`

2. Добавьте в созданный файл секцию `[ExcludedForProgram.item_#]`. Эта секция содержит следующие параметры:

   - `ProgramPath` – путь к исключаемому процессу или к директории с исключаемыми процессам.
   - `ApplyToDescendants` – параметр, показывающий, нужно ли исключать из проверки дочерних процессов исключаемого процесса, указанного параметром `ProgramPath` (возможные значения: `Yes` или `No`).
   - `AreaDesc` – описание области исключения по процессам, содержащее дополнительную информацию об области исключения.
   - `UseExcludedForProgram` – параметр, показывающий, нужно ли исключать указанную область из проверки 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. Импортируйте параметры из конфигурационного файла в задачу Защита от файловых угроз с помощью следующей команды:

   ```
   kesl-control --set-settings 1 --file <полный путь к конфигурационному файлу>
   ```

Приложение не будет проверять файлы в сетевых директориях, при этом сама команда `cp` (для приведенного выше примера) и локальные файлы будут проверяться.

kaspersky

Задача Поиск вредоносного ПО (Scan_My_Computer, ID:2)

Поиск вредоносного ПО – это однократная полная или выборочная проверка файлов на устройстве, выполняемая приложением Kaspersky Endpoint Security. Приложение может выполнять несколько задач поиска вредоносного ПО одновременно. Вы также можете создавать пользовательские задачи поиска вредоносного ПО.

По умолчанию в приложении создается предустановленная задача поиска вредоносного ПО – *полная проверка*. 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.

При обнаружении вредоносного ПО приложение Kaspersky Endpoint Security 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*.

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Поиск вредоносного ПО.

Таблица 13. 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.

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.
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.
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.

Параметр	Описание	Значения
FirstAction	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	`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. Например, Kaspersky Endpoint Security сразу удаляет троянские программы, 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: `Recommended`.
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_#`.

Параметр	Описание	Значения

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=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 веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/.
		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
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.
ReportUnprocessed Objects	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.

Параметр	Описание	Значения
UseIChecker	Включение использования технологии iChecker. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.	`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="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. 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.	<путь к локальной директории> – исключать из проверки объекты в указанной 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.

kaspersky

Задача Выборочная проверка (Scan_File, ID:3)

Задача Выборочная проверка используется для хранения значений параметров, которые применяются при выполнении команды `kesl-control --scan-file`.

При запуске команды секции [ScanScope.item_#] и [ExcludedFromScanScope.item_#] в параметрах этой задачи не наследуются из исходной задачи с ID=3.

Вы можете изменить параметры проверки для задачи Scan_File из командной строки.

При обнаружении вредоносного ПО приложение Kaspersky Endpoint Security может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Выборочная проверка.

Таблица 14. Параметры задачи Выборочная проверка

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.

Параметр	Описание	Значения
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.
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.

Параметр	Описание	Значения
FirstAction	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	`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. Например, Kaspersky Endpoint Security сразу удаляет троянские программы, 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: `Recommended`.
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_#`.

Параметр	Описание	Значения

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 веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

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.
ReportUnprocessed Objects	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. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.

Параметр	Описание	Значения
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.
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.
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).

Параметр	Описание	Значения
Path	Путь к директории с исключаемыми объектами. 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.	<путь к локальной директории> – исключать из проверки объекты в указанной 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.

kaspersky

Задача Проверка важных областей (Critical_Areas_Scan, ID:4)

Задача Проверка важных областей позволяет проверять загрузочные секторы, объекты автозапуска, память процессов и память ядра.

При обнаружении вредоносного ПО приложение Kaspersky Endpoint Security может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Проверка важных областей.

Таблица 15. 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.

Параметр	Описание	Значения
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.
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.

Параметр	Описание	Значения
FirstAction	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	`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. Например, Kaspersky Endpoint Security сразу удаляет троянские программы, 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: `Recommended`.
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_#`.

Параметр	Описание	Значения

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=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 веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/.
		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
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.
ReportUnprocessed Objects	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.

Параметр	Описание	Значения
UseIChecker	Включение использования технологии iChecker. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.	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 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.
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).

Параметр	Описание	Значения
Path	Путь к директории с исключаемыми объектами. 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.	<путь к локальной директории> – исключать из проверки объекты в указанной 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.

kaspersky

Задача Обновление (Update, ID:6)

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), обновление баз на защищенных виртуальных машинах выполняется с помощью специальной локальной задачи *Обновление*, в которой в качестве источника обновлений указана директория на SVM. Задача обновления запускается автоматически. Вы не можете удалять эту задачу и изменять ее параметры.

Обновление баз и модулей приложения Kaspersky Endpoint Security 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 приложения.

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

Основным источником обновлений (см. раздел "Об источниках обновлений" на стр. 173) служат серверы обновлений "Лаборатории Касперского".

Для успешной загрузки пакета обновлений с серверов обновлений "Лаборатории Касперского" устройство должно быть подключено к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, требуется настроить параметры прокси-сервера. Загрузка пакета обновлений выполняется с помощью задачи Обновление.

В процессе обновления на вашем устройстве загружаются и устанавливаются базы приложения. Во время установки приложение получает актуальные базы с одного из HTTP-серверов обновлений "Лаборатории Касперского". Если для обновления используется предустановленная задача с параметрами по умолчанию (ID=6), приложение обновляет базы с периодичностью один раз в 60 минут. Вы можете изменять параметры предустановленной задачи обновления баз и создавать пользовательские задачи обновления.

В процессе обновления базы на вашем устройстве сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы отличаются от актуальной версии недостающая часть обновлений устанавливается на устройство.

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.

По умолчанию приложение записывает в журнал событие *Базы устарели* (*BasesAreOutOfDate*), если последние установленные обновления баз были опубликованы на сервере "Лаборатории Касперского" более трех, но менее семи дней назад. Если базы не обновляются в течение семи дней, приложение записывает в журнал событие *Базы сильно устарели* (*BasesAreTotallyOutOfDate*). Базы актуальны, если они были загружены менее трех дней назад.

Если загрузка обновлений баз 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.

Допускается устанавливать только обновления модулей приложения, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу приложения из сертифицированного состояния.

В этом разделе

Об источниках обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей приложения Kaspersky Endpoint Security. Источником обновлений могут быть FTP-, HTTP- или HTTPS-серверы (например, серверы обновлений Kaspersky Security Center и "Лаборатории Касперского") и локальные или сетевые директории, смонтированные пользователем.

В предустановленной задаче Обновление в качестве источника обновлений по умолчанию выбраны серверы обновлений "Лаборатории Касперского". На серверы обновлений выкладываются обновления баз и программных модулей для многих приложений "Лаборатории Касперского". Обновления загружаются по протоколу HTTPS.

Если по каким-то причинам вы не можете использовать в качестве источника обновлений серверы обновлений "Лаборатории Касперского", вы можете получать обновления из *пользовательского источника обновлений* – из указанной 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 (см. раздел "Параметры задачи Обновление" на стр. 173).

Параметры задачи Обновление

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Обновление.

Таблица 16. Параметры задачи Обновление

Параметр	Описание	Значения
SourceType	Источник (см. раздел "Об источниках обновлений" на стр. 173), 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 Kaspersky Security Center. 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	Включение использования 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.

Задача Откат обновления баз (Rollback, ID:7)

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), не поддерживается использование локальной задачи приложения *Откат обновления баз*.

После первого обновления баз приложения становится доступна функция отката баз приложения к их предыдущей версии.

Каждый раз, когда пользователь запускает процесс обновления, Kaspersky Endpoint Security создает резервную копию текущих баз приложения. Это позволяет откатить базы приложения до предыдущей версии, если потребуется. Откат последних обновлений используется, например, если новая версия баз приложения содержит недопустимые сигнатуры, что приводит к блокировке безопасных приложений приложением Kaspersky Endpoint Security.

Задача Откат обновления баз не имеет параметров.

kaspersky

Задача Лицензирование (License, ID:9)

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), отдельно активировать приложение не требуется. Вы активируете решение Kaspersky Security для виртуальных сред Легкий агент, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионного ключа на SVM. Команды управления задачей Лицензирование завершаются с ошибкой.

Задача Лицензирование позволяет управлять лицензионными ключами (см. раздел "О лицензионном ключе" на стр. 77) приложения Kaspersky Endpoint Security.

В этом разделе

Добавление лицензионного ключа

Команда добавления лицензионного ключа может быть выполнена, только если приложение используется в автономном режиме (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23). При использовании приложения в режиме Легкого агента для защиты виртуальных сред эта команда завершается с ошибкой.

Команда `kesl-control --add-active-key` добавляет активный ключ (см. раздел "О лицензионном ключе" на стр. 77).

Синтаксис команды

```
kesl-control [-L] --add-active-key <путь к файлу ключа>
```

Аргументы и ключи

`<путь к файлу ключа>` – путь к файлу ключа (см. раздел "О лицензионном ключе" на стр. 77). Если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

Добавить ключ в качестве активного ключа с помощью файла /home/test/00000001.key:

```
kesl-control --add-active-key /home/test/00000001.key
```

Команда `kesl-control --add-reserve-key` добавляет резервный ключ (см. раздел "О лицензионном ключе" на стр. 77).

Если активный ключ не добавлен, то резервный ключ будет добавлен как основной.

Синтаксис команды

```
kesl-control [-L] --add-reserve-key <путь к файлу ключа>
```

Аргументы и ключи

`<путь к файлу ключа>` – путь к файлу ключа (см. раздел "О лицензионном ключе" на стр. 77). Если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

Добавить резервный ключ с помощью файла /home/test/00000002.key:

```
kesl-control --add-reserve-key /home/test/00000002.key
```

Удаление лицензионного ключа

Команда удаления лицензионного ключа может быть выполнена, только если приложение используется в автономном режиме (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23). При использовании приложения в режиме Легкого агента для защиты виртуальных сред эта команда завершается с ошибкой.

Команда `kesl-control --remove-active-key` удаляет активный ключ.

Синтаксис команды

```
kesl-control [-L] --remove-active-key
```

Команда `kesl-control --remove-reserve-key` удаляет резервный ключ.

Синтаксис команды

```
kesl-control [-L] --remove-reserve-key
```

kaspersky

Задача Управление Хранилищем (Backup, ID:10)

Хранилище – это список резервных копий файлов, которые были удалены или изменены в процессе лечения. *Резервная копия* – копия файла, которая создается при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

По умолчанию Хранилище расположено в директории /var/opt/kaspersky/kesl/common/objects-backup/. Файлы в Хранилище могут содержать персональные данные. Для доступа к файлам в Хранилище требуются root-права.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете попытаться восстановить файл (см. раздел "Восстановление объектов из Хранилища" на стр. 180) из его вылеченной копии в директорию исходного размещения файла.

В этом разделе

Параметры задачи Управление Хранилищем

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Управление Хранилищем.

Таблица 17. Параметры задачи Управление Хранилищем

Параметр	Описание	Значение
DaysToLive	Интервал времени, в течение которого объекты хранятся в Хранилище (в сутках). Чтобы снять ограничение для времени хранения объектов в Хранилище, укажите значение 0.	0 – время хранения объектов в Хранилище не ограничено. Значение по умолчанию: 90.
BackupSizeLimit	Максимальный размер Хранилища (в мегабайтах). При достижении максимального размера Хранилища, приложение удаляет самые старые объекты. Чтобы снять ограничение для размера Хранилища, укажите значение 0.	0 – 999999 0 – размер Хранилища не ограничен. Значение по умолчанию: 0.

Параметр	Описание	Значение
BackupFolder	Путь к директории Хранилища. Вы можете указать в качестве Хранилища пользовательскую директорию, отличную от директории, заданной по умолчанию. В качестве Хранилища можно использовать директории на любых устройствах. Не рекомендуется указывать директории, расположенные на удаленных устройствах, например смонтированных по протоколам Samba и NFS. Kaspersky Endpoint Security 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/kesl/common/objects-backup/ Для доступа к заданной по умолчанию директории Хранилища требуются root-права.

Просмотр идентификаторов объектов в Хранилище

Когда объект помещается в Хранилище, приложение присваивает ему числовой идентификатор. Этот идентификатор используется для выполнения действий над объектом, таких как восстановление (см. раздел "Восстановление объектов из Хранилища" на стр. 180) или удаление объекта из Хранилища (см. раздел "Удаление объектов из Хранилища" на стр. 181).

► *Чтобы просмотреть идентификаторы объектов в Хранилище, выполните следующую команду:*

```
kesl-control -B --query
```

Идентификатор объекта будет выведен в строке `ObjectId`.

Восстановление объектов из Хранилища

Kaspersky Endpoint Security хранит объекты в Хранилище в зашифрованном виде, чтобы предохранить защищаемое устройство от их возможного вредоносного действия.

Если требуется, вы можете восстанавливать объекты из Хранилища. Восстановление объектов может потребоваться, например, если при лечении зараженного файла приложению не удалось сохранить его целостность, и в результате информация в файле стала недоступной.

Восстановление зараженных объектов может привести к заражению устройства.

kaspersky

При восстановлении из Хранилища вы можете сохранить файл под другим именем.

► *Чтобы восстановить объект с исходным именем в исходное местоположение, выполните следующую команду:*

```
kesl-control [-B] --restore <ID объекта>
```

где <ID объекта> – это идентификатор объекта (см. раздел "Просмотр идентификаторов объектов в Хранилище" на стр. 180) в Хранилище.

► *Чтобы восстановить объект с новым именем в указанную директорию, выполните следующую команду:*

```
kesl-control [-B] --restore <ID объекта> --file <имя файла и путь к директории файла>
```

Если указанной директории не существует, приложение создает ее.

Удаление объектов из Хранилища

► *Чтобы удалить объект из Хранилища, выполните следующую команду:*

```
kesl-control -B --mass-remove --query "ObjectId == '<ID объекта>'"
```

Пример:

Чтобы удалить объект с ID=15:

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

► *Чтобы удалить несколько объектов из Хранилища, выполните следующую команду:*

```
kesl-control -B --mass-remove --query "<поле> <логическое выражение> '<значение>' [и <поле> <логическое выражение> '<значение>']"
```

Пример:

Чтобы удалить объекты, в названии которых или в пути к которым содержится "test":

```
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

► *Чтобы удалить все объекты из Хранилища, выполните одну из следующих команд:*

```
kesl-control -B --mass-remove
```

или

```
kesl-control -B --mass-remove --query
```

kaspersky

Задача Контроль целостности системы (System_Integrity_Monitoring, ID:11)

Задача Контроль целостности системы предназначена для отслеживания действий, выполняемых с файлами и директориями в области мониторинга, указанной в параметрах задачи. Вы можете использовать задачу, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом сервере.

Для использования задачи требуется лицензия, которая включает эту функцию.

Контроль целостности системы может выполняться в режиме реального времени при запуске задачи Контроль целостности системы при доступе (OAFIM) (на стр. 182). Кроме того, вы можете создавать и запускать задачи Контроль целостности системы по требованию (ODFIM) (на стр. 183).

Оба типа задачи отправляют уведомления об изменениях в списках контроля доступа к объектам. В случае задачи OAFIM в отчет не включаются данные о том, какие именно изменения внесены. В случае задачи ODFIM в отчет включаются данные об измененных атрибутах и перемещенных файлах и директориях.

В этом разделе

Контроль целостности системы при доступе (OAFIM)

Во время работы задачи OAFIM каждое изменение объекта определяется путем перехвата файловых операций в режиме реального времени. При изменении объекта приложение Kaspersky Endpoint Security отправляет событие на Сервер администрирования Kaspersky Security Center. Во время работы задачи контрольная сумма файла не рассчитывается. Приложение не отслеживает изменения файлов (атрибутов и содержимого) с жесткими ссылками, которые расположены вне области мониторинга. Приложение отслеживает операции с конкретными файлами или в областях мониторинга, указанных в параметрах задачи.

Области мониторинга

Для задачи Контроль целостности системы требуется указать области мониторинга. Администратор может изменять области мониторинга в режиме реального времени. Вы можете указать несколько областей мониторинга. Если область мониторинга не указана, параметры задачи невозможно сохранить в конфигурационном файле.

Исключения из области мониторинга

Вы можете создавать исключения из области мониторинга. Исключения указываются для каждой отдельной области и работают только для указанной области мониторинга. Вы можете указать несколько областей исключения из мониторинга.

Исключения имеют более высокий приоритет, чем область мониторинга, и не проверяются задачей, даже если указанная директория или файл находятся в области мониторинга. Если параметры одного из правил указывают область мониторинга на более низком уровне, чем директория, указанная в исключении, область мониторинга не рассматривается при выполнении задачи.

Для указания исключений вы можете использовать те же маски в формате командной оболочки, которые используются для указания областей мониторинга.

При добавлении области мониторинга или области исключения приложение не проверяет, существует ли такая директория.

Контролируемые параметры

Во время работы задачи Контроль целостности системы контролируется изменение следующих параметров:

- содержимое (write (), truncate (), etc.);
- метаданные (правообладание (chmod/chown));
- отметки времени (utimensat);
- расширенные атрибуты (setxattr) и другие.

Технологические ограничения операционной системы Linux не позволяют задаче Контроль целостности системы определять, какой администратор или процесс внес изменение в файл.

Контроль целостности системы по требованию (ODFIM)

В процессе выполнения задачи ODFIM изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы, по критериям: хеш файла, время изменения файла, размер файла.

Снимок состояния системы создается во время первого выполнения задачи ODFIM на устройстве. Вы можете создать несколько задач ODFIM. Для каждой задачи ODFIM создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы относится к области мониторинга. Если снимок состояния системы не соответствует области мониторинга, приложение создает событие о нарушении целостности системы. Снимок состояния системы содержит пути к контролируемым объектам и их метаданные. Снимок состояния системы может также содержать персональные данные.

Снимок состояния системы создается заново после завершения задачи ODFIM. Вы можете заново создать снимок для задачи с помощью параметра RebuildBaseline (см. раздел "Параметры задачи Контроль целостности системы по требованию" на стр. 186). Снимок состояния системы также создается при изменении параметров задачи, например, при добавлении новой области мониторинга. При следующем выполнении задачи снимок состояния системы формируется заново. Вы можете удалить снимок состояния системы, удалив соответствующую задачу ODFIM.

Задача ODFIM создает хранилище для снимков состояния системы на устройстве с установленным компонентом Контроль целостности системы. По умолчанию снимки состояния системы хранятся в базе данных /var/opt/kaspersky/kesl/private/fim.db. Для доступа к базе данных, в которой хранятся снимки состояния системы, требуются root-права.

Параметры задачи Контроль целостности системы при доступе

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Контроль целостности системы при доступе.

Таблица 18. Параметры задачи Контроль целостности системы при доступе

Параметр	Описание	Значения
UseExcludeMasks	Включение исключения из области мониторинга объектов, указанными параметром `ExcludeThreats.item_#`. Этот параметр работает, только если указано значение параметра `ExcludeMasks.item_#`.	`Yes` – исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга. `No` (значение по умолчанию) – не исключать объекты, указанные параметром `ExcludeMasks.item_#`, 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 `UseExcludeMasks`. 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.

Параметр	Описание	Значения
UseScanArea	Включение мониторинга указанной области.	`Yes` (значение по умолчанию) – контролировать указанную область. `No` – не контролировать указанную область.
Path	Путь к директории для мониторинга. 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.	Для указания пути вы можете использовать маски. Значение по умолчанию: /opt/kaspersky/kesl/
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_#]. Объекты, удовлетворяющие правилам любой из секций [ExcludedFromScanScope.item_#], будут исключены из мониторинга. 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 мониторинга, содержит дополнительную информацию об области исключения из мониторинга.	Значение по умолчанию не задано.

Параметр	Описание	Значения
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. 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.	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).

Параметры задачи Контроль целостности системы по требованию

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Контроль целостности системы по требованию.

Таблица 19. Параметры задачи Контроль целостности системы по требованию

Параметр	Описание	Значения
RebuildBaseline	Включение повторного создания снимка состояния системы после завершения задачи ODFIM.	`Yes` – создавать снимок состояния системы повторно после завершения задачи ODFIM. `No` (значение по умолчанию) – не создавать снимок состояния системы повторно после завершения задачи ODFIM.
CheckFileHash	Включение проверки хеша (SHA-256).	`Yes` – включить проверку хеша. `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. `No` (значение по умолчанию) – не контролировать директории.
TrackLastAccessTime	Включение проверки времени последнего доступа к файлу. В операционных системах Linux это параметр `noatime`.	`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 `ExcludeMasks.item_#`. Этот параметр работает, только если указано значение параметра `ExcludeMasks.item_#`.	`Yes` – исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга. `No` (значение по умолчанию) – не исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга.

Параметр	Описание	Значения
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 `UseExcludeMasks`. 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.

Параметр	Описание	Значения
Path	Путь к директории для мониторинга. 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.	Для указания пути вы можете использовать маски. Значение по умолчанию: /opt/kaspersky/kesl/
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_#]. Объекты, удовлетворяющие правилам любой из секций [ExcludedFromScanScope.item_#], будут исключены из мониторинга. 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 мониторинга, содержит дополнительную информацию об области исключения из мониторинга.	Значение по умолчанию не задано.

Параметр	Описание	Значения
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. 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.	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).

kaspersky

Задача Управление сетевым экраном (Firewall_Management, ID:12)

Во время работы в локальных сетях и интернете устройство подвержено не только заражению вирусами и другими вредоносными программами, но и различного рода атакам, использующим уязвимости операционных систем и программного обеспечения. Сетевой экран операционной системы защищает персональные 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. Задача Управление сетевым экраном позволяет задать статус этих сетевых соединений при помощи настройки сетевых пакетных правил (см. раздел "О сетевых пакетных правилах" на стр. 192). Настройка сетевых пакетных правил позволяет вам 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 задачи Управление сетевым экраном.

Задача Управление сетевым экраном предоставляет графическую оболочку для управления межсетевым экраном, входящим в состав операционной системы.

Во время работы задачи Управление сетевым экраном приложение Kaspersky Endpoint Security блокирует любую настройку параметров сетевого экрана операционной системы, когда, например, какая-либо утилита или программа добавляет или удаляет какое-то правило сетевого экрана. Приложение проверяет сетевой экран операционной системы каждые 60 секунд и восстанавливает набор правил сетевого экрана, если требуется. Периодичность проверки изменить невозможно.

В операционных системах Red Hat Enterprise Linux и CentOS 8 правила сетевого экрана, созданные с помощью приложения Kaspersky Endpoint Security, можно просмотреть только с помощью приложения (команда `kesl-control -F --query`).

Проверка сетевого экрана операционной системы по-прежнему выполняется, когда задача Управление сетевым экраном остановлена. Это позволяет приложению восстанавливать динамические правила (см. раздел "О динамических правилах" на стр. 192).

Во избежание возможных проблем на системах с nftables приложение Kaspersky Endpoint Security использует системные утилиты iptables и iptables-restore при добавлении правил для системного сетевого экрана.

Приложение создает специальную разрешающую цепочку правил kesl_bypass и добавляет ее первой в список таблицы mangle утилит iptables и ip6tables. Правила цепочки kesl_bypass позволяют исключать трафик из проверки приложением Kaspersky Endpoint Security. Изменение правил в этой цепочке выполняется средствами операционной системы.

При удалении приложения цепочка правил kesl_bypass в iptables и ip6tables удаляется, только если она была пустая.

kaspersky

Перед включением задачи Управление сетевым экраном рекомендуется выключить другие средства управления сетевым экраном операционной системы.

В этом разделе

О сетевых пакетных правилах

Сетевое пакетное правило представляет собой разрешающее или запрещающее действие, которое совершает задача Управление сетевым экраном, 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 задачи Управление 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

Компоненты приложения Kaspersky Endpoint Security позволяют добавлять и удалять в сетевой экран *динамические правила*, необходимые для его правильной работы. Например, Агент администрирования добавляет динамические правила, которые разрешают соединение с Kaspersky Security Center, инициируемое как приложением, так и Kaspersky Security Center. Правила задачи Защита от шифрования тоже являются динамическими.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, в сетевой экран автоматически добавляются динамические правила, которые разрешают соединения с SVM и Сервером интеграции.

Задача Управление сетевым экраном не контролирует динамические правила и не блокирует доступ к сетевым ресурсам для компонентов приложения. Динамические правила не зависят от состояния задачи Управление сетевым экраном (запущена / остановлена) или от изменения параметров этой задачи. Приоритет выполнения динамических правил выше приоритета сетевых пакетных правил (см. раздел "О сетевых пакетных правилах" на стр. 192). 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 `kesl-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 для параметра `--remote`. В Kaspersky Endpoint Security 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 (см. раздел "Добавление сетевого адреса в секцию зоны" на стр. 199) IP-адреса и подсети в сетевую зону или удалять (см. раздел "Удаление сетевого адреса из секции зоны" на стр. 199) их из нее.

Параметры задачи Управление сетевым экраном

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Управление сетевым экраном.

Таблица 20. Параметры задачи Управление сетевым экраном

Параметр	Описание	Значения
DefaultIncomingAction	Действие по умолчанию, применяемое к входящему соединению, если другие сетевые правила не применяются к этому виду соединения.	`Allow` (значение по умолчанию) – разрешать входящие соединения. `Block` – запрещать входящие соединения.

Параметр	Описание	Значения
DefaultIncomingPacketAction	Действие по умолчанию, применяемое к входящему пакету, если другие сетевые пакетные правила не применяются к этому виду соединения.	`Allow` (значение по умолчанию) – разрешать входящие пакеты. `Block` – запрещать входящие пакеты.
OpenNagentPorts	Добавление динамических правил для Агента администрирования в пакетные правила.	`Yes` (значение по умолчанию) – добавлять динамические правила для Агента администрирования в пакетные правила. `No` – 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 `[PacketRules.item_#]` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Каждая секция `[PacketRules.item_#]` содержит следующие параметры:		
Name	Имя сетевого пакетного правила.	Значение по умолчанию: Packet rule #<n>, где n – это индекс.
FirewallAction	Действие, применяемое к соединениям, указанным в сетевом пакетном правиле.	`Allow` (значение по умолчанию) – разрешать сетевые соединения. `Block` – запрещать сетевые соединения.

Protocol	Тип протокола, для которого необходим мониторинг сетевой активности.	`Any` (значение по умолчанию) – задача Управление сетевым экраном контролирует всю сетевую активность.
		`TCP`
		`UDP`
		`ICMP`
		`ICMPv6`
		`IGMP`
		`GRE`

RemotePorts	Номера портов удаленных устройств, соединение между которыми отслеживается. Этот параметр можно указать, только если для параметра `Protocol` установлено значение `TCP` или `UDP`.	`Any` (значение по умолчанию) – контролировать все удаленные порты. `0` – `65535`. Для этого параметра вы можете указать значение в виде целого числа или в виде интервала.
LocalPorts	Номера портов локальных устройств, соединение между которыми отслеживается. Этот параметр можно указать, только если для параметра `Protocol` установлено значение `TCP` или `UDP`.	`Any` (значение по умолчанию) – контролировать все локальные порты. `0` – `65535`. Для этого параметра вы можете указать значение в виде целого числа или в виде интервала.

Параметр	Описание	Значения
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.
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.

Параметр	Описание	Значения
LocalAddress	Сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, 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	Указывает, следует ли включать в отчет действия сетевого правила.	`Yes` – отражать действия в отчете. `No` (значение по умолчанию) – не отражать действия в отчете.
Секция **[NetworkZonesPublic]** содержит сетевые адреса, связанные с публичными 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 **[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).

Параметр	Описание	Значения
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).

Добавление сетевого пакетного правила

Вы можете добавить сетевое пакетное правило (см. раздел "О сетевых пакетных правилах" на стр. 192) вручную.

Сетевые пакетные правила можно добавлять только по одному.

► *Чтобы добавить сетевое пакетное правило, выполните следующую команду:*

```
kesl-control -F --add-rule --name <имя правила> --action <действие> --protocol <протокол> --direction <направление> --remote <удаленный адрес> --local <локальный адрес> --at <индекс в списке сетевых пакетных правил>
```

В конфигурационный файл задачи Управление сетевым экраном будет добавлен раздел, содержащий параметры нового сетевого пакетного правила. Если вы не указали в команде конкретный параметр, устанавливается значение по умолчанию (см. раздел "Конфигурационный файл задачи Управление сетевым экраном" на стр. 535).

Параметр `--at` позволяет указать индекс создаваемого правила в списке сетевых пакетных правил. Если параметр `--at` не указан или его значение больше числа правил в списке, новое правило добавляется в конец списка.

Примеры:

Чтобы создать правило, блокирующее все входящие и создаваемые соединения по протоколу TCP через порт 23, выполните следующую команду:

```
kesl-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:

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in
--protocol TCP --local any:23 --remote Public
```

Удаление сетевого пакетного правила

Вы можете удалить сетевое пакетное правило вручную.

Сетевые пакетные правила можно удалять только по одному.

► *Чтобы удалить сетевое пакетное правило, выполните одну из следующих команд:*

- `kesl-control -F --del-rule --name <имя правила>`

  Сетевое пакетное правило будет удалено по имени. Если список сетевых пакетных правил содержит несколько правил с одинаковым именем, приложение не удаляет ни одно из них.

- `kesl-control -F --del-rule --index <индекс>`

  Сетевое пакетное правило будет удалено по индексу в списке сетевых пакетных правил.

Из конфигурационного файла задачи Управление сетевым экраном будет удален блок, содержащий параметры сетевого пакетного правила.

Если список сетевых пакетных правил не содержит правило с указанным именем или индексом, происходит ошибка.

Изменение приоритета выполнения сетевого пакетного правила

Вы можете вручную изменить приоритет выполнения сетевого пакетного правила.

► *Чтобы изменить приоритет выполнения сетевого пакетного правила, выполните следующую команду:*

```
kesl-control -F --move-rule [--name <имя правила>|--index <индекс>] --at
<индекс>
```

Приоритет выполнения сетевого пакетного правила будет изменен в соответствии с указанным индексом.

kaspersky

Добавление сетевого адреса в секцию зоны

Вы можете вручную добавить в конфигурационный файл задачи Управление сетевым экраном (на стр. 535) сетевые адреса, связанные с определенным типом сети.

► *Чтобы добавить сетевой адрес в зону, выполните следующую команду:*

```
kesl-control -F --add-zone <Public|Local|Trusted> --address <адрес>
```

Сетевой адрес будет добавлен в секцию указанной зоны в конфигурационном файле задачи.

Удаление сетевого адреса из секции зоны

Вы можете вручную удалить из конфигурационного файла задачи Управление сетевым экраном (см. раздел "Конфигурационный файл задачи Управление сетевым экраном" на стр. 535) сетевые адреса, связанные с определенным типом сети. Это может понадобиться, если сетевые адреса больше не используются.

► *Чтобы удалить сетевой адрес из зоны, выполните следующую команду:*

```
kesl-control -F --del-zone <зона> [--address <адрес>| --index <индекс адреса в зоне>]
```

Указанный сетевой адрес будет удален из секции указанной зоны в конфигурационном файле.

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.

kaspersky

Задача Защита от шифрования (Anti_Cryptor, ID:13)

Задача Защита от шифрования позволяет защитить ваши файлы в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования.

В процессе выполнения задачи Защита от шифрования приложение Kaspersky Endpoint Security проверяет обращения удаленных устройств сети к файлам, расположенным в общих сетевых директориях защищаемого устройства. Если приложение расценивает действия удаленного устройства, получающего доступ к общим сетевым ресурсам, как вредоносное шифрование, оно добавляет это устройство в список недоверенных устройств и запрещает ему доступ к общим сетевым директориям. По умолчанию приложение блокирует доступ недоверенных устройств к сетевым файловым ресурсам на 30 минут. Приложение не расценивает действия как шифрование, если активность шифрования обнаружена в директориях, исключенных из области защиты (см. раздел "Параметры задачи Защита от шифрования" на стр. 201) задачи Защита от шифрования.

Для использования задачи требуется лицензия, которая включает эту функцию.

Для корректной работы задачи Защита от шифрования требуется, чтобы в операционной системе была установлена хотя бы одна из служб: Samba или NFS. Для службы NFS требуется установленный пакет rpcbind.

Задача 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.

Задача Защита от шифрования 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

О блокировке доступа к недоверенным устройствам

При обнаружении вредоносного шифрования приложение создает и включает правило для сетевого экрана операционной системы, которое блокирует сетевой трафик от скомпрометированного устройства.

Скомпрометированное устройство добавляется в список недоверенных устройств. Приложение блокирует доступ к общим сетевым директориям для всех удаленных устройств в списке недоверенных устройств. Информация обо всех заблокированных устройствах отправляется в Kaspersky Security Center.

Правила сетевого экрана, созданные задачей Защита от шифрования, нельзя удалить с помощью утилиты iptables, так как приложение восстанавливает набор правил каждую минуту. Используйте команду `--allow-hosts` (см. раздел "Разблокировка заблокированных устройств" на стр. 205), чтобы разблокировать устройство.

По умолчанию приложение удаляет недоверенные устройства из списка через 30 минут после добавления в список. Доступ устройств к сетевым файловым ресурсам восстанавливается автоматически после удаления недоверенного устройства из списка. Вы можете изменять список заблокированных устройств и указывать период, после которого заблокированные устройства будут автоматически разблокированы.

Параметры задачи Защита от шифрования

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Защита от шифрования.

Таблица 21. Параметры задачи Защита от шифрования

Параметр	Описание	Значения
UseHostBlocker	Включение блокировки недоверенных устройств. Если блокировка недоверенных устройств выключена, приложение все равно проверяет действия удаленных устройств с сетевыми файловыми ресурсами на наличие вредоносного шифрования, когда работает задача Защита от шифрования. В случае обнаружения вредоносного шифрования создается событие *EncryptionDetected*, но атакующее устройство не блокируется.	`Yes` (значение по умолчанию) – включить блокировку недоверенных устройств. `No` – выключить блокировку недоверенных устройств.
BlockTime	Длительность блокировки доступа к недоверенному устройству 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.

Параметр	Описание	Значения
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`.
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).

Параметр	Описание	Значения
Path	Путь к директории с защищаемыми объектам. 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.	<путь к локальной директории> – защищать локальную директорию, доступную через SMB/NFS. Для указания пути вы можете использовать маски. 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.
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: All objects.
UseScanArea	Исключение указанной области из защиты.	Yes (значение по умолчанию) – исключать указанную область из защиты. No – не исключать указанную область из защиты.

Параметр	Описание	Значения
AreaMask.item_#	Ограничение области исключения из защиты. В области исключения 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 все объекты).
Path	Путь к директории с объектами, исключаемыми из защиты. 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.	`<путь к локальной директории>` – исключать из защиты объекты в указанной директории. Для указания пути вы можете использовать маски. `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.

Просмотр списка заблокированных устройств

Вы можете просматривать список недоверенных устройств, заблокированных задачей Защита от шифрования.

► *Чтобы просмотреть список заблокированных устройств, выполните следующую команду:*

```
kesl-control -H --get-blocked-hosts
```

Приложение отобразит устройства, заблокированные задачей Защита от шифрования.

kaspersky

Разблокировка заблокированных устройств

Вы можете вручную разблокировать устройства, заблокированные задачей Защита от шифрования, и восстановить сетевой доступ для них.

► *Чтобы разблокировать устройства, выполните следующую команду:*

```
kesl-control [-H] --allow-hosts <устройство>
```

где <устройство> может быть списком действительных адресов IPv4/IPv6 (включая адреса в короткой форме) или подсетей. Таким образом, вы можете указать устройства в виде списка.

Указанные устройства будут разблокированы.

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 - ::
```

kaspersky

Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)

Во время работы задачи Защита от веб-угроз приложение проверяет входящий трафик, предотвращает загрузку вредоносных файлов из интернета, а также блокирует доступ к фишинговым, рекламным и прочим опасным веб-сайтам. Приложение проверяет трафик, передаваемый по протоколам HTTP, HTTPS и FTP. Также выполняется проверка веб-сайтов и IP-адресов. Вы можете указать определенные сетевые порты или диапазоны сетевых портов (см. раздел "Параметры проверки зашифрованных соединений" на стр. 129) для проверки.

Удаление сертификатов приложения может привести к некорректной работе задачи Защита от веб-угроз.

По умолчанию задача Защита от веб-угроз не запущена. При этом задача запустится автоматически, если в системе обнаружен один из перечисленных исполняемых файлов браузеров, в том числе и snap-формата:

- chrome;
- chromium;
- chromium-browser;
- firefox;
- firefox-esr;
- google-chrome;
- opera;
- yandex-browser.

Для проверки HTTPS-трафика вам нужно включить проверку защищенных соединений (см. раздел "Параметры проверки зашифрованных соединений" на стр. 129).
Для проверки FTP-трафика вам нужно задать значение параметра `MonitorNetworkPorts=All` (см. раздел "Параметры проверки зашифрованных соединений" на стр. 129).
Приложение Kaspersky Endpoint Security добавляет в список таблицы mangle утилит iptables и ip6tables специальную разрешающую цепочку правил kesl_bypass, которая позволяет исключать трафик из проверки приложением. Если в цепочке настроены правила исключения трафика, они влияют на работу задачи Защита от веб-угроз.

При открытии веб-сайта задача Защита от веб-угроз 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.
3. Проверяет надежность веб-сайта с помощью репутационных баз "Лаборатории Касперского", если включено использование Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network с помощью командной строки" на стр. 262).

   Рекомендуется включить использование Kaspersky Security Network, чтобы увеличить эффективность работы задачи Защита 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.

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Защита от веб-угроз.

Таблица 22. Параметры задачи Защита от веб-угроз

Параметр	Описание	Значения
ActionOnDetect	Действия, выполняемые при обнаружении зараженного объекта в веб-трафике.	`Notify` – разрешить загрузку обнаруженного объекта, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте. `Block` (значение по умолчанию) – запретить доступ к обнаруженному объекту, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.
CheckMalicious	Показывает, выполняется ли проверка 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	Показывает, выполняется ли проверка 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	Показывает, используется ли эвристический анализ 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.

Параметр	Описание	Значения
CheckAdware	Показывает, выполняется ли проверка 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.
CheckOther	Показывает, будет ли выполняться проверка ссылок на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда устройству или персональным данным.	`Yes` – проверять ссылки на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда устройству или персональным данным. `No` (значение по умолчанию) – не проверять ссылки на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда устройству или персональным данным.
UseTrustedAddresses	Включает или выключает использование списка доверенных веб-адресов. Приложение не анализирует информацию, полученную с доверенных веб-адресов, и не проверяет их на вирусы и другие вредоносные объекты. Доверенные веб-адреса можно указать с помощью параметра `TrustedAddresses.item_#`.	`Yes` (значение по умолчанию) – использовать список доверенных веб-адресов. `No` – не использовать список доверенных веб-адресов.
TrustedAddresses.item_#	Доверенные веб-адреса.	Значение по умолчанию не задано. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается.

kaspersky

Задача Контроль устройств (Device_Control, ID:15)

Во время выполнения задачи Контроль устройств приложение Kaspersky Endpoint Security управляет доступом пользователей к устройствам, которые установлены на клиентском устройстве или подключены к нему (например, жестким дискам, камерам или модулям Wi-Fi). Это позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных.

По умолчанию задача Контроль устройств запускается автоматически при запуске приложения. Если требуется, вы можете остановить (см. раздел "Запуск и остановка задачи" на стр. 123) задачу в любой момент.

Задача Контроль устройств управляет доступом пользователей к устройствам с помощью правил доступа (см. раздел "О правилах доступа" на стр. 210). Вы можете выбрать действие, которое должна выполнять задача Контроль устройств: *применять правила* или *информировать* о запуске устройства, удовлетворяющего правилу.

Задача Контроль устройств управляет доступом на следующих уровнях:

- **Тип устройства**. Например, принтеры, съемные диски, CD/DVD-приводы.
- **Шина подключения**. Шина подключения – это интерфейс, используемый для подключения устройств к клиентскому устройству (USB или FireWire).
- **Доверенные устройства**. *Доверенные устройства* – это устройства, к которым у пользователей есть полный доступ.

  Вы можете добавить устройства в список доверенных по идентификатору устройства. У каждого устройства есть уникальный идентификатор `DeviceId`. Вы можете посмотреть идентификаторы подключенных устройств (см. раздел "Просмотр списка подключенных устройств" на стр. 219), выполнив команду `kesl-control --get-device-list` (см. раздел "Просмотр списка подключенных устройств" на стр. 219).

При первом запуске задачи для всех обнаруженных устройств с известным типом устройства или шины формируется событие *DeviceAllowed*, а при следующих запусках повторные события для этих устройств не формируются, если не было изменений в параметрах задачи для этих устройств.

При остановке выполнения задачи Контроль устройств приложение разблокирует доступ к заблокированным устройствам.

Если в общих параметрах приложения (см. раздел "Описание общих параметров приложения" на стр. 106) для параметра `InterceptorProtectionMode` указано значение `Notify`, то невозможно заблокировать доступ к устройствам с помощью расписания доступа для устройств (секция `[Schedules.item_#]` (см. раздел "Параметры задачи Контроль устройств" на стр. 211)).

Kaspersky Endpoint Security игнорирует исключенные точки монтирования (см. раздел "Описание общих параметров приложения" на стр. 106) для задачи Контроль устройств. Правила доступа применяются к устройству, смонтированному в глобальной исключенной точке монтирования.

kaspersky

В этом разделе

О правилах доступа

Правило доступа к устройству – это параметр, определяющий какие пользователи и в какое время могут получить доступ к устройствам, установленным на клиентском устройстве или подключенным к нему.

Для каждого типа устройств можно указать следующие режимы доступа: *Allow*, *Block* или *DependsOnBus*. Если указано значение *DependsOnBus*, доступ к устройству определяется правилом доступа к шине подключения.

Для некоторых типов устройств вы можете также указать режим доступа *ByRule*, который означает, что доступ к устройству определяется настроенным правилом доступа. Если при попытке совершить операцию с устройством, для которого установлен режим доступа *ByRule*, не нашлось правила, активного на момент доступа, то операция будет запрещена.

Правило доступа к шине подключения разрешает или запрещает доступ к шине подключения (USB или FireWire). Для каждой шины подключения можно указать следующие режимы доступа: *Allow* или *Block*. Например, можно разрешить или запретить подключение всех устройств по USB. Также вы можете разрешить доступ к конкретным USB-устройствам или только к USB-накопителям, при этом доступ к остальным USB-устройства будет запрещен.

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 нужного 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*`

По умолчанию, правила доступа к устройствам создаются для всех типов устройств по классификации компонента Контроль устройств. Такие правила предоставляют пользователям полный доступ к устройствам, если разрешен доступ к шинам подключения для соответствующих типов устройств.

Вы можете изменять (см. раздел "Параметры задачи Контроль устройств" на стр. 211) правила доступа к устройствам и правила доступа к шинам подключения.

kaspersky

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 23. Параметры задачи Контроль устройств

Параметр	Описание	Значения
RulesAction	Действие, выполняемое приложением при попытке доступа к устройству, запрещенному правилами доступа (см. раздел "О правилах доступа" на стр. 210).	`ApplyRules` (значение по умолчанию) – приложение применяет правила доступа и выполняет заданное в правилах действие. `TestRules` – приложение тестирует правила, разрешает доступ и формирует событие об обнаружении устройства, удовлетворяющего правилу.
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 жестким дискам зависит от правила доступа к шине подключения. `Block` – пользователям запрещен доступ ко всем жестким дискам (за исключением системных жестких дисков, которые задача 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 съемным дискам зависит от правила доступа к шине подключения. `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 дискетам зависит от правила доступа к шине подключения. `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-приводам зависит от правила доступа к шине подключения. `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 устройствам, подключенным через последовательный порт, зависит от правила доступа к шине 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 устройствам, подключенным через параллельный порт, зависит от правила доступа к шине 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 принтерам зависит от правила доступа к шине подключения. `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 модемам зависит от правила доступа к шине подключения. `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 стримерам зависит от правила доступа к шине подключения. `Block` – пользователям запрещен доступ к стримерам.
MultifuncDevice	Режим доступа к мультифункциональным устройствам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к мультифункциональным устройствам. `DependsOnBus` (значение по умолчанию) – доступ к мультифункциональным устройствам зависит от правила доступа к шине подключения. `Block` – пользователям запрещен доступ к мультифункциональным 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 устройствам чтения смарт-карт зависит от правила доступа к шине подключения `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-адаптерам зависит от правила доступа к шине 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 внешним сетевым адаптерам зависит от правила доступа к шине подключения. 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 портативным устройствам зависит от правила доступа к шине подключения. `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-устройствам зависит от правила доступа к шине подключения. `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 устройствам обработки изображений зависит от правила доступа к шине подключения. `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 звуковым адаптерам зависит от правила доступа к шине подключения. `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 устройствам ввода зависит от правила доступа к шине подключения. `Block` – пользователям запрещен доступ к устройствам ввода.
Секция **[DeviceBus]** содержит правила доступа к шине подключения, определяющие, разрешено или запрещено подключение устройств.		
USB	Правила доступа к шине подключения 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	Правила доступа к шине подключения 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, доступ к которым не будет ограничен правилами из секций [DeviceClass] и [DeviceBus].		
DeviceId	Идентификатор или маска идентификатора доверенного устройства.	Вы можете использовать маски * (любая последовательность символов) или ? (один любой символ), чтобы указать идентификатор устройства.
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: `Default`. Расписание `Default` обеспечивает полный доступ к устройствам для всех пользователей в любое время, если для соответствующего типа устройства разрешен доступ по шине подключения. Расписание `Default` 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:
		`[Schedules.item_0001]`
		`ScheduleName=schedule_1`
		`DaysHours=Su-Sa:0..11,12..15,16..24`
		Расписание schedule_2, действующее по четвергам с 12 до 14 и по пятницам с 2 до 15 и с 16 до 24:
		`[Schedules.item_0002]`
		`ScheduleName=schedule_2`
		`DaysHours=Th:12..14;Fr:2..15,16..24`
		Расписание schedule_3, действующее 24 часа 7 дней в неделю:
		`[Schedules.item_0003]`
		`ScheduleName=schedule_3`
		`DaysHours=All`

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.		
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.

Параметр	Описание	Значения
[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.
[RemovableDrive Principals.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 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.		

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.
[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.	—
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.

kaspersky

Просмотр списка подключенных устройств

Только пользователи с ролями admin и audit могут просматривать список подключенных устройств.

► *Чтобы просмотреть список подключенных устройств, выполните следующую команду:*

```
kesl-control [-D] --get-device-list
```

Kaspersky Endpoint Security отобразит следующую информацию о подключенных устройствах:

- **Класс**. Класс 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.

kaspersky

Задача Проверка съемных дисков (Removable_Drives_Scan, ID:16)

Во время работы задачи Проверка съемных дисков приложение проверяет подключенное устройство и его загрузочные секторы на вирусы и другие вредоносные программы. Выполняется проверка следующих съемных дисков: CD/DVD-приводов, Blu-ray дисков, флеш-накопителей (включая USB-модемы), внешних жестких дисков и дискет. Если запущена задача Проверка съемных дисков, приложение контролирует подключение съемных дисков к устройству. При подключении съемного диска приложение создает и запускает временную задачу Scan_Boot_Sectors с типом ODS (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118) с параметром `ScanBootSectors=yes` (см. раздел "Задача Выборочная проверка (Scan_File, ID:3) " на стр. 156). Эту задачу остановить невозможно. После завершения выполнения задачи приложение автоматически ее удаляет.

Если вы настроили проверку файлов, приложение также запускает одну или несколько пользовательских задач Scan_File с типом ODS (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118) с параметром `ScanFiles=yes` (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 156). Если требуется, пользователь с правами администратора может остановить выполнение этой задачи.

При изменении параметров задачи Проверка съемных дисков, новые значения не применяются к уже запущенным задачам Scan_Boot_Sectors и Scan_File. При остановке задачи Проверка съемных дисков уже запущенные задачи Scan_Boot_Sectors и Scan_File не останавливаются.

По умолчанию задача Проверка съемных дисков не запущена. Если требуется, вы можете запустить или остановить (см. раздел "Запуск и остановка задачи" на стр. 123) задачу в любой момент.

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Проверка съемных дисков.

Таблица 24. 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. описание параметра `ScanOpticalDrives`). 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.	`DetailedScan` – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При детализированной проверке используются параметры по умолчанию для задачи Выборочная проверка (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 156). `QuickScan` – проверять только файлы определенных типов на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При быстрой проверке используются параметры по умолчанию для задачи Защита от файловых угроз (см. раздел "Параметры задачи Защита от файловых угроз" на стр. 134). `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. 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.	`DetailedScan` – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. При детализированной проверке используются параметры по умолчанию для задачи Выборочная проверка (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 156). `QuickScan` – проверять только файлы определенных типов на CD/DVD-приводах и Blu-ray дисках. При быстрой проверке используются параметры по умолчанию для задачи Защита от файловых угроз (см. раздел "Параметры задачи Защита от файловых угроз" на стр. 134). `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.

kaspersky

Задача Защита от сетевых угроз (Network_Threat_Protection, ID:17)

Во время работы задачи Защита от сетевых угроз приложение проверяет входящий сетевой трафик на действия, характерные для сетевых атак. Приложение проверяет входящий трафик для TCP-портов, номера которых Kaspersky Endpoint Security получает из актуальных баз приложения (см. раздел "Задача Обновление (Update, ID:6)" на стр. 172). При запуске задачи текущие соединения для перехватываемых TCP-портов будут сброшены.

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.

При обнаружении попытки сетевой атаки, нацеленной на ваше устройство, приложение блокирует сетевую активность со стороны атакующего устройства и записывает в журнал соответствующее событие. Приложение блокирует сетевой трафик со стороны атакующего устройства на один час. Вы можете изменить продолжительность блокировки в параметрах задачи.

Приложение Kaspersky Endpoint Security добавляет в список таблицы mangle утилит iptables и ip6tables специальную разрешающую цепочку правил kesl_bypass, которая позволяет исключать трафик из проверки приложением. Если в цепочке настроены правила исключения трафика, они влияют на работу задачи Защита от сетевых угроз.

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Защита от сетевых угроз.

Таблица 25. Параметры задачи Защита от сетевых угроз

Параметр	Описание	Значения
ActionOnDetect	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак.	`Notify` – разрешить сетевую активность, записать в журнал информацию об обнаруженной сетевой активности. `Block` (значение по умолчанию) – заблокировать сетевую активность и записать в журнал информацию об этом.
BlockAttackingHosts	Блокировка сетевой активности со стороны атакующих устройств.	`Yes` (значение по умолчанию) – запретить сетевую активность со стороны атакующего устройства. `No` – разрешить сетевую активность со стороны атакующего устройства.

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 данные о вредоносной активности со стороны этих устройств. Вы можете добавить IP-адреса в список исключений с помощью параметра `ExcludeIPs.item_#`. По умолчанию список пуст.	`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.	`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 не задано.

kaspersky

Задача Проверка контейнеров (Container_Scan, ID:18)

Во время работы задачи Проверка контейнеров приложение Kaspersky Endpoint Security проверяет контейнеры и образы на наличие вирусов и других вредоносных программ. Вы можете одновременно запустить несколько задач Проверка контейнеров.

Поддерживается интеграция с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Для использования задачи требуется лицензия, которая включает эту функцию.

В этом разделе

Параметры задачи Проверка контейнеров

В таблице описаны все доступные значения и значения по умолчанию для всех параметров проверки контейнеров и образов.

Таблица 26. 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.

Параметр	Описание	Значения

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 тега 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.

В таблице ниже описаны параметры, которые применяются к объектам внутри контейнеров и образов.

Таблица 27. 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.

Параметр	Описание	Значения
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.
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 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 Endpoint Security сразу удаляет троянские программы, 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: `Recommended`.
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	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_#`.

Параметр	Описание	Значения

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_#`.

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 веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

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.
ReportUnprocessed Objects	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. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.

Интеграция с Jenkins

Приложение Kaspersky Endpoint Security 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 Endpoint Security с Jenkins:*

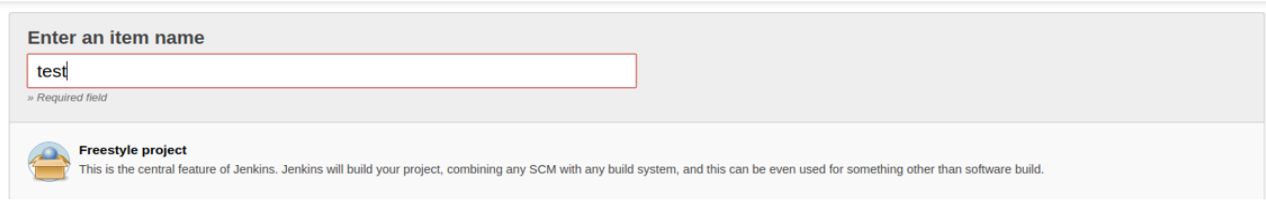
1. Установите Kaspersky Endpoint Security на узле Jenkins.
2. Установите Docker Engine на узле Jenkins.

   Дополнительная информация приведена в документации Docker Engine (https://docs.docker.com/install/).
3. Предоставьте пользователю Jenkins права администратора приложения Kaspersky Endpoint Security:

   ```
   kesl-control --grant-role admin <имя пользователя Jenkins>
   ```
4. Добавьте пользователя Jenkins в группу docker:

   ```
   sudo usermod -aG docker <имя пользователя Jenkins>
   ```

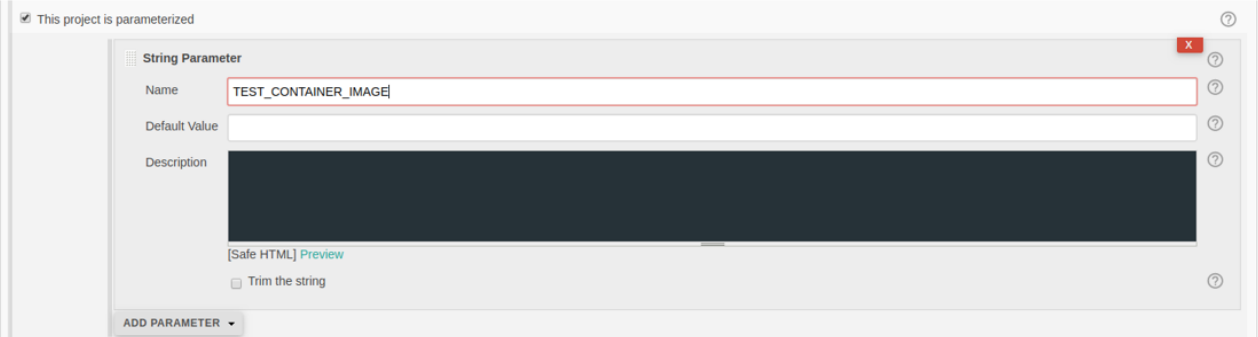
   Обычно используется имя jenkins.
5. В Jenkins создайте новое задание на сборку с названием `test` (**New Item** → **Enter an item name**).

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/kesl_cs_info для дальнейшей проверки:

   ```
   TMP_FILE="/tmp/kesl_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}
```



8. 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/kesl_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=$(kesl-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/kesl/bin/kesl-control --scan-container ${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. Сохраните задание на сборку.

kaspersky

Задача Выборочная проверка контейнеров (Custom_Container_Scan, ID:19)

Задача Выборочная проверка контейнеров используется для хранения значений параметров, которые применяются при выполнении команды `kesl-control --scan-container`.

Для использования задачи требуется лицензия, которая включает эту функцию.

При запуске задачи Выборочная проверка контейнеров приложение создает временную задачу Проверка контейнеров (см. раздел "Задача Проверка контейнеров (Container_Scan, ID:18)" на стр. 224) (с типом ContainerScan (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118)) с параметрами задачи Custom_Container_Scan. Вы можете изменить значения параметров задачи Custom_Container_Scan из командной строки. После завершения проверки задача Custom_Container_Scan автоматически удаляется. Вы не можете удалить задачу Выборочная проверка контейнеров.

► *Чтобы запустить задачу Выборочная проверка контейнеров, выполните следующую команду:*

```
kesl-control --scan-container <идентификатор контейнера или образа|имя контейнера|имя образа[:тег]>
```

Если существует несколько элементов с одинаковым именем, приложение проверяет их все.

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.

При создании задачи Выборочная проверка контейнеров с помощью команды `kesl-control --create-task <название задачи> --type ContainerScan` приложение использует те же значения параметров, что и для задачи Проверка контейнеров (Container_Scan) (см. раздел "Задача Проверка контейнеров (Container_Scan, ID:18)" на стр. 224).

Примеры:

Проверка контейнера с именем my_container:

```
kesl-control --scan-container my_container
```

Проверка образа с именем my_image (все теги):

```
kesl-control --scan-container my_image*
```

В таблице описаны все доступные значения и значения по умолчанию для всех параметров проверки контейнеров и образов.

Таблица 28. Параметры задачи Выборочная 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.

Параметр	Описание	Значения

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 тега 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.
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.

В таблице ниже описаны параметры, которые применяются к объектам внутри контейнеров и образов.

Таблица 29. Параметры задачи Выборочная 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.
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 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, приложение сразу удаляет троянские программы, 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: `Recommended`.
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	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_#`.

Параметр	Описание	Значения

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_#`.

ExcludeThreats.item_#	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значение 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 веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/.
		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
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.
ReportUnprocessed Objects	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.

Параметр	Описание	Значения
UseIChecker	Включение использования технологии iChecker. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.

kaspersky

Задача Анализ поведения (Behavior_Detection, ID:20)

Задача Анализ поведения контролирует вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности Kaspersky Endpoint Security может завершать процесс приложения, осуществляющего вредоносную активность.

Если включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response, исключения по процессам не применяются.

По умолчанию задача Анализ поведения запускается автоматически при запуске приложения. Если требуется, вы можете остановить (см. раздел "Запуск и остановка задачи" на стр. 123) задачу в любой момент.

Таблица 30. Параметры задачи Анализ поведения

Параметр	Описание	Значения
TaskMode	Действие, выполняемое приложением при обнаружении вредоносной активности в операционной системе.	`Block` (значение по умолчанию) – завершать процесс приложения, осуществляющего вредоносную активность. `Notify` – 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 Endpoint Security 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.	

kaspersky

Задача Контроль приложений (Application_Control, ID:21)

Во время выполнения задачи Контроль приложений приложение Kaspersky Endpoint Security управляет запуском приложений на устройствах пользователей. Это позволяет снизить риск заражения устройства, ограничивая доступ к приложениям. Запуск приложений регулируется с помощью *правил контроля приложений* (см. раздел "*О правилах контроля приложений*" на стр. 244).

Для использования задачи требуется лицензия, которая включает эту функцию.

Задача Контроль приложений может работать в двух режимах:

- *Список запрещенных*. Режим, при котором приложение Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. Этот режим работы задачи Контроль приложений настроен по умолчанию.
- *Список разрешенных*. Режим, при котором приложение Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.

Таким образом, если правила контроля приложений сформированы максимально полно, Kaspersky Endpoint Security 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. 88) может запрещать или разрешать запуск процессов под учетной записью root, используя задачу Контроль приложений.

Для каждого режима работы задачи Контроль приложений вы можете создать отдельные правила (см. раздел "О правилах контроля приложений" на стр. 244), а также выбрать действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения на устройстве пользователя.

Если вы меняете список разрешенных приложений или запрещаете запуск всех приложений и/или приложений, влияющих на работу Kaspersky Endpoint Security, то при изменении параметров задачи с помощью конфигурационного файла (см. раздел "Изменение параметров задачи с помощью конфигурационного файла" на стр. 121) или с помощью командной строки требуется запускать команду `--set-settings` с флагом `--accept`.

Kaspersky Endpoint Security поддерживает следующие интерпретаторы: python, perl, bash, ssh.

Контроль приложений не контролирует запуск скриптов из интерпретаторов, не поддерживаемых приложением Kaspersky Endpoint Security и запуск скриптов, передаваемых интерпретатору не через командную строку. Если запуск интерпретатора разрешен правилами Контроля приложений, то Kaspersky Endpoint Security 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 Endpoint Security блокирует все скрипты, указанные в командной строке интерпретатора. Исключение: cat script.py | python.

В этом разделе

О правилах контроля приложений

Правило контроля приложений представляет собой набор параметров, необходимых для работы задачи Контроль приложений:

- 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 Kaspersky Security Center не поддерживается.

- 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 Endpoint Security применяет или не применяет правило к приложению. В правилах используются включающие и исключающие условия:
  - *Включающие условия*. Kaspersky Endpoint Security применяет правило к приложению, если приложение соответствует хотя бы одному включающему условию.
  - *Исключающие условия*. Kaspersky Endpoint Security не применяет правило к приложению, если приложение соответствует хотя бы одному исключающему 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 (SHA-256) исполняемого файла приложения.

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 значениям критериев, указанных во включающем условии, правило срабатывает. В этом случае Контроль приложений выполняет действие, указанное в правиле. Если параметры приложения соответствуют значениям критериев, указанных в исключающем условии, Контроль приложений не контролирует запуск приложения.

Для каждого режима работы задачи Контроля приложений вам нужно создать отдельные правила, а также выбрать действие, которое задача Контроль приложений должна выполнять при обнаружении попытки запуска приложения.

Правила контроля приложений имеют три *статуса работы*:

- *Включено* – правило включено, Kaspersky Endpoint Security применяет это правило во время работы задачи Контроль приложений.
- *Выключено* – правило выключено и не используется во время работы задачи Контроль приложений.
- *Тест* – Kaspersky Endpoint Security разрешает запуск приложений, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих приложений в отчете.

Статус работы правила имеет более высокий приоритет чем действие, указанное в правиле.

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 31. Параметры задачи Контроль приложений

Параметр	Описание	Значения
AppControlMode	Режим работы задачи Контроль приложений (см. раздел "Задача Контроль приложений (Application_Control, ID:21)" на стр. 243).	`AllowList` – Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. `DenyList` (значение по умолчанию) – Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.
AppControlRulesAction	Действие, выполняемое приложением Kaspersky Endpoint Security (см. раздел "О правилах контроля приложений" на стр. 244) при обнаружении попытки запуска приложения.	`ApplyRules` (значение по умолчанию) – Kaspersky Endpoint Security применяет правила контроля приложений и выполняет заданное в правилах действие. `TestRules` – Kaspersky Endpoint Security тестирует правила и формирует событие об обнаружении приложения, удовлетворяющему правилу.

Параметр	Описание	Значения
Секция **[Categories.item_#]** содержит следующие параметры:		
Name	Название создаваемой категории приложений, для которой будет применяться правило.	
UseIncludes	Использование включающих условий (см. раздел "О правилах контроля приложений" на стр. 244) 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. 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.
IncludeFolders.item_#	Имя директории с исполняемым файлом приложения, на которое срабатывает правило.	Для указания имени директории 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.
IncludeHashes.item_#	Хеш (SHA-256) исполняемого файла, на который срабатывает правило.	

Параметр	Описание	Значения
UseExcludes	Использование исключающих условий (см. раздел "О правилах контроля приложений" на стр. 244) для срабатывания правила.	`Yes` – не применять правило к приложению, если приложение соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию. `No` (значение по умолчанию) – применять правило к приложению, даже если приложение соответствует исключающему условию.
ExcludeFileNames.item_#	Имя исполняемого файла, на которое срабатывает правило.	Для указания имени файла 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.
ExcludeFolders.item_#	Имя директории с исполняемым файлом приложения, на которое срабатывает правило.	Для указания имени директории 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.
ExcludeHashes.item_#	Хеш (SHA-256) исполняемого файла, на который срабатывает правило.	
Секция **[AllowListRules.item_#]** содержит список правил контроля приложений для режима работы `AllowList`. Каждая секция [AllowListRules.item_#] содержит следующие параметры:		

Параметр	Описание	Значения
Description	Описание правила контроля приложений.	
AppControlRuleStatus	Статус работы правила контроля приложений (см. раздел "О правилах контроля приложений" на стр. 244).	`On` (значение по умолчанию) – правило включено, Kaspersky Endpoint Security применяет это правило во время работы задачи Контроль приложений. `Off` – правило не используется во время работы задачи Контроль приложений. `Test` – Kaspersky Endpoint Security разрешает запуск приложений, на которые распространяется действие правила, но фиксирует информацию о запуске этих приложений в отчете.
Category	Название созданной категории приложений, для которой применяется правило. Вы можете указать в качестве категории категорию "Golden Image" (см. раздел "Параметры задачи Инвентаризация" на стр. 251).	
Секция **[AllowListRules.item_#.ACL.item_#]** содержит список пользователей, которым разрешен или запрещен запуск приложений.		
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 `DenyList`. Каждая секция [DenyListRules.item_#] содержит следующие параметры:		
Description	Описание правила контроля приложений.	

Параметр	Описание	Значения
AppControlRuleStatus	Статус работы правила контроля приложений (см. раздел "О правилах контроля приложений" на стр. 244).	`On` (значение по умолчанию) – правило включено, Kaspersky Endpoint Security применяет это правило во время работы задачи Контроль приложений. `Off` – правило не используется во время работы задачи Контроль приложений. `Test` – Kaspersky Endpoint Security разрешает запуск приложений, на которые распространяется действие правила, но фиксирует информацию о запуске этих приложений в отчете.
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. 251).	
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.
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.

Просмотр списка созданных категорий

Вы можете просматривать список созданных категорий приложений.

В списке созданных категорий отображаются следующие категории:

- категории, созданные в Kaspersky Security Center;
- категории, добавленные в параметрах задачи Контроль приложений (см. раздел "Параметры задачи Контроль приложений" на стр. 245) через командную строку;

- категория GoldenImage, созданная с помощью задачи Инвентаризация (см. раздел "Задача Инвентаризация (Inventory_Scan, ID:22)" на стр. 251) (в политике Kaspersky Endpoint Security или через командную строку).

► *Чтобы просмотреть список созданных категорий приложений, выполните следующую команду:*

```
kesl-control [-A] --get-categories
```

Kaspersky Endpoint Security отобразит следующую информацию о категории приложений:

- уникальный идентификатор (GUID) категории;
- название категории;
- описание категории (если есть);
- список условий включения файла или директории с файлами в категорию;
- список условий исключения файла или директории с файлами из категории.

Если в параметрах задачи Контроль приложений (см. раздел "Параметры задачи Контроль приложений" на стр. 245) 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 программ для этих условий будет отображаться исходный путь, на который ссылается символическая ссылка.

kaspersky

Задача Инвентаризация (Inventory_Scan, ID:22)

Задача Инвентаризация позволяет получить информацию обо всех исполняемых файлах приложений, хранящихся на устройствах пользователя. Получение информации о приложениях, установленных на устройствах, может быть полезно, например, для создания правил контроля приложений (см. раздел "О правилах контроля приложений" на стр. 244).

Для использования задачи требуется лицензия, которая включает эту функцию.

В этом разделе

Параметры задачи Инвентаризация

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Инвентаризация.

Таблица 32. 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 pyc).	`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.

Параметр	Описание	Значения
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. 244) 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).
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.

Параметр	Описание	Значения
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

Вы можете просматривать список приложений, обнаруженных на устройстве в результате выполнения задачи Инвентаризация. Получение информации о приложениях, установленных на устройствах, может быть полезно, например, для создания правил контроля приложений (см. раздел "О правилах контроля приложений" на стр. 244).

► *Чтобы просмотреть список приложений, обнаруженных на устройстве, выполните следующую команду:*

```
kesl-control [-A] --get-app-list
```

Kaspersky Endpoint Security 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 (см. раздел "Просмотр списка созданных категорий" на стр. 249) с помощью команды `kesl-control [-A] --get-categories`.

При добавлении новой категории информация о ней в списке приложений автоматически не обновляется. Для обновления списка приложений требуется повторный запуск задачи Инвентаризация.

kaspersky

Задача Интеграция с Kaspersky Endpoint Detection and Response (KATA) (KATAEDR, ID:24)

Приложение Kaspersky Endpoint Security 12.0 поддерживает интеграцию с решением Kaspersky Anti Targeted Attack Platform 6.0. Интеграция Kaspersky Endpoint Security 12.0 с решением Kaspersky Anti Targeted Attack Platform 5.1 не поддерживается.

Kaspersky Endpoint Detection and Response (KATA) (далее также EDR (KATA)) – компонент в составе решения Kaspersky Anti Targeted Attack Platform, которое предназначено для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats (далее также "APT"). Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform https://support.kaspersky.com/help/KATA/5.1/ru-RU/246841.htm.

При взаимодействии с EDR (KATA) приложение Kaspersky Endpoint Security может выполнять следующие функции:

- Отправлять данные о событиях на устройствах (телеметрию) на сервер Kaspersky Anti Targeted Attack Platform с компонентом Central Node (далее также сервер KATA). Приложение Kaspersky Endpoint Security передает на сервер KATA 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 следующие ответные действия, направленные на обеспечение функций безопасности, по командам, полученным от Kaspersky Anti Targeted Attack Platform:
  - Задача Получить файл (Get file task) позволяет получать файлы с устройств пользователей. Например, вы можете настроить получение файла журнала событий, который создает сторонняя программа.
  - Задача Удалить файл (Delete file task) позволяет удаление файла с устройства.
  - Задача Запустить процесс (Run process) позволяет удаленно запускать файлы на устройстве. Например, вы можете удаленно запустить утилиту, которая создает файл с конфигурацией устройства, а затем получить созданный файл с помощью задачи Получить файл.
  - Задача Завершить процесс (Terminate process) позволяет удаленно завершать процессы на устройстве. Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи запуска процесса.
  - Задача Поиск IOC (IOC Scan task) позволяет обнаруживать *индикаторы компрометации* на устройстве и выполнять действия по реагированию на угрозы. Индикатор компрометации (англ. Indicator of Compromise, IOC) – набор данных об объекте или активности, который указывает на несанкционированный доступ к устройству (компрометация данных). Для поиска IOC используются IOC-файлы. 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.
  - Сетевая изоляция устройства позволяет изолировать устройства от сети. Вы можете выключить сетевую изоляцию устройства в случае потери связи с сервером KATA после включения сетевой изоляции.

kaspersky

Ограничения сетевой изоляции

При использовании сетевой изоляции настроятельно рекомендуется ознакомиться с ограничениями, описанными ниже.

Для работоспособности сетевой изоляции требуется, чтобы приложение Kaspersky Endpoint Security было запущено. Во время сбоя в работе приложения Kaspersky Endpoint Security (когда приложение не запущено), блокировка трафика при включении сетевой изоляции решением Kaspersky Anti Targeted Attack Platform 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 Endpoint Security не сможет получить к нему доступ. Это же относится к узлам отказоустойчивого сервера KATA. Не рекомендуется менять их адреса, чтобы приложение Kaspersky Endpoint Security не потеряло с ними связь.

Прокси-сервер также в исключения из сетевой изоляции автоматически не добавляется, поэтому требуется добавить его в исключения вручную, чтобы приложение Kaspersky Endpoint Security не потеряло связь с сервером KATA.

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 и указать Kaspersky Security Center в качестве источника обновлений баз. В случае невозможности использования Kaspersky Security Center в качестве прокси-сервера, настройте параметры нужного прокси-сервера и добавьте его в исключения.

Условия интеграции

Задача Интеграция с Kaspersky Endpoint Detection and Response (KATA) позволяет настроить и включить интеграцию приложения Kaspersky Endpoint Security с компонентом EDR (KATA). Вы также можете управлять интеграцией приложения Kaspersky Endpoint Security с EDR (KATA) с помощью Консоли администрирования Kaspersky Security Center (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response (KATA)" на стр. 341) и Kaspersky Security Center Web Console (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response (KATA)" на стр. 458).

Для интеграции с EDR (KATA) должна быть запущена задача Анализ поведения.

Интеграция приложения Kaspersky Endpoint Security с EDR (KATA) возможна, только если задача Анализ поведения запущена. В противном случае необходимые данные телеметрии не передаются.

Для работы исключений из телеметрии требуется, чтобы интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response была выключена. Если интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response включена, исключения по процессам не применяются.

Дополнительно EDR (KATA) может использовать данные, полученные от следующих задач:

- Защита от файловых угроз.
- Защита от сетевых угроз.
- Защита от веб-угроз.

Безопасность соединения

Во время интеграции с EDR (KATA), устройства с Kaspersky Endpoint Security устанавливают защищенные соединения с сервером KATA по протоколу HTTPS. Для обеспечения безопасности соединения используются следующие сертификаты, выданные сервером KATA:

- Сертификат сервера KATA. Соединение шифруется с помощью TLS-сертификата сервера. Вы можете повысить уровень безопасности соединения, включив проверку сертификата сервера на стороне Kaspersky Endpoint Security. Для этого вам нужно добавить сертификат сервера интеграции перед запуском задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA).
- Сертификат клиента. Этот сертификат используется для дополнительной защиты подключения с помощью двусторонней аутентификации (проверки устройств с Kaspersky Endpoint Security сервером KATA). Один и тот же сертификат клиента может использоваться несколькими устройствами. По умолчанию сервер KATA не выполняет проверку сертификатов клиентов, но двусторонняя аутентификация может быть включена на стороне Kaspersky Anti Targeted Attack Platform. В этом случае вам нужно включить двустороннюю аутентификацию (см. раздел "Параметры задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA)" на стр. 257) в параметрах задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA) и добавить сертификат клиента (см. раздел "Управление сертификатами для подключения к серверам KATA" на стр. 258) (криптоконтейнер с сертификатом и закрытым ключом).

Сертификаты для защиты соединения с сервером KATA предоставляет администратор Kaspersky Anti Targeted Attack Platform.

Для подключения к серверу KATA используется прокси-сервер, если использование прокси-сервера настроено (см. раздел "Описание общих параметров приложения" на стр. 106) в общих параметрах приложения Kaspersky Endpoint Security.

Запись событий

При интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Anti Targeted Attack Platform в журнал systemd может записываться большое количество событий. Если вы хотите отключить запись событий аудита в systemd, вам нужно отключить сокет systemd-journald-audit и перезагрузить операционную систему.

► *Чтобы отключить сокет systemd-journald-audit, выполните следующие команды:*

```
systemctl stop systemd-journald-audit.socket
systemctl disable systemd-journald-audit.socket
systemctl mask systemd-journald-audit.socket
```

В этом разделе

kaspersky

Параметры задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA)

В таблице ниже описаны все доступные параметры и значения по умолчанию для всех параметров, которые вы можете указать для задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA).

Таблица 33. Параметры задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA)

Параметр	Описание	Значение
Address	Адрес сервера KATA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером KATA 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 KATA.	Значение по умолчанию: `443`.
UseClientPinnedCertificate	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу KATA. Если двусторонняя аутентификация включена на стороне сервера KATA, вам нужно включить двустороннюю аутентификацию в параметрах задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA) и добавить сертификат клиента (см. раздел "Управление сертификатами для подключения к серверам KATA" на стр. 258) перед запуском задачи.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу KATA. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
SynchronizationPeriod	Периодичность отправки запросов на синхронизацию на сервер KATA в минутах.	Значение по умолчанию: `5`.
ConnectionTimeout	Максимальное время ожидания соединения с сервером KATA в секундах.	Значение по умолчанию: `10`.
RequestTimeout	Максимальное время ожидания ответа от сервера KATA в секундах.	Значение по умолчанию: `10`.
MaximumDataTransferTime	Максимальная задержка отправки событий на сервер KATA в секундах.	Значение по умолчанию: `30`.

Параметр	Описание	Значение
UseRequestCountLimits	Включение и выключение регулирования количества событий, отправляемых на сервер KATA.	`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 (например, событий изменений в реестре) к общему количеству событий превышает установленное ограничение в процентах.	Значение по умолчанию: `15`.
EnableTelemetry	Включение и выключение отправки данных о событиях на устройствах (телеметрии) на сервер KATA.	`Yes` (значение по умолчанию) – отправлять телеметрию на сервер KATA. `No` – не отправлять телеметрию.

Управление сертификатами для подключения к серверам KATA

Для управления сертификатами требуются root-права.

Вы можете управлять сертификатами, которые используются для подключения к серверам KATA, 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:*

```
kesl-control [-R] --add-kataedr-server-certificate <имя и путь к файлу>
```

где `<имя и путь к файлу>` – имя и путь к файлу, содержащему сертификат сервера.

► *Чтобы добавить или заменить сертификат клиента:*

1. Выполните команду:

   `kesl-control [-R] --add-kataedr-client-certificate <имя и путь к файлу>`

   где `<имя и путь к файлу>` – имя и путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

2. Если криптоконтейнер защищен паролем, введите пароль по запросу.

Сертификат клиента используется для дополнительной защиты соединения с сервером KATA, если в параметрах сервера KATA включена проверка сертификата клиента и в параметрах задачи Интеграция с Kaspersky Anti Targeted Attack Platform для параметра `UseClientPinnedCertificate` установлено значение `yes`.

► *Чтобы вывести информацию о сертификате, выполните следующую команду:*

- для сертификата сервера:

  `kesl-control [-R] --query-kataedr-server-certificate`

- для сертификата клиента:

  `kesl-control [-R] --query-kataedr-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;
- SHA-1 и SHA-256 отпечатки сертификата.

► *Чтобы удалить сертификат сервера, выполните следующую команду:*

`kesl-control [-R] --remove-kataedr-server-certificate`

► *Чтобы удалить сертификат клиента, выполните следующую команду:*

`kesl-control [-R] --remove-kataedr-client-certificate`

Если использование сертификата настроено в параметрах задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA) и задача запущена, удаление этого сертификата завершается с ошибкой.

kaspersky

Использование Kaspersky Security Network

Для повышения эффективности защиты устройств и данных пользователей Kaspersky Endpoint Security 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. Приложение Kaspersky Endpoint Security предлагает включить использование KSN во время установки. Вы можете включить или выключить использование KSN в любой момент.

Инфраструктурные решения Kaspersky Security Network

Kaspersky Endpoint Security 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 Endpoint Security 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 изменения лицензии Kaspersky Endpoint Security для использования KPSN требуется предоставить поставщику услуг информацию о новом 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security

Если приложение Kaspersky Endpoint Security используется в автономном режиме и вы используете KSN в работе приложения, вы можете включать (см. раздел "Включение и выключение использования Kaspersky Security Network с помощью командной строки" на стр. 262) *облачный режим* работы приложения. Если включен облачный режим, Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО.

Kaspersky Endpoint Security 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 Endpoint Security загружает полную версию баз приложения с серверов "Лаборатории Касперского" в ходе очередного обноления баз и модулей приложения.

Включение облачного режима приводит к выходу приложения из сертифицированного состояния.

Работу приложения с облегченными базами вредоносного ПО обеспечивает Kaspersky Security Network. Если вы не используете KSN или облачный режим выключен, Kaspersky Endpoint Security использует полную версию баз приложения. Облачный режим выключается автоматически, если выключено использование KSN.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, работа с облегченными базами вредоносного ПО не поддерживается. Kaspersky Endpoint Security получает от Сервера защиты специальные базы, необходимые для работы Легкого агента.

Использование службы прокси-сервера KSN

Устройства пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN напрямую или при помощи службы прокси-сервера KSN.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, взаимодействие с инфраструктурой KSN обеспечивает служба прокси-сервера KSN. Если прокси-сервер KSN недоступен, KSN не используется в работе приложения.

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 Kaspersky Security Center. Подробнее о прокси-сервере KSN см. в справке Kaspersky Security Center.

В этом разделе

Включение и выключение использования Kaspersky Security Network с помощью командной строки

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 в расширенном режиме, выполните команду:*

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

► *Чтобы включить использование Kaspersky Security Network в стандартном режиме, выполните команду:*

```
kesl-control --set-app-settings UseKSN=Basic --accept-ksn
```

► *Чтобы выключить использование Kaspersky Security Network, выполните команду:*

```
kesl-control --set-app-settings UseKSN=No
```

► *Чтобы включить или выключить использование Kaspersky Security Network с помощью конфигурационного файла, выполните команду:*

```
kesl-control --set-app-settings --file <имя конфигурационного файла> [--accept-ksn]
```

Для включения использования Kaspersky Security Network требуется запускать команду `kesl-control --set-settings` с флагом `--accept-ksn`.

Если приложение Kaspersky Endpoint Security, 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 Endpoint Security, установленное на клиентском устройстве, прекращает работать под управлением политики, параметру присваивается значение `UseKSN=No`.

Файл ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network находится в директории /opt/kaspersky/kesl/doc/.

Проверка подключения к Kaspersky Security Network с помощью командной строки

► *Чтобы проверить подключение к Kaspersky Security Network, выполните следующую команду:*

```
kesl-control --app-info
```

В строке **Использование Kaspersky Security Network** отображается статус подключения к Kaspersky Security Network (см. раздел «Использование Kaspersky Security Network» на стр. 260):

- Если отображается статус `Расширенный режим KSN`, приложение Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 (см. раздел "Включение и выключение использования Kaspersky Security Network с помощью командной строки" на стр. 262).
- Приложение не активировано, или срок действия лицензии истек.
- Выявлены проблемы, связанные с лицензионным ключом. Например, ключ находится в списке запрещенных ключей.

kaspersky

Проверка целостности компонентов приложения

Приложение Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security.

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 приложения. Имя файла манифеста для каждого компонента одно и тоже, но содержимое файлов манифестов различается. Файлы манифеста подписаны цифровой подписью, их целостность также проверяется.

Проверка целостности компонентов приложения выполняется с помощью утилиты проверки целостности integrity_checker.

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/kesl/bin/integrity_checker;
- для проверки плагина управления Kaspersky Endpoint Security – в директории, где расположены исполняемые модули (DLL) плагина управления:
  - C:\Program Files\Kaspersky Lab\Kaspersky Security Center\Plugins\<версия плагина>.linux.plg\integrity_checker.exe – для 32-битных операционных систем;

- C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\Plugins\<версия плагина>.linux.plg\integrity_checker.exe – для 64-битных операционных систем.

Файлы манифеста расположены по следующим путям:

- /opt/kaspersky/kesl/bin/integrity_check.xml – для проверки целостности пакета приложения;
- /opt/kaspersky/kesl/bin/gui_integrity_check.xml – для проверки целостности пакета графического пользовательского интерфейса;
- /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – для проверки Агента администрирования для 32-битных операционных систем;
- /opt/kaspersky/klnagent64/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 Endpoint Security 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 Endpoint Security формирует событие *IntegrityCheckFailed* в журнале событий и в Kaspersky Security Center.

kaspersky

События и отчеты

В процессе работы приложения возникают различного рода *события* (см. раздел "*Просмотр событий*" на стр. 267). 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 некоторого компонента, которую требуется устранить.

На основе событий, происходящих во время работы приложения, приложение формирует различные типы *отчетов* (см. раздел "*Просмотр отчетов*" на стр. 270).

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 задачей Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 200);
- IP-адреса отправителей и получателей сетевых пакетов, проверяемых задачей Управление сетевым экраном;
- веб-адреса источников обновлений (см. раздел "Об источниках обновлений" на стр. 173);
- общие параметры приложения (см. раздел "Описание общих параметров приложения" на стр. 106);
- названия и параметры задач (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118);
- обнаруженные вредоносные, фишинговые, рекламные веб-адреса и веб-адреса, содержащие легальные программы, которые могут использоваться злоумышленниками для нанесения вреда устройству или персональным данным;
- названия контейнеров и образов;
- пути к контейнерам и образам;
- названия и идентификаторы устройств;
- веб-адреса репозиториев;
- имена файлов, пути к файлам и хеш-суммы исполняемых файлов приложений;
- названия категорий приложений.

В этом разделе

Просмотр событий

Вы можете просматривать события следующими способами:

- В журнале событий приложения. Журнал событий расположен в директории, указанной общим параметром приложения (см. раздел "Описание общих параметров приложения" на стр. 106)

EventsStoragePath. По умолчанию приложение сохраняет информацию о событиях в базе данных /var/opt/kaspersky/kesl/private/storage/events.db. Для доступа к базе данных событий требуются root-права.

- Если в общих параметрах приложения (см. раздел "Описание общих параметров приложения" на стр. 106) для параметра UseSysLog указано значение Yes, то данные о событиях также записываются в syslog. Для доступа к syslog требуются root-права.
- Включить вывод текущих событий (см. раздел "Включение вывода событий" на стр. 95) приложения с помощью команды kesl-control -W.
- Если управление приложением Kaspersky Endpoint Security осуществляется с помощью Kaspersky Security Center, данные о событиях могут передаваться на Сервер администрирования.

  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. Администратор может настроить выполнение скрипта при получении события из приложения или получение уведомлений о событиях по электронной почте. Подробную информацию о событиях см. в документации Kaspersky Security Center.
- Если включен графический пользовательский интерфейс (GUI), информация о событиях отображается в отчетах (см. раздел "Просмотр отчетов" на стр. 505) и во всплывающих окнах приложения.

► *Чтобы получить информацию обо всех событиях в журнале событий, выполните следующую команду:*

```
kesl-control -E --query|less
```

По умолчанию в приложении хранится до 500 000 событий. С помощью утилиты less вы можете перемещаться по списку отображаемых событий.

Вы можете просматривать конкретные события с помощью системы запросов (см. раздел "Использование фильтра для ограничения результатов запроса" на стр. 103) к хранилищу событий приложения. При создании запроса требуется указать нужное поле, выбрать операцию сравнения и задать нужное значение. Значение требуется указывать в одинарных кавычках (‘), а запрос целиком – в двойных кавычках (").

```
--query "<поле> <операция сравнения> '<значение>' [and <поле> <операция сравнения> '<значение>' *]"
```

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.

kaspersky

Пример события ThreatDetected:

```
EventType=ThreatDetected
EventId=2671
Initiator=Product
Date=2020-04-30 17:17:17
DangerLevel=Critical
FileName=/root/eicar.com.txt
ObjectName=File
TaskName=File_Monitoring
RuntimeTaskId=2
TaskId=1
DetectName=EICAR-Test-File
TaskType=OAS
FileOwner=root
FileOwnerId=0
DetectCertainty=Sure
DetectType=Virware
DetectSource=Local
ObjectId=1
AccessUser=root
AccessUserId=0
```

Примеры запросов:

Вывести все события с заданным значением поля EventType:

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

Вывести все события с заданными значениями полей EventType и FileName:

```
kesl-control -E --query "EventType == 'ThreatDetected' and FileName like '%eicar%'"
```

Вывести все события, сформированные задачей File_Threat_Protection после даты, указанной в системе отметок времени UNIX™ (количество секунд, прошедших с 00:00:00 (UTC), 1 января 1970 года):

```
kesl-control -E --query "TaskName == 'File_Threat_Protection' and Date >
'1588253494'"
```

Вывести все события, сформированные задачей File_Threat_Protection после даты, указанной в формате YYYY-MM-DD hh:mm:ss:

```
kesl-control -E --query "TaskName == 'File_Threat_Protection' and Date > '2022-11-
22 18:42:54'"
```

Просмотр отчетов

Информация о работе каждого компонента приложения Kaspersky Endpoint Security, результаты выполнения каждой задачи и работы всего приложения в целом записываются в отчеты.

Вы можете просматривать отчеты следующими способами:

- Если управление приложением Kaspersky Endpoint Security осуществляется с помощью Kaspersky Security Center, вы можете формировать и просматривать отчеты Kaspersky Security Center в Консоли администрирования и в Web Console. С помощью отчетов Kaspersky Security Center вы можете, например, получить сведения о зараженных файлах, использовании ключей и баз приложения. Подробную информацию о работе с отчетами Kaspersky Security Center см. в документации Kaspersky Security Center.
- Если включен графический пользовательский интерфейс (GUI), информация о событиях в работе приложения отображается в отчетах приложения (см. раздел "Просмотр отчетов" на стр. 505).

kaspersky

Управление приложением с помощью Консоли администрирования

Этот раздел содержит информацию об управлении приложением Kaspersky Endpoint Security с помощью Консоли администрирования Kaspersky Security Center.

Описание приведено для версии Kaspersky Security Center 14.2.

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.

Консоль администрирования позволяет удаленно устанавливать и удалять, запускать и останавливать приложение Kaspersky Endpoint Security, настраивать параметры работы приложения и запускать задачи на управляемых устройствах.

Управление приложением через Консоль администрирования осуществляется с помощью mmc-плагина управления Kaspersky Endpoint Security.

Чтобы управлять через Консоль администрирования работой приложения Kaspersky Endpoint Security, 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 Endpoint Security и настроить правила автоматического перемещения устройств в группы администрирования. Или вы можете вручную переместить устройства из папки **Нераспределенные устройства** в группы администрирования после установки приложения Kaspersky Endpoint Security (см. подробнее в документации Kaspersky Security Center).

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

- просматривать состояние защиты устройств (см. раздел "Просмотр состояния защиты устройства" на стр. 273);
- просматривать общие параметры приложения;
- обновлять базы и модули приложения;
- управлять политиками;
- управлять задачами приложения.

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. Кроме того, настройка некоторых параметров не поддерживается в KESL-контейнере.

kaspersky

В этом разделе

Запуск и остановка приложения на клиентском устройстве

► *Чтобы запустить или остановить приложение на клиентском устройстве:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
3. В рабочей области выберите закладку **Устройства**.
4. В списке управляемых устройств выберите устройство, на котором вы хотите запустить или остановить приложение, и в контекстном меню устройства выберите пункт **Свойства**.
5. В окне **Свойства: <Имя устройства>** выберите раздел **Программы**.

   В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.
6. Выберите приложение Kaspersky Endpoint Security 12.0 для Linux.
7. Выполните одно из следующих действий:

   a. Если вы хотите запустить приложение, нажмите на кнопку  справа от списка приложений "Лаборатории Касперского" или в контекстном меню приложения выберите пункт **Запустить**.

   b. Если вы хотите остановить работу приложения, нажмите на кнопку  справа от списка приложений "Лаборатории Касперского" или в контекстном меню приложения выберите пункт **Остановить**.

kaspersky

Просмотр состояния защиты устройства

► *Чтобы просмотреть состояние защиты устройства:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
3. В рабочей области выберите закладку **Устройства**.
4. В списке управляемых устройств выберите нужное вам устройство и в контекстном меню устройства выберите пункт **Свойства**.
5. В окне **Свойства: <Имя устройства>** выберите раздел **Защита**.

В разделе **Защита** отображается следующая информация о защищаемом устройстве:

- **Статус устройства** – статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на устройстве и активности устройства в сети.
- **Все проблемы** – полный список проблем, обнаруженных управляемыми приложениями, установленными на клиентском устройстве. Каждая проблема имеет статус, который приложение предлагает вам назначить устройству.
- **Статус постоянной защиты** – текущий статус задачи Защита от файловых угроз, например, *Выполняется* или *Остановлена*. При изменении статуса устройства новый статус отображается в окне свойств устройства только после синхронизации клиентского устройства с Сервером администрирования.
- **Последняя проверка по требованию** – дата и время выполнения последнего поиска вредоносного ПО на клиентском устройстве.
- **Всего обнаружено угроз** – общее количество угроз, обнаруженных на клиентском 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 клиентском устройстве.

Просмотр параметров приложения

► *Чтобы просмотреть параметры приложения:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
3. В рабочей области выберите закладку **Устройства**.
4. В списке управляемых устройств выберите нужное вам устройство и в контекстном меню устройства выберите пункт **Свойства**.
5. В окне **Свойства: <Имя устройства>** выберите раздел **Программы**.

   В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.

6. Выберите приложение Kaspersky Endpoint Security 12.0 для Linux.
7. Нажмите на кнопку **Свойства** под списком приложений или в контекстном меню приложения выберите пункт **Свойства**.

   Откроется окно **Параметры Kaspersky Endpoint Security 12.0 для Linux**.

В окне **Параметры Kaspersky Endpoint Security 12.0 для Linux** отображается следующая информация о Kaspersky Endpoint Security:

- В разделе **Общие** содержится общая информация об установленном приложении:
  - **Номер версии** – номер версии приложения.
  - **Установлено** – дата и время установки приложения на защищаемом устройстве.
  - **Текущее состояние** – состояние задачи Защита от файловых угроз, например: *Выполняется* или *Приостановлена*.
  - **Последнее обновление ПО** – дата и время последнего обновления модулей приложения Kaspersky Endpoint Security.
  - **Установленные обновления** – список модулей, для которых установлены обновления.
  - **Базы программы** – дата и время создания и последнего 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 строке **Режим Легкого агента для защиты виртуальных сред** вы можете посмотреть информацию о режиме использования приложения (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23):
  - статус *выполняется* означает, что приложение используется в режиме Легкого агента;
  - статус *не установлено* означает, что приложение используется в автономном режиме.
- В разделе **Лицензионные ключи** приведена информация об активном и резервном 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.
  - **Срока 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.

kaspersky

Обновление баз и модулей приложения

Процедура обновления баз и модулей Kaspersky Endpoint Security зависит от режима использования приложения (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23). В этом разделе описана процедура обновления приложения в автономном режиме. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается обновление баз и модулей приложения с помощью задачи, созданной в Kaspersky Security Center. Обновление выполняется с помощью локальной предустановленной задачи.

Обновление баз и модулей приложения Kaspersky Endpoint Security 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 Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы приложения.

На устройствах пользователей обновляются 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.
- 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.

  Допускается устанавливать только обновления модулей приложения, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу приложения из сертифицированного состояния.

Приложение Kaspersky Endpoint Security поддерживает следующие схемы обновления баз и модулей:

- Обновление с серверов "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 Kaspersky Endpoint Security переключается к следующему серверу.
- 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.

     Загрузку пакета обновлений в хранилище 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 Endpoint Security *Обновление* (на стр. 361). Вы можете создать неограниченное количество задач обновления для каждой из групп администрирования.

По умолчанию список источников обновлений содержит серверы обновлений "Лаборатории Касперского" и Сервер администрирования Kaspersky Security Center. Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений вы можете указывать FTP-, HTTP- или HTTPS-серверы.

Если обновление не может быть выполнено с одного источника обновлений, приложение Kaspersky Endpoint Security переключается к следующему источнику.

Загрузка обновлений с серверов обновлений "Лаборатории Касперского" или с других FTP-, HTTP- или HTTPS-серверов осуществляется по стандартным сетевым протоколам. Если для доступа к источникам обновлений требуется подключение к прокси-серверу, укажите параметры прокси-сервера (на стр. 330) в параметрах политики Kaspersky Endpoint Security.

В этом разделе

Обновление из хранилища Сервера администрирования

Для экономии интернет-трафика вы можете настроить обновление баз и модулей приложения на устройствах локальной сети организации из серверного хранилища. Для этого требуется настроить в Kaspersky Security Center загрузку пакета обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования. В этом случае остальные устройства локальной сети организации смогут получать пакет обновлений из серверного хранилища.

Настройка обновления баз и модулей приложения из серверного хранилища состоит из следующих этапов:

1. Загрузка баз и модулей приложения в хранилище Сервера администрирования с помощью задачи Kaspersky Security Center *Загрузка обновлений в хранилище Сервера администрирования*.
2. Настройка обновления баз и модулей приложения из хранилища Сервера администрирования на остальных клиентских устройствах с помощью задачи *Обновление* (см. раздел "*Обновление*" на стр. 361).

► *Чтобы настроить обновление баз и модулей приложения из хранилища* Сервера администрирования*:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Задачи**.

   В рабочей области в правой части окна отобразится список задач.
3. В списке задач выберите задачу **Обновление** (на стр. 361) приложения Kaspersky Endpoint Security и откройте окно свойств задачи двойным щелчком мыши.

   Задача *Обновление* создается автоматически мастером первоначальной настройки.
4. В окне свойств задачи в списке слева выберите раздел **Источники обновлений**.

   В правой части окна отобразятся параметры задачи.
5. В блоке **Источник обновлений баз** выберите вариант **Сервер администрирования Kaspersky Security Center**.
6. Установите флажок **Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны**, если вы хотите, чтобы в случае недоступности хранилища Сервера администрирования задача Обновление использовала серверы обновлений "Лаборатории Касперского".
7. Нажмите на кнопку **Применить**.

kaspersky

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 серверов обновлений "Лаборатории Касперского" и копировать полученные пакеты обновлений в общую директорию с помощью утилиты. В этом случае остальные устройства локальной сети организации смогут получать пакет обновлений из общей директории.

Настройка обновления баз и модулей приложения из общей директории состоит из следующих этапов:

1. Установка Kaspersky Update Utility на одном из устройств локальной сети организации.
2. Настройка копирования пакета обновлений в общую директорию в параметрах Kaspersky Update Utility.
3. Настройка обновления баз и модулей приложения из указанной общей директории на остальных устройствах локальной сети организации.

Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта службы технической поддержки "Лаборатории Касперского" https://support.kaspersky.ru/updater3. После установки утилиты 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.

► *Чтобы настроить обновление из общей директории:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Задачи**.

   В рабочей области в правой части окна отобразится список задач.
3. В списке задач выберите задачу **Обновление** приложения Kaspersky Endpoint Security и откройте окно свойств задачи двойным щелчком мыши.

   Задача *Обновление* создается автоматически мастером первоначальной настройки.
4. В окне свойств задачи выберите раздел **Источники обновлений**.

   В правой части окна отобразятся параметры задачи.
5. В блоке **Источник обновлений баз** выберите вариант **Другие источники в локальной или глобальной сети**.
6. В таблице источников обновлений нажмите на кнопку **Добавить**.
7. В поле **Источник обновлений** укажите путь к общей директории.

   Адрес источника должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.
8. Установите флажок **Использовать этот источник** и нажмите на кнопку **ОК**.
9. В таблице источников обновлений настройте порядок их использования с помощью кнопок **Вверх** и **Вниз**.
10. Нажмите на кнопку **Применить**.

kaspersky

Использование прокси-сервера при обновлении

Для загрузки обновлений баз и модулей приложения из источника обновлений может потребоваться указать параметры прокси-сервера. Если источников обновлений несколько, параметры прокси-сервера применяются для всех источников. Если для некоторых источников обновлений прокси-сервер не нужен, вы можете выключить использование прокси-сервера в параметрах политики Kaspersky Endpoint Security. Приложение также будет использовать прокси-сервер для доступа к Kaspersky Security Network и серверам активации.

► *Чтобы включить использование прокси-сервера для определенной группы администрирования:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием нужной группы администрирования, на устройствах которой вы хотите выключить использование прокси-сервера.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и в контекстном меню политики выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название политики>**.
5. Выберите раздел **Общие параметры** → **Параметры прокси-сервера** (на стр. 448).
6. В блоке **Параметры прокси-сервера** выберите вариант **Использовать параметры указанного прокси-сервера** и укажите параметры нужного прокси-сервера.
7. Нажмите на кнопку **ОК**.

Управление политиками в Консоли администрирования

Политика – это набор параметров работы приложения Kaspersky Endpoint Security, которые применяются для группы администрирования. С помощью политик вы можете установить одинаковые значения параметров работы приложения Kaspersky Endpoint Security 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 (см. раздел "Создание политики" на стр. 279) 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.

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

- Если параметр закрыт "замком" (), это означает, что вы не можете изменить значение параметра. Для всех клиентских устройств группы администрирования используется значение параметра, заданное политикой.
- Если параметр не закрыт "замком" (), это означает, что вы можете изменить значение параметра. Для всех клиентских устройств группы администрирования используются значения параметра, заданные локально. Значение параметра, заданное в политике, не применяется.

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

Вы можете выполнять следующие действия с политиками:

- Создавать политику (см. раздел "Создание политики" на стр. 279).
- Изменять параметры политики.

  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.
- Удалять политику.
- Экспортировать и импортировать политику.
- Изменять статус политики.
- Сравнивать версии политик в окне свойств политики в разделе **История ревизий**.

Кроме того, вы можете создавать *профили политики*. 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**.

Общая информация о работе с политиками и профилями политик приведена в документации Kaspersky Security Center.

В этом разделе

Создание политики

► *Чтобы создать политику:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства**, если вы хотите создать политику для всех устройств, управляемых приложением Kaspersky Security Center.

- В папке **Управляемые устройства** выберите папку с названием группы администрирования, содержащую клиентские устройства, для которых должна применяться политика.

3. В рабочей области выберите закладку **Политики**.
4. Нажмите на кнопку **Новая политика**.

   Запустится мастер создания политики.
5. В открывшемся окне в списке выберите **Kaspersky Endpoint Security 12.0 для Linux**.

   Перейдите к следующему шагу мастера.
6. Введите название создаваемой политики.
7. Если вы хотите перенести в создаваемую политику параметры из политики предыдущей версии приложения Kaspersky Endpoint Security, установите флажок **Использовать параметры политики для предыдущей версии программы**.

   Перейдите к следующему шагу мастера.
8. Примите решение об использовании Kaspersky Security Network (на стр. 305). 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.
9. Укажите, в каком режиме вы используете приложение Kaspersky Endpoint Security:

   - **Автономный режим** – приложение используется для защиты устройств под управлением операционных систем Linux.
   - **Режим Легкого агента для защиты виртуальных сред** – приложение используется в составе решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.

   Перейдите к следующему шагу мастера.
10. Если вы используете приложение в режиме Легкого агента для защиы виртуальных сред, настройте параметры обнаружения SVM:

    a. Выберите способ, который используют Легкие агенты для обнаружения доступных для подключения SVM:

       - **Использовать Сервер интеграции**

         Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них.
       - **Использовать список адресов SVM, заданный вручную**

         Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.

Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/index.htm), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** (на стр. 348) требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

b. Если вы выбрали Сервер интеграции, в окне мастера отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. Если требуется, укажите новые параметры подключения:

   a. Нажмите на кнопку **Изменить** и укажите новые параметры подключения в открывшемся окне:

      - **Адрес**

        IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

        Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен, в поле по умолчанию указано доменное имя этого устройства.

        Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или Сервер интеграции установлен на другом устройстве, поле требуется заполнить вручную.

      Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

      - **Порт**

        Порт для подключения к Серверу интеграции.

        По умолчанию указан порт 7271.

   b. Нажмите на кнопку **OK**.

   c. Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, для аутентификации на Сервере интеграции используется учетная запись администратора Сервера интеграции.

      В открывшемся окне введите пароль администратора Сервера интеграции (пароль учетной записи `admin`) и нажмите на кнопку **OK**.

   d. Mmc-плагин проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. С помощью ссылки в окне вы можете посмотреть информацию о полученном сертификате.

      При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

c. Если вы выбрали список адресов SVM, заданный вручную, в окне отображается список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Чтобы добавить SVM в список, нажмите на кнопку **Добавить** и укажите в открывшемся окне IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки.

> Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения.

Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**.

Перейдите к следующему шагу мастера.

11. Если требуется, настройте параметры Защиты от файловых угроз (см. раздел "Защита от файловых угроз" на стр. 285).

    Перейдите к следующему шагу мастера.

12. Если требуется, измените настроенные по умолчанию параметры проверки (см. раздел "Окно Параметры проверки" на стр. 289).

    Перейдите к следующему шагу мастера.

13. Если требуется, настройте области исключения (на стр. 292).

    Перейдите к следующему шагу мастера.

14. Если требуется, измените настроенные по умолчанию действия при обнаружении угрозы (см. раздел "Окно Действие при обнаружении угрозы" на стр. 291).

    Перейдите к следующему шагу мастера.

15. Завершите работу мастера создания политики.

Изменение параметров политики

► *Чтобы изменить параметры политики:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием нужной группы администрирования, для которой вы хотите изменить параметры политики.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и в контекстном меню политики выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название политики>**.

5. Измените параметры политики.
6. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**, чтобы сохранить изменения.

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.

Параметры политики

Вы можете использовать политику для настройки параметров работы приложения Kaspersky Endpoint Security для всех клиентских устройств, входящих в состав группы администрирования.

Набор параметров и значения по умолчанию для параметров политики зависят от типа лицензии. Некоторые параметры политики применяются или не применяются в работе приложения в зависимости от режима, в котором используется приложение (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23).

С помощью политики вы можете настраивать параметры работы приложения в разделах и подразделах окна свойств политики, приведенных в таблице ниже. О настройке общих параметров политики и параметрах событий см. в документации Kaspersky Security Center.

Таблица 34. Разделы окна свойств политики

Раздел	Подразделы
Базовая защита	**Защита от файловых угроз** (на стр. 285) **Области исключения** (на стр. 292) **Исключения по процессам** (на стр. 295) **Управление сетевым экраном** (на стр. 298) **Защита от веб-угроз** (на стр. 302) **Защита от сетевых угроз** (на стр. 304)
Продвинутая защита	**Kaspersky Security Network** (на стр. 305) **Контроль приложений** (на стр. 310) **Защита от шифрования** (на стр. 313) **Контроль целостности системы** (на стр. 319) **Контроль устройств** (на стр. 322) **Анализ поведения** (на стр. 326)
Локальные задачи	**Управление задачами** (на стр. 328) **Проверка съемных дисков** (на стр. 329)
Общие параметры	**Параметры прокси-сервера** (на стр. 330) **Параметры приложения** (на стр. 331) **Параметры проверки контейнеров** (на стр. 333) **Managed Detection and Response** (на стр. 335) **Параметры сети** (на стр. 335) **Глобальные исключения** (на стр. 338) **Исключение памяти процессов** (на стр. 339) **Параметры Хранилища** (на стр. 340) **Endpoint Detection and Response (KATA)** (см. раздел "**Интеграция с Kaspersky Endpoint Detection and Response (KATA)**" на стр. 341)
Режим Легкого агента (на стр. 345)	**Подключение к Серверу интеграции** (на стр. 345) **Параметры обнаружения SVM** (на стр. 347) **Тег для подключения к SVM** (на стр. 348) **Алгоритм выбора SVM** (на стр. 348) **Защита соединения** (на стр. 350)

В сертифицированной версии приложения не поддерживаются следующие функции:

- интеграция с решением Kaspersky Managed Detection and Response;
- механизм автоматической загрузки обновлений приложения.

kaspersky

В этом разделе

Защита от файловых угроз

Защита от файловых угроз позволяет избежать заражения файловой системы устройства пользователя. Защита от файловых угроз запускается автоматически с параметрами по умолчанию при запуске приложения Kaspersky Endpoint Security, постоянно находится в оперативной памяти устройства и проверяет все открываемые, сохраняемые и запускаемые файлы.

Таблица 35. Параметры Защиты от файловых угроз

Параметр	Описание
Включить Защиту от файловых угроз	Флажок включает или выключает Защиту от файловых угроз на всех управляемых устройствах. По умолчанию флажок установлен.
Режим Защиты от файловых угроз	В раскрывающемся списке вы можете выбрать режим работы Защиты 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 и параметры проверки (см. раздел "Окно Параметры проверки" на стр. 289).
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. 291), в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

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 36. 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 Endpoint Security 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 <Название области проверки>

В этом окне вы можете добавить или настроить область проверки.

Таблица 37. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области 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	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 38. Параметры Защиты от файловых угроз

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, Kaspersky Endpoint Security 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 Endpoint Security не проверяет архивы. По умолчанию флажок снят.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, Kaspersky Endpoint Security проверяет самораспаковывающиеся архивы. Если флажок снят, Kaspersky Endpoint Security 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 Endpoint Security проверяет файлы почтовых баз. Если флажок снят, Kaspersky Endpoint Security 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 Endpoint Security проверяет сообщения в текстовом формате. Если флажок снят, Kaspersky Endpoint Security не проверяет сообщения в текстовом формате. По умолчанию флажок снят.

Параметр	Описание
Пропускать текстовые файлы	Временное исключение из проверки файлов в текстовом формате. Если флажок установлен, Kaspersky Endpoint Security 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 Endpoint Security 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 Kaspersky Endpoint Security 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 Endpoint Security проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, Kaspersky Endpoint Security записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, Kaspersky Endpoint Security не записывает в журнал события типа *ObjectProcessed*. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, Kaspersky Endpoint Security записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, Kaspersky Endpoint Security не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, Kaspersky Endpoint Security записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, Kaspersky Endpoint Security не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.

Параметр	Описание
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, Kaspersky Endpoint Security проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, Kaspersky Endpoint Security проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.
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 Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Таблица 39. Параметры Защиты от файловых угроз

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое Kaspersky Endpoint Security выполняет над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Блокировать** доступ к объекту.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое Kaspersky Endpoint Security выполняет над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в 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 исключения

Исключение из проверки – это совокупность условий, при выполнении которых приложение Kaspersky Endpoint Security не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете также исключать объекты из проверки по маскам и названиям угроз.

Таблица 40. 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. 410). 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. 295). 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. 295). 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 41. 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 <Название области исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Таблица 42. 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. 410). 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.

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.

Исключения по процессам

Вы можете настроить исключение активности процессов из проверки. Приложение не будет проверять активность указанных процессов. Вы также можете исключать из проверки файлы, изменяемые указанными процессами.

Блок параметров **Исключения по процессам** содержит кнопку **Настроить**, по которой открывается окно **Исключения по процессам**. В этом окне вы можете задать список областей исключений по процессам.

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 43. 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. 296), изменять (см. раздел "Окно Доверенный процесс" на стр. 296) 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 44. 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.

Параметр	Описание
	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. 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.
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.

kaspersky

Управление сетевым экраном

Сетевой экран операционной системы защищает персональные 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. Задача Управление сетевым экраном позволяет задать статус этих сетевых соединений при помощи настройки сетевых пакетных правил (см. раздел "О сетевых пакетных правилах" на стр. 192).

Задача Управление сетевым экраном предоставляет графическую оболочку для управления межсетевым экраном, входящим в состав операционной системы.

Настройка сетевых пакетных правил позволяет вам 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 задачи Управление сетевым экраном.

Перед включением компонента Управление сетевым экраном рекомендуется выключить другие средства управления сетевым экраном операционной системы.

Таблица 45. 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. 299). 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 **Список доступных сетей** (см. раздел "**Окно Доступные сети**" на стр. 301). 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.

Параметр	Описание
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 46. Параметры сетевых пакетных правил

Параметр	Описание
Название	Имя сетевого пакетного правила.
Действие	Действие, выполняемое компонентом Управление сетевым экраном при обнаружении сетевой активности.
Локальный адрес	Сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, 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.

Сетевые пакетные правила в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно Добавление сетевого пакетного правила

В этом окне вы можете настроить параметры добавляемого сетевого пакетного правила.

Таблица 47. 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**

Параметр	Описание
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 типа (в поле **ICMP-тип**) и с указанным 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 Endpoint Security, 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 Endpoint Security и любым IP-адресом. • **Определенный адрес**. Если выбран этот вариант, сетевое правило контролирует указанные в поле ниже сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, 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 48. 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 49. Сетевое соединение

Параметр	Описание
IP-адрес	Поле ввода IP-адреса сети.
Тип сети	Вы можете выбрать тип сети: • **Публичная сеть**. • **Локальная сеть**. • **Доверенная сеть**.

Защита от веб-угроз

Во время работы компонента Защита от веб-угроз приложение проверяет входящий трафик, не допускает загрузку вредоносных файлов из интернета, а также блокирует фишинговые, рекламные и прочие опасные веб-сайты.

Приложение проверяет трафик, передаваемый по протоколам HTTP, HTTPS и FTP. Также выполняется проверка веб-сайтов и IP-адресов. Вы можете указать определенные сетевые порты или диапазоны сетевых портов для проверки.

Для проверки HTTPS-трафика требуется включить проверку зашифрованных соединений (см. раздел "Параметры сети" на стр. 335). Для проверки FTP-трафика требуется установить флажок **Отслеживать все сетевые порты** (см. раздел "**Параметры сети**" на стр. 335).

Таблица 50. Параметры Защиты 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. 303), в котором вы можете указать список доверенных веб-адресов. Приложение Kaspersky Endpoint Security не проверяет содержание веб-сайтов, веб-адреса которых указаны в этом списке.

Параметр	Описание
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 (значение по умолчанию). • **Информировать** пользователя при обнаружении опасного объекта в веб-трафике. 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. 303), 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 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).

Вы можете добавлять, изменять и удалять веб-адреса в списке. По умолчанию список пустой.

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 51. 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 программы	Флажок включает или выключает проверку ссылок по базе рекламных веб-адресов. По умолчанию флажок снят.
Обнаруживать легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройствам или данным	Флажок включает или выключает проверку ссылок по базе легальных программ, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. По умолчанию флажок снят.

Защита от сетевых угроз

Во время работы компонента Защита от сетевых угроз приложение проверяет входящий сетевой трафик на действия, характерные для сетевых атак. Защита от сетевых угроз запускается по умолчанию при запуске приложения.

Приложение проверяет входящий трафик для TCP-портов, номера которых получает из актуальных баз приложения. При обнаружении попытки сетевой атаки на ваше устройство, приложение блокирует сетевую активность со стороны атакующего устройства и записывает в журнал событие об обнаруженной сетевой активности.

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.

Таблица 52. Параметры Защиты от сетевых угроз

Параметр	Описание
Включить Защиту от сетевых угроз	Флажок включает или выключает компонент Защита от сетевых угроз. По умолчанию флажок установлен.

Параметр	Описание
Действие при обнаружении угрозы	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак: • **Информировать** пользователя. 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 (значение по умолчанию).
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 Endpoint Security 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. 305), 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.

Вы можете добавлять, изменять и удалять IP-адреса в списке.

Окно IP-адрес

Вы можете добавлять и изменять IP-адреса, сетевые атаки с которых не будут заблокированы приложением Kaspersky Endpoint Security.

Таблица 53. IP-адреса

Параметр	Описание
Укажите IP-адрес (IPv4 или IPv6)	Поле для ввода IP-адреса. IP-адреса можно указывать в форматах IPv4 и IPv6.

Kaspersky Security Network

Для повышения эффективности защиты устройств и данных пользователей Kaspersky Endpoint Security 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. Приложение Kaspersky Endpoint Security предлагает включить использование KSN во время установки. Вы можете включить или выключить использование KSN в любой момент.

Инфраструктурные решения Kaspersky Security Network

Kaspersky Endpoint Security 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 Endpoint Security 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 изменения лицензии Kaspersky Endpoint Security для использования KPSN требуется предоставить поставщику услуг информацию о новом 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 Endpoint Security 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 Endpoint Security 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. 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**.

Облачный режим работы Kaspersky Endpoint Security

Если приложение Kaspersky Endpoint Security используется в автономном режиме и вы используете KSN в работе приложения, вы можете включать *облачный режим* работы приложения. Облачный режим – это режим работы приложения Kaspersky Endpoint Security, при котором используется облегченная версия баз вредоносного ПО.

Включение облачного режима приводит к выходу приложения из сертифицированного состояния.

Работу приложения с облегченными базами вредоносного ПО обеспечивает Kaspersky Security Network.

Если вы планируете использовать облачный режим, убедитесь, что KSN доступен на устройстве. Информация о доступности KSN отображается в Kaspersky Security Center с помощью статуса клиентского устройства (*OK, Критический, Предупреждение*) в списке управляемых устройств на закладке **Устройства**.

Kaspersky Endpoint Security переходит к использованию облегченной версии баз вредоносного ПО после включения облачного режима и выполнения очередного обновления баз и модулей приложения. Если вы не используете KSN или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию баз приложения с серверов "Лаборатории Касперского" в ходе очередного обновления баз приложения. Облачный режим выключается автоматически, если выключено использование KSN.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, работа с облегченными базами вредоносного ПО не поддерживается. Kaspersky Endpoint Security получает от Сервера защиты специальные базы, необходимые для работы Легкого агента.

Использование службы прокси-сервера KSN

Устройства пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN напрямую или при помощи службы прокси-сервера KSN.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, взаимодействие с инфраструктурой KSN обеспечивает служба прокси-сервера KSN. Если прокси-сервер KSN недоступен, KSN не используется в работе приложения.

Вы можете настроить параметры прокси-сервера KSN в свойствах Сервера администрирования Kaspersky Security Center. Подробнее о прокси-сервере KSN см. в справке Kaspersky Security Center.

Таблица 54. 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 Endpoint Security. По кнопке **Изменить** открывается окно, в котором вы можете настроить использование Kaspersky Security Network (см. раздел "Параметры Kaspersky Security Network" на стр. 308).
Включить облачный режим	Флажок включает или выключает режим работы, при котором приложение Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО. Флажок доступен, если включено использование KSN. Флажок установлен, если при создании политики вы приняли условия Положения о Kaspersky Security Network и используете расширенный режим KSN. Режим включается или выключается после следующего обновления баз приложения. Включение облачного режима приводит к выходу приложения из сертифицированного состояния.
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. Параметр применяется, только если приложение используется в автономном режиме.

Параметры Kaspersky Security Network

В этом окне вы можете настроить параметры использования Kaspersky Security Network.

Таблица 55. 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. **309**), 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 56. 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. 308) 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. 308) 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 57. 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.

Контроль приложений

Во время выполнения задачи Контроль приложений приложение Kaspersky Endpoint Security управляет запуском приложений на устройствах пользователей. Это позволяет снизить риск заражения устройства, ограничивая доступ к приложениям. Запуск приложений регулируется с помощью *правил контроля приложений* (см. раздел "*О правилах контроля приложений*" на стр. 244).

Для использования компонента требуется лицензия, которая включает эту функцию.

Контроль приложений может работать в двух режимах:

- *Список запрещенных*. Режим, при котором приложение Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. Этот режим работы компонента Контроль приложений настроен по умолчанию.
- *Список разрешенных*. Режим, при котором приложение Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.

Для каждого режима работы Контроля приложений вы можете создать отдельные правила, а также выбрать действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения: *применять правила* или *информировать* о попытке запуска приложения, удовлетворяющего правилам.

Параметры Контроля приложений описаны в таблице ниже.

Таблица 58. Параметры Контроля приложений

Параметр	Описание
Включить Контроль приложений	Флажок включает компонент Контроль приложений. По умолчанию флажок снят.
Действие при попытке запуска приложения	Действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам: • **Применять правила** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security применяет правила контроля приложений и выполняет заданное в правилах действие. • **Информировать (тестовый режим)**. При выборе этого варианта приложение Kaspersky Endpoint Security тестирует правила и формирует событие о попытке запуска приложения, удовлетворяющего правилам.

Параметр	Описание
Режим Контроля приложений	Режим работы компонента Контроль приложений: • **Список разрешенных**. При выборе этого варианта приложение Kaspersky Endpoint Security 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 Endpoint Security 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. 311).

Окно Правила Контроля приложений

Таблица **Правила Контроля приложений** содержит правила, используемые компонентом Контроль приложений. По умолчанию таблица правил контроля приложений пустая.

Таблица 59. Параметры правил контроля приложений

Параметр	Описание
Название категории	Название категории приложений, которая используется в работе правила.
Статус	Статус работы правила контроля приложений: • *Включено* – правило включено, Контроль приложений применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля приложений. • *Тест* – 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 / Изменение правила**" на стр. **311**).

Вы можете добавлять, изменять (см. раздел "Окно Добавление правила / Изменение правила" на стр. 311) и удалять правила контроля приложений.

Окно Добавление правила / Изменение правила

В этом окне вы можете настроить параметры создаваемого правила контроля приложений.

Таблица 60. Добавление правила контроля приложений

Параметр	Описание
Описание	Описание правила Контроля приложений.

Параметр	Описание
Статус правила	В раскрывающемся списке вы можете выбрать статус работы правила контроля приложений: • *Включено* – правило включено, Контроль приложений применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля приложений. • *Тест* – 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. 312).
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, изменять (см. раздел "Окно Имя пользователя или группы" на стр. 312) и 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 Kaspersky Security Center не поддерживается.

Таблица 61. 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 Имя пользователя или группы

В этом окне вы можете указать локального или доменного пользователя или группу пользователей, для которых вы хотите настроить правило.

Таблица 62. 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** запуск приложений или **Блокировать** запуск приложений.

Защита от шифрования

Защита от шифрования позволяет защитить ваши файлы в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования.

Во время работы компонента Защита от шифрования приложение проверяет обращения удаленных устройств сети к файлам, расположенным в общих сетевых директориях защищаемого устройства. Если приложение расценивает действия удаленного устройства, получающего доступ к общим сетевым ресурсам, как вредоносное шифрование, она добавляет это устройство в список недоверенных устройств и запрещает ему доступ к общим сетевым директориям. Приложение не расценивает действия как вредоносное шифрование, если активность обнаружена в директориях, которые не входят в область защиты компонента Защита от шифрования.

Для использования компонента требуется лицензия, которая включает эту функцию.

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, чтобы был установлен пакет rpcbind.

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.

Защита от шифрования не блокирует доступ к сетевым файловым ресурсам до тех пор, пока действия устройства не расцениваются как вредоносные. Таким образом, как минимум один файл будет зашифрован, прежде чем приложение обнаружит вредоносную активность.

Таблица 63. Параметры Защиты 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 установлен.
Области защиты	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки и параметры защиты (см. раздел "Окно Параметры защиты" на стр. 316).

Параметр	Описание
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. 295). 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 64. 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 Endpoint Security 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 <Название области проверки>

В этом окне можно добавить или настроить область защиты компонента Защита от шифрования.

Таблица 65. Параметры области защиты

Параметр	Описание
Название области	Поле ввода названия области защиты. Это название будет отображаться в таблице окна **Области 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 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.

Параметр	Описание
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.
	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, /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 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 66. Параметры защиты

Параметр	Описание
Включить блокирование недоверенных устройств	Флажок включает или выключает блокировку недоверенных устройств. По умолчанию флажок установлен.
Блокировать недоверенное устройство на (мин)	Поле, в котором вы можете указать длительность блокировки недоверенного устройства в минутах. По истечении указанного времени приложение Kaspersky Endpoint Security 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 4294967295. 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 67. 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 <Название области исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Таблица 68. 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. 410). Поле ввода не должно быть пустым.

Параметр	Описание
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.

Контроль целостности системы

Контроль целостности системы предназначен для отслеживания действий, выполняемых с файлами и директориями в области мониторинга, указанной в параметрах работы компонента. Вы можете использовать Контроль целостности системы, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве.

Для использования компонента требуется лицензия, которая включает эту функцию.

Таблица 69. Параметры Контроля 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. 432).
Исключения из мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения** (см. раздел "**Окно Области исключения**" на стр. 320)
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. 321).

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/kesl/).

Таблица 70. 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 Endpoint Security 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 <Название области проверки>

В этом окне вы можете добавить или настроить области мониторинга для компонента Контроль целостности системы.

Таблица 71. 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. 432). 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/kesl.
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 72. 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 73. 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. 320). 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.

kaspersky

Контроль устройств

Во время выполнения задачи Контроль устройств приложение Kaspersky Endpoint Security управляет доступом пользователей к устройствам, которые установлены на клиентском устройстве или подключены к нему (например, жестким дискам, камерам или модулям Wi-Fi). Это позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных. Контроль устройств управляет доступом пользователей к устройствам с помощью правил доступа (см. раздел "О правилах доступа" на стр. 210).

При подключении устройства, доступ к которому запрещен задачей Контроль устройств, к клиентскому устройству, 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.

Таблица 74. Параметры Контроля устройств

Параметр	Описание
Включить Контроль устройств	Флажок включает или выключает компонент Контроль устройств. По умолчанию флажок установлен.
Доверенные устройства	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные устройства** (см. раздел "**Окно Доверенные устройства**" на стр. 322). В этом окне вы можете добавить устройство в список доверенных устройств по его идентификатору (см. раздел "Окно Доверенное устройство" на стр. 323) или выбрав его в списке устройств, обнаруженных на клиентских устройствах (см. раздел "Окно Устройства на клиентских устройствах" на стр. 324).
Действие Контроля устройств	Действие, выполняемое приложением при попытке доступа к устройству, к которому запрещен доступ в соответствии с правилом доступа: • **Применять правила** (значение по умолчанию). При выборе этого варианта приложение применяет правила доступа и выполняет заданное в правилах действие. • **Тестировать правила**. При выборе этого варианта приложение тестирует правила доступа и формирует событие об обнаружении попытки доступа к устройству.
Параметры Контроля устройств	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить правила доступа для различных типов устройств (см. раздел "Окно Тип устройства" на стр. 324) и правила доступа к шинам подключения (см. раздел "Окно Шины подключения" на стр. 326).

Окно Доверенные устройства

Таблица содержит список доверенных устройств. По умолчанию таблица пустая.

Таблица 75. 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.

Вы можете добавить устройство в список доверенных устройств по идентификатору или маске (см. раздел "Окно Доверенное устройство" на стр. 323) или выбрав нужное устройство в списке устройств, обнаруженных на устройстве пользователя (см. раздел "Окно Устройства на клиентских устройствах" на стр. 324).

Доверенные устройства в таблице можно изменять и удалять.

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 76. 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 77. 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 78. Режим доступа для типов устройств

Параметр	Описание
Тип устройства	Тип устройства (например, Жесткие диски, Принтеры).
Доступ	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 правила доступа для шины подключения (см. раздел "Окно Шины подключения" на стр. 444). • **По правилам** – разрешить или запретить доступ к устройствам в зависимости от правила доступа (см. раздел "Окно Настройка правила доступа к устройствам" на стр. 325) и расписания (см. раздел "Окно Расписание доступа к устройствам" на стр. 325).

Кроме того, для устройств, к которым разрешен доступ с ограничениями, вы можете настроить правила доступа и расписания доступа в окне **Настройка правил доступа к устройствам** (см. раздел "**Окно Настройка правила доступа к устройствам**" на стр. 325), 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. 324).

Таблица 79. 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). 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. 326). Вы можете добавлять, изменять (см. раздел "Окно Расписание доступа к устройствам" на стр. 325) и удалять расписания доступа для выбранных пользователей. Расписание **По умолчанию** невозможно изменить или удалить.

Окно Имя пользователя или группы

В этом окне вы можете настроить параметры создаваемого правила доступа к устройствам.

Таблица 80. 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 к устройствам

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 к устройствам невозможно.

Таблица 81. 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 правила доступа для шин подключения.

Таблица 82. Правила доступа для шин подключения

Параметр	Описание
Шина подключения	Шина подключения, используемая для подключения устройства к клиентскому устройству: • **FireWire** • **USB**
Доступ	Правило доступа к шине подключения. При нажатии на правую кнопку мыши открывается контекстное меню, в котором вы можете выбрать один из следующих элементов: • **Разрешать** (значение по умолчанию) – предоставить доступ к устройствам, подключенным с помощью этой шины подключения. • **Блокировать** – запретить доступ к устройствам, подключенным с помощью этой шины подключения.

Анализ поведения

По умолчанию компонент Анализ поведения запускается при запуске приложения Kaspersky Endpoint Security и контролирует вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности приложение Kaspersky Endpoint Security может завершать процесс приложения, осуществляющего вредоносную активность.

Таблица 83. Параметры компонента Анализ поведения

Параметр	Описание
Включить Анализ поведения	Флажок включает или выключает компонент Анализ поведения. По умолчанию флажок установлен.
Действие при обнаружении вредоносной активности	Действие, которое Kaspersky Endpoint Security будет выполнять при обнаружении вредоносной активности в операционной системе: • **Блокировать** приложение, осуществляющее вредоносную активность (значение по умолчанию). Kaspersky Endpoint Security завершает процесс, осуществляющий вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности. • **Информировать** пользователя. Kaspersky Endpoint Security 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. 327). 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 Endpoint Security с решением Kaspersky Managed Detection and Response, исключения по процессам не применяются.

Таблица 84. 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. 328) 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 85. 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. 327).
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.
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.

Управление задачами

Вы можете настроить возможность просмотра и управления задачами приложения Kaspersky Endpoint Security на управляемых устройствах.

Таблица 86. Параметры управления задачами

Параметр	Описание
Разрешить пользователям просмотр и управление локальными задачами	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в приложении Kaspersky Endpoint Security, 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.

Проверка съемных дисков

Во время выполнения задачи Проверка съемных дисков приложение проверяет съемный диск и его загрузочные секторы на вирусы и другие вредоносные программы. Выполняется проверка следующих съемных дисков: CD/DVD-приводов, Blu-ray дисков, флеш-накопителей (включая USB-модемы), внешних жестких дисков и дискет.

Таблица 87. Параметры задачи 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. При быстрой проверке используются параметры, заданные по умолчанию для компонента Защита от файловых угроз (на стр. 285). • **Подробная проверка** – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При подробной проверке используются параметры, заданные по умолчанию для задачи Поиск вредоносного ПО (на стр. 363).

Параметр	Описание
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 только файлы определенных типов на CD/DVD-приводах и Blu-ray дисках. При быстрой проверке используются параметры, заданные по умолчанию для компонента Защита от файловых угроз (на стр. 285). • **Подробная проверка** – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. При подробной проверке используются параметры, заданные по умолчанию для задачи Поиск вредоносного ПО (на стр. 363).
Блокировать доступ к съемному диску во время проверки	Флажок включает или выключает блокировку файлов на подключенном диске во время выполнения задачи Проверка съемных дисков. По умолчанию флажок снят.

Параметры прокси-сервера

Вы можете настроить параметры прокси-сервера, если доступ пользователей с клиентских устройств в интернет осуществляется через прокси-сервер. Приложение Kaspersky Endpoint Security может использовать прокси-сервер для подключения к серверам "Лаборатории Касперского", например, при обновлении баз и модулей или при взаимодействии с Kaspersky Security Network и Kaspersky Endpoint Detection and Response (KATA).

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование прокси-сервера для подключения к Kaspersky Security Network, к SVM и к Серверу интеграции.

Таблица 88. Параметры прокси-сервера

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, прокси-сервер не используется в работе приложения Kaspersky Endpoint Security.
Использовать параметры указанного прокси-сервера	Если выбран этот вариант, Kaspersky Endpoint Security использует указанные параметры прокси-сервера, например для интеграции с Kaspersky Endpoint Detection and Response (KATA).
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 параметры указанного прокси-сервера**.

Параметр	Описание
Использовать имя пользователя и пароль	Флажок включает или выключает аутентификацию с помощью имени пользователя и пароля при доступе к прокси-серверу. Флажок доступен, если выбран вариант **Использовать параметры указанного 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 имя пользователя и пароль**.
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 имя пользователя и пароль**.
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 Endpoint Security использует Kaspersky Security Center в качестве прокси-сервера при активации приложения. По умолчанию флажок снят. Параметр применяется, только если приложение используется в автономном режиме. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, информацию о лицензии предоставляет Сервер защиты.

Параметры приложения

Вы можете настроить общие параметры приложения Kaspersky Endpoint Security.

Таблица 89. Общие параметры приложения

Параметр	Описание
Обнаруживать легальные программы, которые могут быть использованы злоумышленником для нанесения вреда устройствам или данным	Флажок включает или выключает обнаружение легальных программ, через которые злоумышленники могут навредить устройству или данным пользователя. По умолчанию флажок снят.
Уведомления о событиях	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Параметры уведомлений**. В этом окне вы можете выбрать события, уведомления о которых приложение будет записывать в журнал операционной системы (syslog). Для этого установите флажок около каждого типа события, уведомление о котором должно записываться. Также вы можете установить флажок около уровня важности событий (**Критические события**, **Информационные сообщения**, **Отказы функционирования**, **Предупреждения**). В этом случае флажки будут установлены автоматически около каждого типа событий, входящего в группу выбранного уровня важности. По умолчанию все флажки сняты.
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 указанного значения (в процентах). По умолчанию флажок снят.
Дополнительные параметры приложения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Дополнительные параметры приложения** (см. раздел "**Окно Дополнительные параметры приложения**" на стр. 333). В этом окне вы можете настроить параметры записи дампов.
Блокировать доступ к файлам во время проверки	Флажок включает или выключает блокировку доступа к файлам во время проверки компонентами Защита от файловых угроз (на стр. 285), Защита от шифрования (на стр. 313), Контроль устройств (на стр. 322) и задачей Проверка съемных дисков (на стр. 329). Если флажок снят, включается информирующий режим работы компонентов Защита от файловых угроз и Контроль устройств. *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 программ, а только информируют пользователя об обнаружении угрозы. По умолчанию флажок установлен.

Окно Дополнительные параметры приложения

В этом окне вы можете настроить параметры записи дампов.

Таблица 90. Параметры записи дампов

Параметр	Описание
Создавать файл дампа при сбое в работе приложения	Флажок включает или выключает создание файла дампа (см. раздел "Содержимое файлов дампа и их хранение" на стр. 515) при сбое в работе приложения. По умолчанию флажок снят. Для применения параметров записи дампов требуется перезапустить приложение.
Путь к директории с файлами дампа	Поле ввода пути к директории, в которой хранятся файлы дампа. Размер поля ввода ограничен 128 символами. Допустимо использовать только символы `0-9`, `a-z`, `A-Z`, а также `_-./` для указания пути. Значение по умолчанию: /var/opt/kaspersky/kesl/common/dumps.

Параметры проверки контейнеров

Вы можете настроить параметры проверки пространств имен и контейнеров приложением Kaspersky Endpoint Security.

Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен. При этом в свойствах устройства в разделе **Программы**, в свойствах приложения в разделе **Компоненты** для проверки контейнеров отображается статус *Остановлена*.

Таблица 91. Параметры проверки контейнеров

Параметр	Описание
Включить проверку пространств имен и контейнеров	Флажок включает или выключает проверку пространств имен и контейнеров. По умолчанию флажок установлен.

Параметр	Описание
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** – 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** (значение по умолчанию) – если не удалось вылечить зараженный объект, приложение останавливает контейнер. Этот параметр доступен при использовании приложения по лицензии, которая включает эту функцию.
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. 334).

Окно Параметры проверки контейнеров

В этом окне вы можете настроить параметры проверки контейнеров приложением Kaspersky Endpoint Security.

Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен. При этом в свойствах устройства в разделе **Программы**, в свойствах приложения в разделе **Компоненты** для проверки контейнеров отображается статус *Остановлена*.

Таблица 92. 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.

Параметр	Описание
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.

Managed Detection and Response

Интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response (MDR) обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.

Эта функциональность не поддерживается в сертифицированной версии приложения. Включение интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response приводит к выходу приложения из сертифицированного состояния.

Таблица 93. Параметры Managed Detection and Response

Параметр	Описание
Включить Managed Detection and Response	Флажок включает интеграцию приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response. По умолчанию флажок снят. Установка флажка приводит к выходу приложения из сертифицированного состояния.
Загрузить	По нажатию на кнопку открывается стандартное окно Microsoft Windows, в котором вы можете выбрать конфигурационный файл BLOB.

Параметры сети

Вы можете настроить параметры проверки зашифрованных соединений. Эти параметры используются в работе компонента Защита от веб-угроз (на стр. 302).

При изменении параметров проверки зашифрованных соединений приложение формирует событие *Параметры сети изменены (Network settings changed)*.

Таблица 94. Параметры сети

Параметр	Описание
Включить проверку зашифрованных соединений	Флажок включает или выключает проверку зашифрованных соединений. По умолчанию флажок установлен.
Действие при обнаружении недоверенного сертификата	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять при обнаружении недоверенного сертификата: • **Разрешить** подключение к домену с недоверенным сертификатом (значение по умолчанию). • **Блокировать** подключение к домену с недоверенным сертификатом.
Действие при обнаружении ошибки проверки зашифрованного соединения	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять при возникновении ошибки во время проверки зашифрованных соединений: • **Добавить 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. • **Отключить** – заблокировать сетевое подключение.
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. 336). В этом окне вы можете настроить список имен доверенных доменов.
Доверенные сертификаты	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные сертификаты** (см. раздел "**Окно Доверенные сертификаты**" на стр. 337). В этом окне вы можете настроить список доверенных сертификатов, который используется при проверке зашифрованных соединений.
Параметры сетевых портов	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Сетевые порты** (см. раздел "**Окно Сетевые порты**" на стр. 337).

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 Доверенные сертификаты

Вы можете настроить список сертификатов, которые приложение Kaspersky Endpoint Security 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 SHA-256** – отпечаток сертификата SHA-256.

По умолчанию список сертификатов пуст.

Вы можете добавлять (см. раздел "Окно Добавление сертификата" на стр. 337) и удалять сертификаты.

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 Сетевые порты

Таблица 95. Параметры сетевых портов

Параметр	Описание
Отслеживать все сетевые порты	Если выбран этот вариант, приложение проверяет все сетевые порты.
Отслеживать только указанные 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 **Отслеживать 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.

kaspersky

Глобальные исключения

Глобальные исключения позволяют задать точки монтирования, которые будут исключены из проверки компонентами приложения, использующими перехватчик файловых операций (Защита от файловых угроз и Защита от шифрования).

Таблица 96. Параметры глобальных исключений

Параметр	Описание
Исключенные точки монтирования	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключенные точки монтирования** (см. раздел "**Окно Исключенные точки монтирования**" на стр. 338).

Окно Исключенные точки монтирования

Список содержит пути к исключенным точкам монтирования. По умолчанию список пуст.

Элементы в списке можно добавлять (см. раздел "Окно Путь к точке монтирования" на стр. 338), изменять (см. раздел "Окно Путь к точке монтирования" на стр. 338) и удалять.

Окно Путь к точке монтирования

Таблица 97. 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.

Параметр	Описание
	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. 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.
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**.

Исключение памяти процессов

Вы можете настраивать исключения из проверки памяти процессов. Приложение не будет проверять память указанных процессов.

Вы можете сформировать список исключений в окне (см. раздел "Окно Исключение памяти процессов из проверки" на стр. 339), которое открывается по кнопке **Настроить** в блоке **Исключение памяти процессов из проверки**.

Окно Исключение памяти процессов из проверки

Список содержит пути к процессам, которые Kaspersky Endpoint Security исключает из проверки памяти процессов. Для указания пути вы можете использовать маски. По умолчанию список пуст.

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.

Элементы в списке можно добавлять, изменять и удалять.

Параметры Хранилища

Хранилище – это список резервных копий файлов, которые были удалены или изменены в процессе лечения. *Резервная копия* – копия файла, которая создается при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности. По умолчанию Хранилище расположено в директории /var/opt/kaspersky/kesl/common/objects-backup/.

Файлы в Хранилище могут содержать персональные данные. Для доступа к файлам в Хранилище требуются root-права.

Таблица 98. Параметры Хранилища

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 управляемом клиентском устройстве. По умолчанию флажок установлен.
Информировать о файлах в Хранилище	Флажок включает или выключает отправку уведомлений о файлах в Хранилище на Сервер администрирования. По умолчанию флажок установлен.
Хранить объекты не более (дней)	Флажок включает или выключает ограничение срока хранения объектов в Хранилище заданным интервалом времени. Доступные значения: 0–3653. Значение по умолчанию: 90. Если задано значение 0, период хранения объектов в Хранилище не ограничен.
Максимальный размер Хранилища (МБ)	Флажок включает или выключает ограничение максимального размера Хранилища заданным значением (в мегабайтах). Доступные значения: 0–999999. Значение по умолчанию: 0 (размер Хранилища не ограничен).

kaspersky

Интеграция с Kaspersky Endpoint Detection and Response (KATA)

Kaspersky Endpoint Detection and Response (KATA) (далее также EDR (KATA)) – компонент в составе решения Kaspersky Anti Targeted Attack Platform, которое предназначено для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats (далее также "APT"). Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform https://support.kaspersky.com/help/KATA/5.1/ru-RU/246841.htm.

При взаимодействии с EDR (KATA) приложение Kaspersky Endpoint Security может отправлять на сервер Kaspersky Anti Targeted Attack Platform с компонентом Central Node (далее также сервер KATA) данные о событиях на устройствах (телеметрию) и выполнять задачи, полученные от Kaspersky Anti Targeted Attack Platform, направленные на обеспечение функций безопасности.

Для интеграции с EDR (KATA) должен быть включен компонент Анализ поведения.

Интеграция приложения Kaspersky Endpoint Security с EDR (KATA) возможна, только если этот компонент включен. В противном случае необходимые данные телеметрии не передаются.

Дополнительно EDR (KATA) может использовать данные, полученные от следующих компонентов:

- Защита от файловых угроз.
- Защита от сетевых угроз.
- Защита от веб-угроз.

Во время интеграции с EDR (KATA) устройства с Kaspersky Endpoint Security устанавливают защищенные соединения с сервером KATA по протоколу HTTPS. Для обеспечения безопасности соединения используются следующие сертификаты, выданные сервером KATA:

- Сертификат сервера KATA. Соединение шифруется с помощью TLS-сертификата сервера. Вы можете повысить уровень безопасности соединения, включив проверку сертификата сервера на стороне Kaspersky Endpoint Security. Для этого вам нужно добавить сертификат сервера (см. раздел "Окно настройки параметров подключения к серверам" на стр. 343) во время настройки параметров интеграции.
- Сертификат клиента. Этот сертификат используется для дополнительной защиты подключения с помощью двусторонней аутентификации (проверки устройств с Kaspersky Endpoint Security сервером KATA). Один и тот же сертификат клиента может использоваться несколькими устройствами. По умолчанию сервер KATA не выполняет проверку сертификатов клиентов, но проверка может быть включена на стороне сервера KATA. В этом случае вам нужно включить двустороннюю аутентификацию в параметрах интеграции и добавить сертификат клиента (см. раздел "Окно настройки параметров подключения к серверам" на стр. 343) (криптоконтейнер с сертификатом и закрытым ключом).

Сертификаты для защиты соединения с сервером KATA предоставляет администратор Kaspersky Anti Targeted Attack Platform.

Для подключения к серверу KATA используется прокси-сервер, если использование прокси-сервера настроено (см. раздел "Параметры прокси-сервера" на стр. 330) в общих параметрах приложения Kaspersky Endpoint Security.

Таблица 99. Параметры интеграции с Kaspersky Endpoint Detection and Response (KATA)

Параметр	Описание
Интеграция с Endpoint Detection and Response (KATA)	Включает или выключает интеграцию приложения Kaspersky Endpoint Security с EDR (KATA). По умолчанию интеграция выключена.
Серверы KATA	По кнопке **Настроить** в блоке открывается окно **Серверы KATA** (см. раздел "**Окно Серверы KATA**" на стр. 342). В этом окне вы можете настраивать подключение к серверам KATA, а также просматривать список серверов, к которым настроено подключение.
Параметры подключения к серверам	По кнопке **Настроить** в блоке открывается окно (см. раздел "Окно настройки параметров подключения к серверам" на стр. 343), в котором вы можете настроить общие параметры подключения к серверам KATA, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверам KATA.
Параметры передачи данных	По кнопке **Настроить** в блоке открывается окно (см. раздел "Окно Параметры передачи данных" на стр. 344), в котором вы можете настроить параметры передачи данных на серверы KATA.

Окно Серверы KATA

В этом окне в таблице отображается список параметров подключения к серверам KATA. 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 добавления параметров подключения к серверу KATA" на стр. 342) параметры подключения к серверу KATA.
- Изменить или удалить ранее настроенные параметры подключения.
- Экспортировать или импортировать список настроенных параметров подключения.

Окно добавления параметров подключения к серверу KATA

В этом окне вы можете указать параметры подключения к серверу KATA.

Таблица 100. Параметры подключения к серверу KATA

Параметр	Описание
Адрес	Адрес сервера KATA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером KATA 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 KATA. Значение по умолчанию: `443`.

Окно настройки параметров подключения к серверам

В этом окне вы можете настроить общие параметры подключения к серверам KATA.

Таблица 101. Параметры подключения к серверам KATA

Параметр	Описание
Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)	Периодичность отправки запросов на синхронизацию на сервер KATA в минутах. Значение по умолчанию: 5.
Максимальное время ожидания соединения с сервером (сек.)	Максимальное время ожидания соединения с сервером KATA в секундах. Значение по умолчанию: `10`.
Максимальное время ожидания ответа от сервера (сек.)	Максимальное время ожидания ответа от сервера KATA в секундах. Значение по умолчанию: `10`.
Разрешить отправку телеметрии	Включает или выключает отправку данных о событиях на устройствах (телеметрии) на сервер KATA. По умолчанию отправка телеметрии включена.
Использовать двустороннюю аутентификацию	Включает или выключает использование двусторонней аутентификации для дополнительной защиты соединения с сервером KATA. Чтобы использовать двустороннюю аутентификацию, вам нужно добавить сертификат клиента. Двусторонняя аутентификация должна быть включена на стороне сервера KATA.
Добавить (сертификат клиента)	Открывает окно добавления сертификата клиента (на стр. 344) для дополнительной защиты соединения с сервером KATA. Кнопка отображается, если сертификат клиента еще не добавлен. Если вы хотите настроить дополнительную защиту соединения, вам нужно включить проверку сертификатов клиентов на стороне сервера KATA 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 (на стр. 344). Кнопка отображается, если сертификат сервера еще не добавлен.
Удалить (сертификат сервера)	Удаляет сертификат сервера. Кнопка отображается, если сертификат сервера добавлен.

Окно добавления сертификата сервера

В этом окне вы можете добавить сертификат сервера KATA одним из следующих способов:

- Указать путь к файлу сертификата в поле **Добавлить 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 Endpoint Security, это позволяет повысить уровень безопасности соединения.

Окно добавления сертификата клиента

В этом окне вы можете добавить сертификат клиента для дополнительной защиты соединения с сервером KATA.

Если вы хотите настроить дополнительную защиту соединения, вам нужно включить проверку сертификатов клиентов на стороне сервера KATA и установить флажок **Использовать двустороннюю аутентификацию** в окне настройки параметров подключения к серверам (см. раздел "Окно настройки параметров подключения к серверам" на стр. 343).

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 Параметры передачи данных

В этом окне вы можете настроить параметры передачи данных на серверы KATA.

Таблица 102. Параметры передачи данных на серверы KATA

Параметр	Описание
Максимальная задержка отправки событий (сек.)	Максимальная задержка отправки событий на сервер KATA в секундах. Значение по умолчанию: `30`.
Включить регулирование количества событий	Включает или выключает регулирование количества событий, отправляемых на сервер KATA.
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`.

kaspersky

Режим Легкого агента

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Для работы приложения Kaspersky Endpoint Security в режиме Легкого агента требуется постоянное взаимодействие между Легким агентом и Сервером защиты, установленным на SVM. Если соединение с Сервером защиты отсутствует, Легкий агент не может передавать фрагменты файлов на проверку Серверу защиты, проверка не выполняется.

Для взаимодействия с Сервером защиты Легкий агент устанавливает и поддерживает подключение к SVM, на которой установлен этот Сервер защиты.

Вы можете настраивать следующие параметры подключения Легкого агента к SVM:

- Способ обнаружения SVM (см. раздел "Параметры обнаружения SVM" на стр. 347). Вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM. Легкий агент может обнаруживать SVM, работающие в сети, одним из следующих способов:
  - С помощью Сервера интеграции. SVM передают информацию о себе на Сервер интеграции. Сервер интеграции формирует список доступных для подключения SVM и предоставляет его Легким агентам.

    Для использования этого способа обнаружения SVM требуется подключение (см. раздел "Подключение к Серверу интеграции" на стр. 345) SVM и Легких агентов к Серверу интеграции.
  - С использованием списка адресов SVM. Вы можете задать список адресов SVM, к которым могут подключаться Легкие агенты.
- Алгоритм выбора SVM (на стр. 348) для подключения. После получения информации о доступных SVM Легкий агент выбирает оптимальную для подключения SVM в соответствии с алгоритмом выбора SVM. Вы можете указать, какой алгоритм должны использовать Легкие агенты при выборе SVM для подключения.
- Теги для подключения (см. раздел "Тег для подключения к SVM" на стр. 348). Вы можете регулировать подключение Легких агентов к SVM с помощью тегов для подключения. Если вы используете теги для подключения, Легкий агент может подключаться только к тем SVM, на которых настроено использование этого тега для подключения.
- Защита соединения (на стр. 350) между Легким агентом и Сервером защиты. Вы можете защищать соединение между Легкими агентами и Серверами защиты с помощью шифрования.

Подробнее о параметрах подключения Легкого агента к SVM см. в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254867.htm.

Подключение к Серверу интеграции

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Подключение к Серверу интеграции требуется, если вы хотите, чтобы Легкие агенты получали информацию об SVM через Сервер интеграции, или если вы хотите защищать соединение между Сервером защиты и Легким агентом.

В этом окне отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. По нажатию на кнопку **Изменить** открывается окно **Подключение к Серверу интеграции** (см. раздел "**Окно Подключение к Серверу интеграции**" на стр. 346), в котором вы можете настроить подключение к Серверу интеграции.

Окно Подключение к Серверу интеграции

В этом окне вы можете указать или изменить параметры подключения Легких агентов к Серверу интеграции.

Таблица 103. Параметры подключения к Серверу интеграции

Параметр	Описание
Адрес	IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции. Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен, в поле по умолчанию указано доменное имя этого устройства. Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или Сервер интеграции установлен на другом устройстве, поле требуется заполнить вручную. Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.
Порт	Порт для подключения к Серверу интеграции. По умолчанию указан порт 7271.

Окно Проверка сертификата Сервера интеграции

Это окно отображается, если SSL-сертификат, полученный от Сервера интеграции, содержит ошибку или не является доверенным.

С помощью ссылки в окне вы можете посмотреть информацию о полученном сертификате.

При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

Окно Аутентификация на Сервере интеграции

Это окно отображается, если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов.

Укажите пароль администратора Сервера интеграции (учетной записи admin) и нажмите на кнопку **ОК**.

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

После подключения к Серверу интеграции с правами администратора в политику автоматически передается пароль учетной записи `agent`, которая используется для подключения Легких агентов к Серверу интеграции.

kaspersky

Параметры обнаружения SVM

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

В этом окне вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM.

Таблица 104. Параметры обнаружения SVM

Параметр	Описание
Использовать Сервер интеграции	Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них. Если вы хотите использовать Сервер интеграции, вам нужно настроить параметры подключения Легких агентов к Серверу интеграции (см. раздел "Подключение к Серверу интеграции" на стр. 345).
Использовать список адресов SVM, заданный вручную	Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.
Список SVM	Список IP-адресов в формате IPv4 или полных доменных имен (FQDN) SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением политики. По нажатию на кнопку **Добавить** открывается окно, в котором вы можете указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки. Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения. Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**. Список адресов SVM отображается, если выбран вариант **Использовать список адресов SVM, заданный вручную**.

Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/index.htm), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** (на стр. 348) требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

Тег для подключения к SVM

В этом окне вы можете включить использование тегов Легким агентом и назначить тег, который Легкий агент будет использовать для подключения.

Убедитесь, что использование тегов для подключения также настроено в параметрах Сервера защиты. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254886.htm. Легкие агенты, которым назначен тег, могут подключаться только к SVM, для которых разрешено подключение Легких агентов с этим тегом.

Таблица 105. Параметры использования тегов для подключения

Параметр	Описание
Использовать теги для подключения Легких агентов	Флажок включает или выключает использование Легким агентом тегов для подключения к SVM.
Тег	Тег, который назначается Легким агентам. В качестве тега вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа `;`. Поле доступно, если установлен флажок **Использовать теги для подключения Легких агентов**.

Алгоритм выбора SVM

В этом окне вы можете указать, какой алгоритм выбора SVM должны использовать Легкие агенты для Linux, и настроить параметры применения расширенного алгоритма выбора SVM.

Таблица 106. Алгоритм выбора SVM

Параметр	Описание
Использовать стандартный алгоритм выбора SVM	Если выбран этот вариант, после установки и запуска на виртуальной машине Легкий агент выбирает для подключения SVM, которая является локальной для Легкого агента. Если нет доступных для подключения локальных SVM, Легкий агент выбирает SVM, к которой подключено наименьшее количество Легких агентов, независимо от расположения SVM в виртуальной инфраструктуре. Этот вариант выбран по умолчанию.
Использовать расширенный алгоритм выбора SVM	Если выбран этот вариант, вы можете указать с помощью ползунка **Расположение SVM**, как расположение SVM в виртуальной инфраструктуре будет учитываться при определении локальности SVM относительно Легкого агента. Легкий агент сможет подключаться только к тем SVM, которые являются локальными. Также вы можете указать, что расположение SVM в виртуальной инфраструктуре не должно учитываться при выборе SVM для подключения. При выборе SVM Легкие агенты учитывают количество Легких агентов, подключенных к этой SVM, чтобы обеспечить равномерное распределение Легких агентов между доступными для подключения SVM.

Расположение SVM	Позволяет указать тип расположения SVM в виртуальной инфраструктуре, который учитывается при выборе SVM для подключения: • **Гипервизор**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры): • SVM развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V®, Citrix Hypervisor, VMware vSphere™, KVM, Proxmox VE, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации или Astra Linux). • SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением Облачной платформы ТИОНИКС или платформы OpenStack®). Если на том же гипервизоре или в той же Группе серверов, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM. • **Кластер**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры): • SVM развернута в том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, Citrix Hypervisor, VMware vSphere, KVM, Proxmox VE, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации или Astra Linux). • SVM развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением Облачной платформы ТИОНИКС или платформы OpenStack). Если в том же кластере гипервизоров или в рамках того же проекта OpenStack, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM. • **Дата-центр**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры): • SVM развернута в том же дата-центре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, Citrix Hypervisor, VMware vSphere, KVM, Proxmox VE, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis или Альт Сервер Виртуализации). • SVM расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением Облачной платформы ТИОНИКС или платформы OpenStack). Если в том же дата-центре или в той же Зоне доступности, где расположена виртуальная машина с Легким агентом, нет доступных для подключения

Параметр	Описание
	SVM, Легкий агент не подключается к SVM. • **Не учитывать расположение SVM**. Легкий агент не учитывает при выборе SVM ее расположение. По умолчанию выбрано значение **Гипервизор**. Параметр доступен, если выбран вариант **Использовать расширенный алгоритм выбора SVM**.

Если для Легкого агента применяется расширенный алгоритм выбора SVM и в качестве способа обнаружения SVM (см. раздел "Параметры обнаружения SVM" на стр. 347) выбран список адресов SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/index.htm), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. Требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

Защита соединения

В этом окне вы можете включить шифрование канала передачи данных между Легким агентом и Сервером защиты.

Убедитесь, что шифрование канала передачи данных между Легким агентом и Сервером защиты включено в параметрах Сервера защиты на SVM. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254886.htm.

Таблица 107. Параметры защиты соединения

Параметр	Описание
Шифровать канал передачи данных между Легким агентом и Сервером защиты	Защитить соединение между Легкими агентами и Сервером защиты с помощью шифрования. Если флажок установлен, между Легким агентом, находящимся под управлением политики, и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается защищенное соединение. Легкий агент, для которого включена защита соединения, может подключиться только к SVM, на которой также включена защита соединения или разрешено незащищенное соединение с Сервером защиты. Если флажок снят, между Легким агентом и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается незащищенное соединение. По умолчанию флажок снят.

Управление задачами в Консоли администрирования

Задачи выполняются, только если на устройствах запущено приложение Kaspersky Endpoint Security (см. раздел "Запуск и остановка приложения на клиентском устройстве" на стр. 272).

Вы можете создавать следующие задачи для работы с приложением Kaspersky Endpoint Security через Консоль администрирования Kaspersky Security Center:

- локальные задачи, определенные для отдельного устройства;
- групповые задачи, определенные для устройств, входящих в группы администрирования;
- задачи для наборов устройств, не входящих 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 набора устройств и локальных задач.

Задачи Добавление ключа, Обновление и Откат обновления баз неприменимы, если приложение используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23).

Вы можете выполнять следующие действия над задачами:

- Запускать, останавливать, приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление выполнения задачи вручную" на стр. 353) выполнение задач.

  Задачу Обновление невозможно приостановить и возобновить, ее можно только запустить или остановить.
- Создавать новые задачи.
- Изменять 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.
- Сравнивать версии задач в окне свойств задачи в разделе **История ревизий**.

Общая информация о задачах Консоли администрирования приведена в документации Kaspersky Security Center.

kaspersky

В этом разделе

Создание локальной задачи

► *Чтобы создать локальную задачу:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
3. В рабочей области выберите закладку **Устройства**.
4. В списке управляемых устройств выберите устройство, для которого вы хотите создать локальную задачу, и в контекстном меню устройства выберите пункт **Свойства**.
5. В окне **Свойства: <Имя устройства>** выберите раздел **Задачи**.
6. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
7. Следуйте указаниям мастера создания задачи.

Создание групповой задачи

► *Чтобы создать групповую задачу:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Задачи**.
3. В рабочей области нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.

Создание задачи для наборов устройств

► *Чтобы создать задачу для наборов устройств:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Задачи**.
3. В рабочей области нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.
5. В окне мастера **Выбор устройств, которым будет назначена задача** нажмите на кнопку **Назначить задачу выборке устройств**.
6. В следующем окне мастера нажмите на кнопку **Обзор**.

   Откроется окно **Выборка устройств**.
7. Выберите нужные устройства и нажмите на кнопку **ОК** в окне **Выборка устройств**.
8. Нажмите на кнопку **Далее** и следуйте указаниям мастера создания задачи.

Запуск, остановка, приостановка и возобновление выполнения задачи вручную

Если на клиентском устройстве запущено приложение (см. раздел "Запуск и остановка приложения на клиентском устройстве" на стр. 272) Kaspersky Endpoint Security, вы можете запустить / остановить / приостановить / возобновить выполнение задачи на этом клиентском устройстве через Kaspersky Security Center. Если приложение Kaspersky Endpoint Security остановлено, выполнение запущенных задач прекращается, а управлять запуском, остановкой, приостановкой и возобновлением задач через Kaspersky Security Center невозможно.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение локальной задачи:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
3. В рабочей области выберите закладку **Устройства**.
4. В списке управляемых устройств выберите устройство, на котором вы хотите запустить / остановить / приостановить / возобновить выполнение локальной задачи.
5. В контекстном меню устройства выберите пункт **Свойства**.
6. В окне **Свойства: <Имя устройства>** выберите раздел **Задачи**.

   В правой части окна отобразится список локальных задач.
7. Выберите локальную задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
8. Выполните одно из следующих действий:

- В контекстном меню локальной задачи выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.
- Нажмите на кнопку  /  справа от списка локальных задач, чтобы запустить или остановить локальную задачу.
- Нажмите на кнопку **Свойства** под списком локальных задач и в открывшемся окне **Свойства: <Название локальной задачи>** на закладке **Общие** нажмите на кнопку **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение групповой задачи:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием группы администрирования, для которой вы хотите запустить / остановить / приостановить / возобновить выполнение групповой задачи.
3. В рабочей области выберите закладку **Задачи**.

   В правой части окна отобразится список групповых задач.
4. Выберите групповую задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
5. В контекстном меню групповой задачи выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

Изменение параметров локальной задачи

► *Чтобы изменить параметры локальной задачи:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
3. В рабочей области выберите закладку **Устройства**.
4. В списке управляемых устройств выберите устройство, для которого вы хотите настроить параметры приложения, и в контекстном меню устройства выберите пункт **Свойства**.
5. В окне **Свойства: <Имя устройства>** выберите раздел **Задачи**.

   В правой части окна отобразится список локальных задач.
6. Выберите нужную локальную задачу и в контекстном меню задачи выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название локальной задачи>**.
7. Измените параметры локальной задачи.
8. В окне **Свойства: <Название локальной задачи>** нажмите на кнопку **ОК**, чтобы сохранить изменения.

Количество и содержимое разделов зависит от типа выбранной задачи. Содержимое разделов **Общие**, **Уведомление**, **Расписание** и **История ревизий** одинаковое для всех задач. Более подробное описание этих разделов приведено в документации к Kaspersky Security Center.

Изменение параметров групповой задачи

► *Чтобы изменить параметры групповой задачи:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием нужной группы администрирования.
3. В рабочей области выберите закладку **Задачи**.
4. В списке групповых задач выберите нужную групповую задачу и в контекстном меню задачи выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название групповой задачи>**.
5. Измените параметры групповой задачи.
6. В окне **Свойства: <Название групповой задачи>** нажмите на кнопку **ОК**, чтобы сохранить изменения.

Количество и содержимое разделов зависит от типа выбранной задачи. Содержимое разделов **Общие**, **Уведомление**, **Расписание** и **История ревизий** одинаковое для всех задач. Более подробное описание этих разделов приведено в документации к Kaspersky Security Center.

Изменение параметров задачи для наборов устройств

► *Чтобы изменить параметры задачи для наборов устройств:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи**.
3. В рабочей области папки **Задачи** в списке задач выберите задачу для наборов устройств, параметры которой вы хотите изменить, и в контекстном меню задачи выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название задачи>**.
4. Измените параметры задачи для наборов устройств.
5. Нажмите на кнопку **ОК** в окне **Свойства: <Название задачи>**.

Количество и содержимое разделов зависит от типа выбранной задачи. Содержимое разделов **Общие**, **Уведомление**, **Расписание** и **История ревизий** одинаковое для всех задач. Более подробное описание этих разделов приведено в документации к Kaspersky Security Center.

Параметры задач

Для управления приложением Kaspersky Endpoint Security в Kaspersky Security Center предусмотрены задачи следующих типов:

- **Поиск вредоносного ПО** (на стр. 363). Во время выполнения задачи приложение проверяет области устройства, указанные в параметрах задачи, на вирусы и другие вредоносные программы.
- **Добавление ключа** (на стр. 356). Во время выполнения задачи приложение добавляет ключ, в том числе резервный, для активации приложения.
- **Инвентаризация** (на стр. 358). Во время выполнения задачи приложение получает информацию обо всех исполняемых файлах приложений, хранящихся на устройствах.

- **Обновление** (на стр. 361). Во время выполнения задачи приложение обновляет базы в соответствии с настроенными параметрами обновления.
- **Откат обновления баз** (на стр. 363). Во время выполнения задачи приложение откатывает последнее обновление баз.
- **Проверка важных областей** (на стр. 370). Во время выполнения задачи приложение проверяет загрузочные секторы, объекты автозапуска, память процессов и память ядра.
- **Проверка контейнеров** (на стр. 377). Во время выполнения задачи приложение проверяет контейнеры и образы на вирусы и другие вредоносные программы.
- **Проверка целостности системы** (на стр. 382). 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.

Набор параметров и значения по умолчанию для параметров задач зависят от типа лицензии. Задачи Добавление ключа, Обновление и Откат обновления баз неприменимы, если приложение используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23).

В этом разделе

Добавление ключа

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), активация приложения с помощью задачи Добавление ключа не поддерживается.

Если приложение Kaspersky Endpoint Security используется в автономном режиме, с помощью задачи Добавление ключа вы можете добавить лицензионный ключ для активации приложения.

Таблица 108. Параметры задачи Добавление ключа

Параметр	Описание
Использовать ключ в качестве резервного	Флажок включает или выключает использование ключа в качестве резервного. Если флажок установлен, приложение использует ключ в качестве резервного. Если флажок снят, приложение использует ключ в качестве активного. По умолчанию флажок снят. Флажок недоступен, если вы добавляете ключ для пробной лицензии или ключ по подписке. Ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве резервного ключа.
Выбрать ключ	При нажатии на кнопку открывается окно **Хранилище ключей Kaspersky Security Center** (см. раздел "**Окно Хранилище ключей Kaspersky Security Center**" на стр. 357). В этом окне вы можете выбрать ключ, ранее добавленный в хранилище ключей Kaspersky Security Center, а также добавить ключ в хранилище ключей Kaspersky Security Center.
Информация о лицензии	В этом блоке приведены данные о ключе и связанной с ним лицензии: • **Лицензионный ключ** – уникальная буквенно-цифровая последовательность. Вы можете использовать приложение только при наличии в нем ключа. • **Тип лицензии** – пробная, коммерческая или коммерческая (подписка). • **Срок действия лицензии** – количество дней, в течение которых возможно использование приложения, активированного путем добавления этого ключа (например, 365 дней). Информация не отображается, если вы используете приложение по подписке. • **Льготный период** – количество дней после приостановки подписки, в течение которых приложение продолжает выполнять все свои функции. Поле отображается, если вы используете приложение по подписке, и поставщик услуг, у которого вы зарегистрировали подписку, предоставляет льготный период для продления подписки. • **Действует до** – дата и время окончания срока использования приложения, активированного путем добавления этого ключа, в формате UTC. Если вы используете приложение по неограниченной подписке, дата окончания срока действия лицензии не указывается. • **Ограничение** – максимальное количество устройств, которые приложение может защищать. • **Описание** – описание лицензии.

Окно Хранилище ключей Kaspersky Security Center

В этом окне вы можете выбрать ключ, ранее добавленный в хранилище ключей Kaspersky Security Center, а также добавить ключ в хранилище ключей Kaspersky Security Center.

Таблица 109. Параметры окна Хранилище ключей Kaspersky Security Center

Параметр	Описание
Таблица ключей	Таблица содержит ключи, добавленные в хранилище ключей Kaspersky Security Center, и состоит из следующих столбцов: • **Тип лицензии** – тип лицензии: пробная, коммерческая или коммерческая (подписка). • **Действует до** – дата окончания срока использования приложения, активированного путем добавления этого ключа. • **Срок действия лицензии** – количество дней, в течение которых возможно использование приложения, активированного путем добавления этого ключа (например, 365 дней). Информация не отображается, если вы используете приложение по подписке. • **Ограничение** – максимальное количество устройств, которые приложение может защищать. • **Описание** – описание лицензии. • **Лицензионный ключ** – уникальная буквенно-цифровая последовательность.
Добавить ключ	При нажатии на кнопку запускается мастер добавления лицензионного ключа. Ключ будет добавлен в хранилище ключей Kaspersky Security Center. После добавления ключа информация о нем будет отображаться в таблице ключей.

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. 244).

Для использования задачи требуется лицензия, которая включает эту функцию.

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 Endpoint Security файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

Таблица 110. 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. 244) 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 pyc). 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**.

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 111. 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.

Окно <Название области проверки>

В этом окне вы можете добавить или настроить область проверки для задачи Инвентаризация.

Таблица 112. Параметры области инвентаризации

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.

Параметр	Описание
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.

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 113. 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 <Название области исключения>

В этом окне вы можете добавить или настроить область исключения из проверки для задачи Инвентаризация.

Таблица 114. 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. 293). 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.

Обновление

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), не поддерживается обновление баз и модулей приложения с помощью задачи, созданной в Kaspersky Security Center. Обновление выполняется с помощью локальной предустановленной задачи.

Обновление баз и модулей приложения Kaspersky Endpoint Security обеспечивает актуальность защиты устройства. Каждый день в мире появляются новые вирусы 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 приложения.

Источник обновлений – это ресурс, содержащий обновления баз и модулей приложения Kaspersky Endpoint Security. Источником обновлений могут быть HTTP-, HTTPS- или FTP-серверы (например, серверы обновлений Kaspersky Security Center и "Лаборатории Касперского"), а также локальные или сетевые директории, смонтированные пользователем.

Таблица 115. Параметры источников 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.

В разделе **Параметры** вы можете указать время ожидания ответа и параметры загрузки обновлений приложения.

Таблица 116. Дополнительные 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**.

Откат обновления баз

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), откат обновления баз с помощью задачи не поддерживается.

После первого обновления баз приложения становится доступна функция отката баз приложения к их предыдущей версии.

Каждый раз, когда пользователь запускает процесс обновления, приложение Kaspersky Endpoint Security 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 Endpoint Security.

Задача Откат обновления баз не имеет параметров.

Поиск вредоносного ПО

Поиск вредоносного ПО – это однократная полная или выборочная проверка файлов на устройстве, выполняемая приложением. Приложение может выполнять несколько задач поиска вредоносного ПО одновременно.

По умолчанию в приложении создается одна стандартная задача поиска вредоносного ПО – полная проверка. Во время выполнения полной проверки 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.

Во время полной проверки диска процессор будет занят. Рекомендуется запускать задачу полной проверки в нерабочее время.

Таблица 117. 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, параметры области проверки (см. раздел "Проверка важных областей" на стр. 370) и параметры проверки (см. раздел "Окно Параметры проверки" на стр. 289).
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. 370), в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В разделе **Исключения** для задачи Поиск вредоносного ПО вы также можете настроить области исключения (см. раздел "Окно Области исключения" на стр. 293), исключения по маске (см. раздел "Окно Исключения по маске" на стр. 295) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 295).

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 118. 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 <Название области проверки>

В этом окне вы можете добавить или настроить область проверки.

Таблица 119. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.

Параметр	Описание
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 Поиск вредоносного ПО. Приложение позволяет проверять файлы, загрузочные секторы, память устройства и объекты автозапуска.

Таблица 120. 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. 367), 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.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Таблица 121. 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 *самораспаковывающихся архивов*. 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 *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. 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. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. 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 устройств.

Окно Действие при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Таблица 122. 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 сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
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 сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в 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).

Проверка важных областей

Задача Проверка важных областей позволяет проверять файлы, загрузочные секторы, объекты автозапуска, память процессов и память ядра.

Таблица 123. 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, параметры области проверки (см. раздел "Проверка важных областей" на стр. 370) и параметры проверки (см. раздел "Окно Параметры проверки" на стр. 289).
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** для задачи Проверка важных областей вы также можете настроить области исключения (см. раздел "Окно Области исключения" на стр. 293), исключения по маске (см. раздел "Окно Исключения по маске" на стр. 295) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 295).

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 124. 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 <Название области проверки>

В этом окне вы можете добавить или настроить область проверки.

Таблица 125. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.

Параметр	Описание
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 126. Параметры области проверки

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, Kaspersky Endpoint Security проверяет файлы. Если флажок снят, Kaspersky Endpoint Security не проверяет файлы. По умолчанию флажок снят.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, Kaspersky Endpoint Security проверяет загрузочные секторы. Если флажок снят, Kaspersky Endpoint Security 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 Endpoint Security проверяет память ядра и запущенные процессы. Если флажок снят, Kaspersky Endpoint Security 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 Endpoint Security проверяет объекты автозапуска. Если флажок снят, Kaspersky Endpoint Security 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. 367), 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.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Таблица 127. 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 *самораспаковывающихся архивов*. 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 *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. 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. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. 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 устройств.

Окно Действие при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

Таблица 128. 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 сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
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 сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в 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).

Проверка контейнеров

Во время работы задачи Проверка контейнеров приложение Kaspersky Endpoint Security проверяет контейнеры и образы на наличие вирусов и других вредоносных программ. Вы можете одновременно запустить несколько задач Проверка контейнеров.

Поддерживается интеграция с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Для использования задачи требуется лицензия, которая включает эту функцию.

Таблица 129. 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. 378) и общие параметры проверки (см. раздел "Окно Параметры проверки" на стр. 367).
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. 382) для задачи Проверка контейнеров вы также можете настроить исключения по маске (см. раздел "Окно Исключения по маске" на стр. 295) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 295).

Окно Параметры проверки контейнеров

В этом окне вы можете настроить параметры проверки контейнеров и образов.

Таблица 130. 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**.

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	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 131. 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 *самораспаковывающихся архивов*. 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.

Параметр	Описание
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.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.

Параметр	Описание
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. 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. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.
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 Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Таблица 132. 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 сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
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 сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в 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 133. 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. 295). 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. 295). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Проверка целостности системы

В процессе выполнения задачи Проверка целостности системы (ODFIM) изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве *снимка состояния системы*.

Для использования задачи требуется лицензия, которая включает эту функцию.

Снимок состояния системы создается во время первого выполнения задачи ODFIM на устройстве. Вы можете создать несколько задач ODFIM. Для каждой задачи ODFIM создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы относится к области мониторинга. Если снимок состояния системы не соответствует области мониторинга, приложение формирует событие о нарушении целостности системы.

Снимок состояния системы создается заново после завершения задачи ODFIM. Вы можете заново создать снимок состояния системы для задачи с помощью соответствующего параметра. Снимок состояния системы также создается при изменении параметров задачи, например, при добавлении новой области мониторинга. При следующем выполнении задачи снимок состояния системы формируется заново. Вы можете удалить снимок состояния системы, удалив соответствующую задачу ODFIM.

Таблица 134. 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 (SHA-256) для проверки	Флажок включает или выключает использование хеша SHA-256 для задачи Проверка целостности системы. SHA-256 – это криптографическая хеш-функция, которая формирует 256-разрядное хеш-значение. 256-разрядное хеш-значение представляет собой последовательность из 64 шестнадцатеричных цифр. Если флажок снят, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром). По умолчанию флажок снят.
Следить за директориями в областях мониторинга	Флажок включает или выключает проверку указанных директорий во время выполнения задачи Проверка целостности системы. По умолчанию флажок снят.
Следить за временем последнего доступа к файлу	Флажок включает или выключает отслеживание времени доступа к файлу во время выполнения задачи Проверка 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. 319).

В разделе **Области исключения** (см. раздел "**Раздел Области исключения**" на стр. 385) для задачи Проверка целостности системы вы также можете настроить области исключения из мониторинга (см. раздел "Окно Области исключения" на стр. 320) и исключения по маске (см. раздел "Окно Исключения по маске" на стр. 321).

Окно Области проверки

Таблица содержит области мониторинга для задачи Проверка целостности системы. Kaspersky Endpoint Security контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/).

Таблица 135. 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 Endpoint Security 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 <Название области проверки>

В этом окне вы можете добавить или настроить области мониторинга для задачи Проверка целостности системы.

Таблица 136. 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. 432). 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.

Параметр	Описание
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, /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 /opt/kaspersky/kesl.
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 137. 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. 320). 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. 321). 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 138. Параметры области исключения из проверки 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 поверки при работе задачи.

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 задачи Проверка целостности системы.

Таблица 139. 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. 385). 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.

Параметр	Описание
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.

Проверка соединения с Сервером администрирования вручную. Утилита klnagchk

В комплект поставки Агента администрирования входит утилита klnagchk, предназначенная для проверки подключения к Серверу администрирования.

После установки Агента администрирования утилита расположена в директории /opt/kaspersky/klnagent/bin в 32-битной операционной системе и в директории /opt/kaspersky/klnagent64/bin в 64-битной операционной системе. В зависимости от используемых ключей Агент администрирования выполняет следующие действия при запуске:

- записывает в файл журнала событий или выводит на экран значения параметров подключения Агента администрирования, установленного на клиентском устройстве, к Серверу администрирования;
- записывает в файл журнала событий или выводит на экран статистику Агента администрирования (с момента его последнего запуска) и результаты выполнения утилиты;
- предпринимает попытку установить соединение Агента администрирования с Сервером администрирования;
- если соединение установить не удалось, посылает ICMP-пакет для проверки статуса устройства, на котором установлен Сервер администрирования.

Синтаксис утилиты

```
klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>] [-restart]
```

Описание ключей

- `-logfile <имя файла>` – записать значения параметров подключения Агента администрирования к Серверу администрирования и результаты работы утилиты в файл журнала событий. Если этот ключ не используется, параметры, результаты и сообщения об ошибках отображаются на экране.
- `-sp` – показать пароль аутентификации пользователя на прокси-сервере. Этот параметр используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.
- `-savecert <имя файла>` – сохранить сертификат, используемый для проверки доступа к Серверу администрирования, в указанном файле.
- `-restart` – перезапустить Агент администрирования.

kaspersky

Подключение к Серверу администрирования вручную. Утилита klmover

В комплект поставки Агента администрирования входит утилита klmover, предназначенная для управления подключением к Серверу администрирования.

После установки Агента администрирования утилита расположена в директории /opt/kaspersky/klnagent/bin в 32-битной операционной системе и в директории /opt/kaspersky/klnagent64/bin в 64-битной операционной системе. В зависимости от используемых ключей Агент администрирования выполняет следующие действия при запуске:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает в файл журнала событий или выводит на экран результаты выполнения операции.

Синтаксис утилиты

```
klmover [-logfile <имя файла>] {-address <адрес сервера>} [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>] [-silent] [-dupfix]
```

Описание ключей

- `-logfile <имя файла>` – записать результаты работы утилиты в указанный файл. Если этот ключ не используется, результаты и сообщения об ошибках выводятся в stdout.
- `-address <адрес сервера>` – адрес Сервера администрирования, используемого для подключения. Это может быть IP-адрес, NetBIOS или DNS-имя устройства.
- `-pn <номер порта>` – номер порта, по которому устанавливается незашифрованное соединение с Сервером администрирования. По умолчанию используется порт 14000.
- `-ps <номер SSL-порта>` – номер SSL-порта, по которому устанавливается зашифрованное соединение с Сервером администрирования по протоколу SSL. По умолчанию используется порт 13000.
- `-nossl` – использовать незашифрованное соединение с Сервером администрирования. Если этот ключ не указан, Агент соединяется с Сервером администрирования через зашифрованный протокол SSL.
- `-cert <путь к файлу сертификата>` – использовать указанный файл сертификата для аутентификации доступа к новому Серверу администрирования. Если ключ не используется, Агент администрирования получит сертификат при первом подключении к Серверу администрирования.
- `-silent` – запустить утилиту в неинтерактивном режиме. Использование ключа может быть полезно, например, при запуске утилиты из сценария запуска при регистрации пользователя.
- `-dupfix` – этот файл ключа используется, если способ установки Агента администрирования отличается от способа установки в составе комплекте поставки, например, восстановление с диска.
- `-cloningmode 1` – перейти в режим клонирования.
- `-cloningmode 0` – выйти из режима клонирования.

Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center

Утилита удаленной диагностики Kaspersky Security Center (далее – утилита удаленной диагностики) предназначена для удаленного выполнения на клиентских устройствах следующих операций:

- включения и выключения трассировки;
- изменения уровня трассировки;
- загрузки файла трассировки;
- загрузки журнала удаленной установки приложения;
- загрузки системных журналов событий (syslog).

Утилита удаленной диагностики автоматически устанавливается на устройство совместно с Консолью администрирования.

Подробнее об утилите удаленной диагностики см. в документации Kaspersky Security Center https://support.kaspersky.com/KSC/14.2/ru-RU/13052.htm.

► *Чтобы открыть главное окно утилиты удаленной диагностики к клиентскому устройству:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
3. В рабочей области выберите закладку **Устройства**.
4. 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 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. В главном окне утилиты удаленной диагностики нажмите на кнопку **Войти**.
3. В открывшемся окне в дереве объектов выберите директорию **Журналы удаленной установки**.

kaspersky

Управление приложением с помощью Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console

Этот раздел содержит информацию об управлении приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console.

Описание приведено для версии Kaspersky Security Center 14.2.

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. Дополнительная информация о Kaspersky Security Center Web Console приведена в документации Kaspersky Security Center.

С помощью Kaspersky Security Center Web Console можно выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- устанавливать приложения "Лаборатории Касперского" на устройства вашей сети;
- управлять установленными приложениями;
- просматривать отчеты о состоянии системы безопасности.

Управление приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console осуществляется с помощью веб-плагина управления Kaspersky Endpoint Security (см. раздел "О веб-плагине управления Kaspersky Endpoint Security" на стр. 49).

Чтобы управлять работой приложения Kaspersky Endpoint Security, установленного на устройствах, через Kaspersky Security Center Web Console, вам нужно поместить эти устройства в группы администрирования. Вы можете создать группы администрирования в Kaspersky Security Center перед началом установки приложения Kaspersky Endpoint Security и настроить правила автоматического перемещения устройств в группы администрирования. Или вы можете вручную переместить устройства в группы администрирования после установки приложения Kaspersky Endpoint Security (см. подробнее в документации Kaspersky Security Center).

Kaspersky Security Center Cloud Console – это облачная версия приложения Kaspersky Security Center. То есть Сервер администрирования и другие компоненты Kaspersky Security Center установлены в облачной инфраструктуре "Лаборатории Касперского". Управление приложением Kaspersky Security Center Cloud Console осуществляется с помощью облачной Консоли администрирования, которая называется Kaspersky Security Center Cloud Console. Эта консоль имеет интерфейс, аналогичный интерфейсу Kaspersky Security Center Web Console.

Использование Kaspersky Security Center Cloud Console приводит к выходу приложения из сертифицированного состояния.

kaspersky

В этом разделе

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.

kaspersky

Запуск и остановка приложения на клиентском устройстве

После установки приложения Kaspersky Endpoint Security на устройство пользователя запуск приложения выполняется автоматически. Далее по умолчанию запуск приложения выполняется сразу после запуска операционной системы.

Вы можете контролировать статус работы приложения с помощью веб-виджета **Состояние защиты** в окне **Мониторинг и отчеты / Панель мониторинга**.

► *Чтобы запустить или остановить приложение дистанционно:*

1. В главном окне Web Console выберите **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 **Программы**.
4. Установите флажок напротив приложения **Kaspersky Endpoint Security 12.0 для Linux**.
5. Нажмите на кнопку **Запустить** или **Остановить**.

Просмотр состояния защиты устройства

► *Чтобы просмотреть состояние защиты устройства:*

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.

   Откроется список управляемых устройств.
2. В списке выберите устройство, информацию о котором вы хотите просмотреть, и по ссылке с названием устройства откройте окно свойств устройства.
3. На закладке **Общие** выберите раздел **Защита**.

В разделе **Защита** отображается следующая информация о выбранном устройстве:

- **Видимо в сети** – видимость выбранного устройства в сети: *Да* или *Нет*.
- **Статус устройства** – текущий статус выбранного устройства: *OK*, *Критический* или *Предупреждение*.
- **Описание статуса** – причины смены статуса устройства на *Критический* или *Предупреждение*.
- **Состояние защиты** – статус задачи Защита от файловых угроз, 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 Endpoint Security.
- **Объекты, которые не удалось вылечить** – количество зараженных объектов, которые приложению Kaspersky Endpoint Security не удалось вылечить.

kaspersky

Обновление баз и модулей приложения

Процедура обновления баз и модулей Kaspersky Endpoint Security зависит от режима использования приложения (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23). В этом разделе описана процедура обновления приложения в автономном режиме. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается обновление баз и модулей приложения с помощью задачи, созданной в Kaspersky Security Center. Обновление выполняется с помощью локальной предустановленной задачи.

Обновление баз и модулей приложения Kaspersky Endpoint Security 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 Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы приложения.

На устройствах пользователей обновляются 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.
- 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.

  Допускается устанавливать только обновления модулей приложения, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу приложения из сертифицированного состояния.

Приложение Kaspersky Endpoint Security поддерживает следующие схемы обновления баз:

- Обновление с серверов "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.
- 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.

     Загрузку пакета обновлений в хранилище 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 Endpoint Security *Обновление* (на стр. 476). Вы можете создать неограниченное количество задач обновления для каждой из групп администрирования.

Для Web Console по умолчанию список источников обновлений содержит серверы обновлений "Лаборатории Касперского" и Сервер администрирования Kaspersky Security Center. Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений вы можете

указывать FTP-, HTTP- или HTTPS-серверы. Если обновление не может быть выполнено с одного источника обновлений, приложение Kaspersky Endpoint Security переключается к следующему источнику.

Загрузка обновлений с серверов обновлений "Лаборатории Касперского" или с других FTP-, HTTP- или HTTPS-серверов осуществляется по стандартным сетевым протоколам. Если для доступа к источникам обновлений требуется подключение к прокси-серверу, укажите параметры прокси-сервера (на стр. 448) в параметрах политики Kaspersky Endpoint Security.

В этом разделе

Обновление из хранилища Сервера администрирования

Для экономии интернет-трафика вы можете настроить обновление баз и модулей приложения на устройствах локальной сети организации из серверного хранилища. Для этого требуется настроить в Kaspersky Security Center загрузку пакета обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования. В этом случае остальные устройства локальной сети организации смогут получать пакет обновлений из серверного хранилища.

Настройка обновления баз и модулей приложения из серверного хранилища состоит из следующих этапов:

1. Загрузка баз и модулей приложения в хранилище Сервера администрирования с помощью задачи Kaspersky Security Center *Загрузка обновлений в хранилище Сервера администрирования*.
2. Настройка обновления баз и модулей приложения из хранилища Сервера администрирования на остальных клиентских устройствах с помощью задачи *Обновление* (см. раздел "*Обновление*" на стр. 476).

► *Чтобы настроить обновление баз и модулей приложения из хранилища* Сервера администрирования*:*

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. В списке задач выберите задачу **Обновление** (на стр. 476) приложения Kaspersky Endpoint Security и по ссылке с названием задачи откройте окно свойств задачи.

   Задача Обновление создается автоматически мастером первоначальной настройки Web Console. Для создания задачи Обновление во время работы мастера установите веб-плагин Kaspersky Endpoint Security.

3. В окне свойств задачи выберите закладку **Параметры программы**.
4. В списке слева выберите раздел **Источник обновлений баз**.

   В правой части окна отобразятся параметры задачи.

5. В блоке **Источник обновлений баз** выберите вариант **Сервер администрирования Kaspersky Security Center**.
6. Установите флажок **Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны**, если вы хотите, чтобы в случае недоступности

хранилища Сервера администрирования задача Обновление использовала серверы обновлений "Лаборатории Касперского".

7. Нажмите на кнопку **Сохранить**.

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. В этом случае остальные устройства локальной сети организации смогут получать пакет обновлений из общей директории.

Настройка обновления баз и модулей приложения из общей директории состоит из следующих этапов:

1. Установка Kaspersky Update Utility на одном из устройств локальной сети организации.
2. Настройка копирования пакета обновлений в общую директорию в параметрах Kaspersky Update Utility.
3. Настройка обновления баз и модулей приложения из указанной общей директории на остальных устройствах локальной сети организации.

Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта службы технической поддержки "Лаборатории Касперского" https://support.kaspersky.ru/updater3. После установки утилиты 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.

► *Чтобы настроить обновление из общей директории:*

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. В списке задач выберите задачу **Обновление** приложения Kaspersky Endpoint Security и по ссылке с названием задачи откройте окно свойств задачи.

   Задача Обновление создается автоматически мастером первоначальной настройки Web Console. Для создания задачи Обновление во время работы мастера установите веб-плагин Kaspersky Endpoint Security.

3. В окне свойств задачи выберите закладку **Параметры программы**.
4. В списке слева выберите раздел **Источник обновлений баз**.

   В правой части окна отобразятся параметры задачи.

5. В блоке **Источник обновлений баз** выберите вариант **Другие источники в локальной или глобальной сети**.
6. В таблице источников обновлений нажмите на кнопку **Добавить**.
7. В поле **Источник обновлений** укажите путь к общей директории.

   Адрес источника должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.

8. Установите флажок **Использовать этот источник** и нажмите на кнопку **ОК**.
9. В таблице источников обновлений настройте порядок их использования с помощью кнопок **Вверх** и **Вниз**.
10. Нажмите на кнопку **Сохранить**.

Использование прокси-сервера при обновлении

Для загрузки обновлений баз и модулей приложения из источника обновлений может потребоваться указать параметры прокси-сервера. Если источников обновлений несколько, параметры прокси-сервера применяются для всех источников. Если для некоторых источников обновлений прокси-сервер не нужен, вы можете выключить использование прокси-сервера в параметрах политики Kaspersky Endpoint Security. Приложение также будет использовать прокси-сервер для доступа к Kaspersky Security Network и серверам активации.

► *Чтобы включить использование прокси-сервера для определенной группы администрирования:*

1. В главном окне Web Console выберите закладку **Устройства** → **Политики и профили**.
2. В списке политик выберите политику Kaspersky Endpoint Security для группы администрирования, на устройствах которой вы хотите выключить использование прокси-сервера, и по ссылке с названием политики откройте окно свойств политики.
3. В окне свойств политики выберите закладку **Параметры программы**.
4. Выберите раздел **Общие параметры** → **Параметры прокси-сервера** (на стр. 448).
5. В блоке **Параметры прокси-сервера** выберите вариант **Использовать параметры указанного прокси-сервера** и укажите параметры нужного прокси-сервера.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**.

Управление политиками в Web Console

Политика – это набор параметров работы приложения Kaspersky Endpoint Security, которые применяются для группы администрирования. С помощью политик вы можете установить одинаковые значения параметров работы приложения Kaspersky Endpoint Security 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 (см. раздел "Создание политики" на стр. 398) все остальные политики в группе администрирования становятся неактивными. Вы можете изменить статус политики (см. раздел "Изменение статуса политики" на стр. 401) 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.

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

- Если параметр закрыт "замком" (), это означает, что вы не можете изменить значение параметра локально. Для всех клиентских устройств группы администрирования используется значение параметра, заданное политикой.
- Если параметр не закрыт "замком" (), это означает, что вы можете изменить значение параметра локально. Для всех клиентских устройств группы администрирования используются значения параметра, заданные локально. Значение параметра, заданное в политике, не применяется.

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

Вы можете выполнять следующие действия с политиками:

- Создавать политику (см. раздел "Создание политики" на стр. 398).
- Изменять параметры политики (см. раздел "Изменение параметров политики" на стр. 400).

  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.
- Удалять политику (см. раздел "Удаление политики" на стр. 402).
- Изменять статус политики (см. раздел "Изменение статуса политики" на стр. 401).
- Копировать и перемещать политику (см. раздел "Действия с политиками" на стр. 401).
- Экспортировать и импортировать политику (см. раздел "Действия с политиками" на стр. 401).
- Сравнивать версии политик в окне свойств политики в разделе **История ревизий**.

Кроме того, вы можете создавать *профили политики*. 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**.

Общая информация о работе с политиками и профилями политик приведена в документации Kaspersky Security Center.

В этом разделе

kaspersky

Создание политики

► *Чтобы создать политику:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую клиентские устройства, для которых должна применяться политика. Для этого нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только политики, настроенные для выбранной группы администрирования.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.

4. В открывшемся окне в списке выберите **Kaspersky Endpoint Security 12.0 для Linux**.

   Перейдите к следующему шагу мастера.

5. Примите решение об использовании Kaspersky Security Network (на стр. 423). 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. Укажите, в каком режиме вы используете приложение Kaspersky Endpoint Security:

   - **Автономный режим** – приложение используется для защиты устройств под управлением операционных систем Linux.
   - **Режим Легкого агента для защиты виртуальных сред** – приложение используется в составе решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.

7. Если вы используете приложение в режиме Легкого агента для защиы виртуальных сред, настройте параметры обнаружения SVM:

   a. Выберите способ, который используют Легкие агенты для обнаружения доступных для подключения SVM:

      - **Использовать Сервер интеграции**

        Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них.

      - **Использовать список адресов SVM, заданный вручную**

        Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие

агенты будут подключаться только к SVM, указанным в списке.

Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/index.htm), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** (на стр. 465) требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

b. Если вы выбрали Сервер интеграции, в окне мастера отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. Если требуется, укажите новые параметры подключения:

   a. Нажмите на кнопку **Настроить** и укажите новые параметры подключения в открывшемся окне:

      - **Адрес**

        IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

        Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

      - **Порт**

        Порт для подключения к Серверу интеграции.

        По умолчанию указан порт 7271.

   b. Нажмите на кнопку **Проверить**.

   c. Веб-плагин проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, в окне **Подключение к Серверу интеграции** отображается сообщение об этом.

      Вы можете посмотреть информацию о сертификате, полученном от Сервера интеграции, нажав на строку **Посмотреть полученный сертификат**. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

      Чтобы сохранить полученный сертификат и продолжить подключение к Серверу интеграции, в блоке **Выбор действия** выберите вариант **Игнорировать**.

   d. Укажите пароль администратора Сервера интеграции (пароль учетной записи `admin`) и нажмите на кнопку **Проверить**.

      Мастер создания политики выполняет подключение к Серверу интеграции. Если установить подключение не удалось, в окне отображается сообщение об ошибке. Если подключение установлено, окно **Подключение к Серверу интеграции** закрывается, в окне мастера создания политики в поле **Подключение к Серверу интеграции** отображается статус **Установлено**.

c. Если вы выбрали список адресов SVM, заданный вручную, в окне отображается список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Чтобы добавить SVM в список, нажмите на кнопку **Добавить** и укажите в открывшемся окне IP-

адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки.

> Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения.

Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**.

Перейдите к следующему шагу мастера.

8. 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 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 (см. раздел "Изменение статуса политики" на стр. 401).
     - **Для автономных пользователей**. Политика, которая становится активной, когда устройство покидает сеть организации. Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.
   - 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 документации Kaspersky Security Center.

9. На закладке **Параметры программы** вы можете изменить параметры политики.
10. Нажмите на кнопку **Сохранить**.

Созданная политика появится в списке политик. Вы можете изменить параметры политики (см. раздел "Изменение параметров политики" на стр. 400) позже. Общая информация об управлении политиками приведена в документации Kaspersky Security Center.

Изменение параметров политики

► *Чтобы изменить параметры политики:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, для которой применяется политика. Для этого нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только политики, настроенные для выбранной группы администрирования.

3. Выберите политику, параметры которой вы хотите изменить, и по ссылке с названием политики откройте окно свойств политики.
4. Измените параметры политики.
5. Нажмите на кнопку **Сохранить**.

Политика будет сохранена с обновленными параметрами.

Изменение статуса политики

► *Чтобы изменить статус политики:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили**.

   Откроется список политик.

2. В списке политик выберите политику, статус которой вы хотите изменить, и по ссылке с названием политики откройте окно свойств политики.
3. На закладке **Общие** в разделе **Состояние политики** выберите нужный статус:

   - **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 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.

   - **Для автономных пользователей**. Политика, которая становится активной, когда устройство покидает сеть организации.

   Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

4. Нажмите на кнопку **Сохранить**.

Статус политики будет изменен.

Действия с политиками

► *Чтобы скопировать, переместить, экспортировать или импортировать политику:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили**.

   Откроется список политик.

2. В списке политик установите флажок рядом с названием нужной политики и нажмите на кнопку нужного действия над списком политик.

kaspersky

Удаление политики

► *Чтобы удалить политику:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили**.

   Откроется список политик.
2. В списке политик установите флажок рядом с названием политики, которую вы хотите удалить.

   Вы можете одновременно выбрать несколько политик для удаления.
3. Нажмите на кнопку **Удалить** над списком политик.
4. Подтвердите удаление политики.

Параметры политики

Вы можете использовать политику для настройки параметров работы приложения Kaspersky Endpoint Security для всех клиентских устройств, входящих в состав группы администрирования.

Набор параметров и значения по умолчанию для параметров политики зависят от типа лицензии. Некоторые параметры политики применяются или не применяются в работе приложения в зависимости от режима, в котором используется приложение (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23).

В этом разделе

Закладка Параметры программы

На закладке **Параметры программы** вы можете выбрать раздел, содержащий набор параметров, которые вы хотите настроить.

Таблица 140. Разделы и подразделы

Раздел	Подразделы
Базовая защита	**Защита от файловых угроз** (на стр. 404) **Исключения из проверки** **Управление сетевым экраном** (на стр. 416) **Защита от веб-угроз** (на стр. 420) **Защита от сетевых угроз** (на стр. 422)
Продвинутая защита	**Kaspersky Security Network** (на стр. 423) **Защита от шифрования** (на стр. 426) **Контроль целостности системы** (на стр. 432) **Контроль приложений** (на стр. 436) **Контроль устройств** (на стр. 439) **Анализ поведения** (на стр. 444)
Локальные задачи	**Управление задачами** (на стр. 446) **Проверка съемных дисков** (на стр. 447)
Общие параметры	**Параметры прокси-сервера** (на стр. 448) **Параметры приложения** (на стр. 450) **Параметры проверки контейнеров** (на стр. 451) **Managed Detection and Response** (на стр. 453) **Параметры сети** (на стр. 453) **Глобальные исключения** (на стр. 456) **Параметры Хранилища** (на стр. 457) **Endpoint Detection and Response (KATA)** (см. раздел "**Интеграция с Kaspersky Endpoint Detection and Response (KATA)**" на стр. 458)

В сертифицированной версии приложения не поддерживаются следующие функции:

- интеграция с решением Kaspersky Managed Detection and Response;
- механизм автоматической загрузки обновлений прложения.

kaspersky

Защита от файловых угроз

Защита от файловых угроз позволяет избежать заражения файловой системы устройства пользователя. Защита от файловых угроз запускается автоматически с параметрами по умолчанию при запуске приложения Kaspersky Endpoint Security, постоянно находится в оперативной памяти устройства и проверяет все открываемые, сохраняемые и запускаемые файлы.

Таблица 141. Параметры Защиты от файловых угроз

Параметр	Описание
Защита от файловых угроз включена / выключена	Переключатель включает или выключает Защиту от файловых угроз на всех управляемых устройствах. По умолчанию переключатель включен.
Режим Защиты от файловых угроз	В раскрывающемся списке вы можете выбрать режим работы Защиты 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 Хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Блокировать** доступ к объекту.
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 Хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в 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 проверки	По ссылке **Настроить области проверки** открывается окно **Области 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, 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 *самораспаковывающихся архивов*. 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, Kaspersky Endpoint Security 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 Endpoint Security 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 *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал событие *ObjectProcessed* 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 *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал событие *ObjectNotProcessed*. 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 *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал событие *PackedObjectDetected*. 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. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.
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.

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 142. 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 Endpoint Security 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 проверки

В этом окне вы можете добавить или настроить область проверки.

Таблица 143. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.

Параметр	Описание
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. 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.

kaspersky

Исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых приложение Kaspersky Endpoint Security не проверяет объекты на наличие вирусов и других вредоносных программ. Вы также можете исключать из проверки объекты по маскам и названиям угроз и настраивать исключения для процессов.

Таблица 144. Параметры исключений из проверки

Параметр	Описание
Области исключения	По ссылке **Настроить области исключения** открывается окно **Области исключения** (см. раздел "**Окно Области исключения**" на стр. 410). В этом окне вы можете задать список исключений из проверки.
Исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске** (см. раздел "**Окно Исключения по маске**" на стр. 413). 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. 413). 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 145. 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 146. 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. 410). 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**.

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.

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 Endpoint Security 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.

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 147. 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. 414), изменять (см. раздел "Окно Доверенный процесс" на стр. 414) и удалять.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Таблица 148. 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. • **Общая** – ресурсы файловой системы 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 сервера, доступные по протоколам Samba и NFS.

Параметр	Описание
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** или **Общая**.
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, /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**.
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.

kaspersky

Управление сетевым экраном

Сетевой экран операционной системы защищает персональные 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. Задача Управление сетевым экраном позволяет задать статус этих сетевых соединений при помощи настройки сетевых пакетных правил (см. раздел "О сетевых пакетных правилах" на стр. 192).

Задача Управление сетевым экраном предоставляет графическую оболочку для управления межсетевым экраном, входящим в состав операционной системы.

Настройка сетевых пакетных правил позволяет вам 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 задачи Управление сетевым экраном.

Перед включением компонента Управление сетевым экраном рекомендуется выключить другие средства управления сетевым экраном операционной системы.

Таблица 149. 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. 299). 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. 301). 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.

Параметр	Описание
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 150. Параметры сетевых пакетных правил

Параметр	Описание
Название	Имя сетевого пакетного правила.
Действие	Действие, выполняемое компонентом Управление сетевым экраном при обнаружении сетевой активности.
Локальный адрес	Сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, 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.

По умолчанию таблица сетевых пакетных правил пуста.

Сетевые пакетные правила в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно Сетевое пакетное правило

В этом окне вы можете настроить сетевое пакетное правило.

Таблица 151. 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).

Параметр	Описание
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 типа (в поле ввода ICMP-типа) и с указанным 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 Endpoint Security, 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 Endpoint Security и любым IP-адресом. • **Определенный адрес**. Если выбран этот элемент, сетевое правило контролирует указанные в поле **Адрес** сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, 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 152. 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 153. Сетевое соединение

Параметр	Описание
IP-адрес	Поле ввода IP-адреса сети.
Тип сети	Вы можете выбрать тип сети: • **Публичная сеть**. • **Локальная сеть**. • **Доверенная сеть**.

Защита от веб-угроз

Во время работы компонента Защита от веб-угроз приложениеKaspersky Endpoint Security проверяет входящий трафик, не допускает загрузку вредоносных файлов из интернета, а также блокирует фишинговые, рекламные и прочие опасные веб-сайты. Защита от веб-угроз запускается по умолчанию при запуске программы.

Приложение проверяет трафик, передаваемый по протоколам HTTP, HTTPS и FTP. Также выполняется проверка веб-сайтов и IP-адресов. Вы можете указать определенные сетевые порты или диапазоны сетевых портов для проверки.

Для проверки HTTPS-трафика требуется включить проверку зашифрованных соединений (см. раздел "Параметры сети" на стр. 453). Для проверки FTP-трафика требуется установить флажок **Отслеживать все сетевые порты** (см. раздел "**Параметры сети**" на стр. 453).

Таблица 154. Параметры Защиты от веб-угроз

Параметр	Описание
Защита от веб-угроз включена / выключена	Переключатель включает или выключает компонент Защита от веб-угроз. По умолчанию переключатель выключен.

Параметр	Описание
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. Приложение позволяет выполнить загрузку объекта на компьютер, 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 (значение по умолчанию).
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 программы	Флажок включает или выключает проверку ссылок по базе рекламных веб-адресов. По умолчанию флажок снят.
Обнаруживать легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройствам или данным	Флажок включает или выключает проверку ссылок по базе легальных программ, 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. 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).

Защита от сетевых угроз

Во время работы компонента Защита от сетевых угроз приложение проверяет входящий сетевой трафик на действия, характерные для сетевых атак. Защита от сетевых угроз запускается по умолчанию при запуске приложения.

Приложение проверяет входящий трафик для TCP-портов, номера которых получает из актуальных баз приложения. При обнаружении попытки сетевой атаки на ваше устройство, приложение блокирует сетевую активность со стороны атакующего устройства и записывает в журнал событие об обнаруженной сетевой активности.

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.

Таблица 155. Параметры Защиты от сетевых угроз

Параметр	Описание
Защита от сетевых угроз включена / выключена	Переключатель включает или выключает компонент Защита от сетевых угроз. По умолчанию переключатель включен.
Действие при обнаружении угрозы	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак: • **Информировать** пользователя. 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 (значение по умолчанию).
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 Endpoint Security разрешает сетевую активность со стороны этого устройства. Доступные значения: целые числа от 1 до 32768. Значение по умолчанию: 60.

Параметр	Описание
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 Endpoint Security.

Таблица 156. IP-адреса

Параметр	Описание
Укажите IP-адрес (IPv4 или IPv6)	Поле для ввода IP-адреса. IP-адреса можно указывать в форматах IPv4 и IPv6.

Kaspersky Security Network

Для повышения эффективности защиты устройств и данных пользователей Kaspersky Endpoint Security может использовать облачную базу знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения – Kaspersky Security Network (KSN). Использование данных KSN обеспечивает более высокую скорость реакции на различные угрозы, высокую производительность компонентов защиты и снижение количества ложных срабатываний.

Использование Kaspersky Security Network является добровольным. Приложение Kaspersky Endpoint Security предлагает включить использование KSN во время установки. Вы можете включить или выключить использование KSN в любой момент.

Инфраструктурные решения Kaspersky Security Network

Kaspersky Endpoint Security 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 Endpoint Security 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. 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 изменения лицензии Kaspersky Endpoint Security для использования KPSN требуется предоставить поставщику услуг информацию о новом 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 Endpoint Security автоматически отправляет в KSN 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 Endpoint Security 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.

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**.

Облачный режим работы Kaspersky Endpoint Security

Если приложение Kaspersky Endpoint Security используется в автономном режиме и вы используете KSN в работе приложения, вы можете включать *облачный режим* работы приложения. Облачный режим – это режим работы приложения Kaspersky Endpoint Security, при котором используется облегченная версия баз вредоносного ПО.

Включение облачного режима приводит к выходу приложения из сертифицированного состояния.

Работу приложения с облегченными базами вредоносного ПО обеспечивает Kaspersky Security Network.

Если вы планируете использовать облачный режим, убедитесь, что KSN доступен на устройстве. Информация о доступности KSN отображается в Kaspersky Security Center с помощью статуса клиентского устройства (*OK, Критический, Предупреждение*) в списке управляемых устройств на закладке **Устройства**.

Kaspersky Endpoint Security переходит к использованию облегченной версии баз вредоносного ПО после включения облачного режима и выполнения очередного обновления баз и модулей приложения. Если вы не используете KSN или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию баз приложения с серверов "Лаборатории Касперского" в ходе очередного обновления баз приложения. Облачный режим выключается автоматически, если выключено использование KSN.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, работа с облегченными базами вредоносного ПО не поддерживается. Kaspersky Endpoint Security получает от Сервера защиты специальные базы, необходимые для работы Легкого агента.

Использование службы прокси-сервера KSN

Устройства пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN напрямую или при помощи службы прокси-сервера KSN.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, взаимодействие с инфраструктурой KSN обеспечивает служба прокси-сервера KSN. Если прокси-сервер KSN недоступен, KSN не используется в работе приложения.

Вы можете настроить параметры прокси-сервера KSN в свойствах Сервера администрирования Kaspersky Security Center. Подробнее о прокси-сервере KSN см. в справке Kaspersky Security Center.

Таблица 157. 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 Endpoint Security использует облегченную версию баз вредоносного ПО. Флажок доступен, если включено использование KSN. Флажок установлен, если при создании политики вы приняли условия Положения о Kaspersky Security Network и используете расширенный режим KSN. Режим включается или выключается после следующего обновления баз приложения. Включение облачного режима приводит к выходу приложения из сертифицированного состояния.
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. Параметр применяется, только если приложение используется в автономном режиме.
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 158. 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.

Защита от шифрования

Защита от шифрования позволяет защитить ваши файлы в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования.

Во время работы компонента Защита от шифрования приложение проверяет обращения удаленных устройств сети к файлам, расположенным в общих сетевых директориях защищаемого устройства. Если

приложение расценивает действия удаленного устройства, получающего доступ к общим сетевым ресурсам, как вредоносное шифрование, она добавляет это устройство в список недоверенных устройств и запрещает ему доступ к общим сетевым директориям. Приложение не расценивает действия как вредоносное шифрование, если активность обнаружена в директориях, которые не входят в область защиты компонента Защита от шифрования.

Для использования компонента требуется лицензия, которая включает эту функцию.

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, чтобы был установлен пакет rpcbind.

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.

Защита от шифрования не блокирует доступ к сетевым файловым ресурсам до тех пор, пока действия устройства не расцениваются как вредоносные. Таким образом, как минимум один файл будет зашифрован, прежде чем приложение обнаружит вредоносную активность.

Таблица 159. Параметры Защиты 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. 428).
Блокировка недоверенных устройств включена / выключена	Переключатель включает или выключает блокировку недоверенных устройств. По умолчанию переключатель включен.
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 4294967295. Значение по умолчанию: 30.
Исключения	По ссылке **Настроить исключения** открывается окно **Области исключения**.

Параметр	Описание
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 160. 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 Endpoint Security 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 проверки

В этом окне можно добавить или настроить область защиты компонента Защита от шифрования.

Таблица 161. Параметры области защиты

Параметр	Описание
Название области проверки	Поле ввода названия области защиты. Это название будет отображаться в таблице окна **Области защиты** (см. раздел "**Окно Области защиты**" на стр. 428). 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.

Параметр	Описание
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 **Общие**.
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).
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 162. 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 163. 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. 410). 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.

Контроль целостности системы

Контроль целостности системы предназначен для отслеживания действий, выполняемых с файлами и директориями в области мониторинга, указанной в параметрах работы компонента. Вы можете использовать Контроль целостности системы, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве.

Для использования компонента требуется лицензия, которая включает эту функцию.

Таблица 164. Параметры Контроля целостности системы

Параметр	Описание
Контроль целостности системы включен / выключен	Переключатель включает или выключает 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. 432).
Исключения из мониторинга	По ссылке **Настроить области исключения из мониторинга** открывается окно **Области исключения** (см. раздел "**Окно Области исключения**" на стр. 320).
Исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске** (см. раздел "**Окно Исключения по маске**" на стр. 321).

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/kesl/).

Таблица 165. 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 Endpoint Security 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 проверки

В этом окне вы можете добавить или настроить область мониторинга для компонента Контроля целостности системы.

Таблица 166. Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна **Области мониторинга** (см. раздел "**Окно Области мониторинга**" на стр. 432). 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.

Параметр	Описание
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, /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.
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 167. 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 168. 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. 320). 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.

kaspersky

Контроль приложений

Во время выполнения задачи Контроль приложений приложение Kaspersky Endpoint Security управляет запуском приложений на устройствах пользователей. Это позволяет снизить риск заражения устройства, ограничивая доступ к приложениям. Запуск приложений регулируется с помощью *правил контроля приложений* (см. раздел "*О правилах контроля приложений*" на стр. 244).

Для использования компонента требуется лицензия, которая включает эту функцию.

Контроль приложений может работать в двух режимах:

- *Список запрещенных*. Режим, при котором приложение Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. Этот режим работы компонента Контроль приложений настроен по умолчанию.
- *Список разрешенных*. Режим, при котором приложение Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.

Для каждого режима работы Контроля приложений вы можете создать отдельные правила, а также выбрать действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения: *применять правила* или *информировать* о попытке запуска приложения, удовлетворяющего правилам.

Параметры Контроля приложений описаны в таблице ниже.

Таблица 169. Параметры Контроля приложений

Параметр	Описание
Контроль приложений включен / выключен	Переключатель включает или выключает Контроль приложений. По умолчанию переключатель выключен.
Действие при запуске приложений, запрещенных правилами	Действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам: • **Информировать (тестовый режим)**. При выборе этого варианта приложение Kaspersky Endpoint Security тестирует правила и формирует событие о попытке запуска приложения, удовлетворяющего правилам. • **Применять правила** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security применяет правила контроля приложений и выполняет заданное в правилах действие.
Режим Контроля приложений	Режим работы компонента Контроль приложений: • **Список разрешенных**. При выборе этого варианта приложение Kaspersky Endpoint Security 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 Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.

Параметр	Описание
Правила Контроля приложений	По ссылке **Настроить правила** открывается окно **Правила Контроля приложений** (см. раздел "**Окно Правила Контроля приложений**" на стр. 437).

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 170. Параметры правил контроля приложений

Параметр	Описание
Категория	Название категории приложений, которая используется в работе правила.
Статус	Статус работы правила контроля приложений: • *Включено* – правило включено, Контроль приложений применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля приложений. • *Тест* – 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. 437), изменять и удалять правила контроля приложений.

Окно Правило Контроля приложений

В этом окне вы можете настроить параметры правила Контроля приложений.

Таблица 171. Настройка правила контроля приложений

Таблица 172.

Параметр	Описание
Описание правила	Описание правила Контроля приложений.
Статус	Вы можете выбрать статус работы правила контроля приложений: • *Включено* – правило включено, Контроль приложений применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля приложений. • *Тест* – 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. 438).

Параметр	Описание
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, изменять (см. раздел "Окно Выбор пользователя или группы" на стр. 438) и 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 Kaspersky Security Center не поддерживается.

Таблица 173. 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.

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 174. 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.

kaspersky

Контроль устройств

Во время выполнения задачи Контроль устройств приложение Kaspersky Endpoint Security управляет доступом пользователей к устройствам, которые установлены на клиентском устройстве или подключены к нему (например, жестким дискам, камерам или модулям Wi-Fi). Это позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных. Контроль устройств управляет доступом пользователей к устройствам с помощью правил доступа (см. раздел "О правилах доступа" на стр. 210).

При подключении устройства, доступ к которому запрещен задачей Контроль устройств, к клиентскому устройству, 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.

Таблица 175. Параметры Контроля устройств

Параметр	Описание
Контроль устройств включен / выключен	Переключатель включает или выключает компонент Контроль устройств. По умолчанию переключатель включен.
Настроить доверенные устройства	По ссылке открывается окно **Доверенные устройства** (см. раздел "**Окно Доверенные устройства**" на стр. 439). В этом окне вы можете добавлять устройства в список доверенных по идентификатору устройства (см. раздел "Окно Доверенное устройство (Идентификатор устройства)" на стр. 440) или выбрав их из списка устройств, обнаруженных на клиентских устройствах (см. раздел "Окно Доверенное устройство (Список обнаруженных устройств)" на стр. 440).
Действие Контроля устройств	Действие, выполняемое приложением при попытке доступа к устройству, к которому запрещен доступ в соответствии с правилами Контроля устройств: • **Тестировать правила**. При выборе этого варианта приложение Kaspersky Endpoint Security тестирует правила доступа и формирует событие об обнаружении попытки доступа к устройству. • **Применять правила** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security применяет правила контроля доступа и выполняет заданное в правилах действие.
Настроить параметры для типов устройств	По ссылке открывается окно **Типы устройств** (см. раздел "**Окно Типы устройств**" на стр. 441). В этом окне вы можете настроить правила доступа для различных типов устройств.
Настроить параметры для шин подключения	По ссылке открывается окно **Шины подключения** (см. раздел "**Окно Шины подключения**" на стр. 444). В этом окне вы можете настроить правила доступа к шинам подключения.

Окно Доверенные устройства

Таблица содержит список доверенных устройств. По умолчанию таблица пустая.

Таблица 176. 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.

Вы можете добавить устройство в список доверенных устройств по идентификатору устройства (см. раздел "Окно Доверенное устройство (Идентификатор устройства)" на стр. 440) или выбрав нужное устройство в списке устройств, обнаруженных на устройстве пользователя (см. раздел "Окно Доверенное устройство (Список обнаруженных устройств)" на стр. 440).

Доверенные устройства в таблице можно изменять и удалять.

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 177. 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 политике Агента администрирования, по умолчанию – каждые 15 минут). При создании новой политики в отсутствие активной политики список будет пустым.

Таблица 178. 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 179. Правила доступа для типов устройств

Параметр	Описание

Доступ к устройствам хранения данных	Таблица содержит следующие столбцы:
	• **Тип** – тип устройств (например, Жесткие диски, Принтеры).
	• **Доступ** – 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.
	  • **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. 444), используемой для подключения устройства.
	  • **По правилам** – разрешить или запретить доступ к устройствам в зависимости от правила доступа и расписания (см. раздел "Окно Правила доступа к устройствам" на стр. 442). Правило доступа и расписание для него можно настроить, выбрав нужный тип устройства.

Доступ к другим устройствам	Таблица содержит следующие столбцы:
	• **Тип** – тип устройства (например, **Устройства ввода**, **Звуковые адаптеры**).
	• **Доступ** – 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 правило доступа **Блокировать**.
	  • **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. 444), используемой для подключения устройства.

Окно Правила доступа к устройствам

В этом окне вы можете настроить правила доступа и расписания для выбранного типа устройств.

Таблица 180. Правила доступа и расписания для устройств

Параметр	Описание
Доступ 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. 444), используемой для подключения устройства. • **По правилам** – разрешить или запретить доступ к устройствам в зависимости от правила доступа и расписания.

Список правил 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. 326).
	Вы можете добавлять, изменять (см. раздел "Окно Правило доступа к устройствам" на стр. 442) и удалять правила доступа.

Окно Правило доступа к устройствам

В этом окне вы можете настроить правило доступа к устройствам.

Таблица 181. 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.

Параметр	Описание
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. 443) и 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. 443) 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 182. 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 к устройствам" на стр. 443) и удалять расписания доступа.

Расписание по умолчанию удалить невозможно.

Окно Расписание доступа к устройствам

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 к устройствам невозможно.

Таблица 183. 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 правила доступа для шин подключения.

Таблица 184. Правила доступа для шин подключения

Параметр	Описание
Шина подключения	Шина подключения, используемая для подключения устройств к клиентскому устройству: • **FireWire** • **USB**
Доступ	Переключатель включает или выключает доступ к устройствам, использующим эту шину для подключения: • **Разрешен** (значение по умолчанию) – предоставить доступ к устройствам, подключенным с помощью этой шины подключения. • **Заблокирован** – запретить доступ к устройствам, подключенным с помощью этой шины подключения.

Анализ поведения

По умолчанию компонент Анализ поведения запускается при запуске приложения Kaspersky Endpoint Security и контролирует вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности приложение Kaspersky Endpoint Security может завершать процесс приложения, осуществляющего вредоносную активность.

Таблица 185. Параметры компонента Анализ поведения

Параметр	Описание
Анализ поведения включен / выключен	Переключатель включает или выключает компонент Анализ поведения. По умолчанию переключатель включен.
Действие при обнаружении вредоносной активности	Действие, которое приложение будет выполнять при обнаружении вредоносной активности в операционной системе: • **Информировать** пользователя. Приложение не завершает процесс, осуществляющий вредоносную активность, только записывает событие об обнаружении вредоносной активности в журнал событий. • **Блокировать** приложение, осуществляющее вредоносную активность (значение по умолчанию). Kaspersky Endpoint Security 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. 445). 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 Endpoint Security с решением Kaspersky Managed Detection and Response, исключения по процессам не применяются.

Таблица 186. 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. 446) 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 187. 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. 445). 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.

Управление задачами

Вы можете настроить возможность просмотра и управления задачами приложения Kaspersky Endpoint Security на управляемых устройствах.

Таблица 188. Параметры управления задачами

Параметр	Описание
Разрешить пользователям просмотр и управление локальными задачами	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в приложении Kaspersky Endpoint Security, и управление этими задачами на управляемых клиентских устройствах. По умолчанию флажок снят.

Параметр	Описание
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.

Проверка съемных дисков

Во время выполнения задачи Проверка съемных дисков приложение проверяет съемный диск и его загрузочные секторы на вирусы и другие вредоносные программы. Выполняется проверка следующих съемных дисков: CD/DVD-приводов, Blu-ray дисков, флеш-накопителей (включая USB-модемы), внешних жестких дисков и дискет.

Таблица 189. Параметры задачи 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. При быстрой проверке используются параметры, заданные по умолчанию для компонента Защита от файловых угроз (на стр. 404). • **Подробная проверка** – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При подробной проверке используются параметры, заданные по умолчанию для задачи Поиск вредоносного ПО (на стр. 478).
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 только файлы определенных типов на CD/DVD-приводах и Blu-ray дисках. При быстрой проверке используются параметры, заданные по умолчанию для компонента Защита от файловых угроз (на стр. 404). • **Подробная проверка** – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. При подробной проверке используются параметры, заданные по умолчанию для задачи Поиск вредоносного ПО (на стр. 478).

Параметр	Описание
Блокировать доступ к съемному диску во время проверки	Флажок включает или выключает блокировку файлов на подключенном диске во время выполнения задачи Проверка съемных дисков. По умолчанию флажок снят.

Параметры прокси-сервера

Вы можете настроить параметры прокси-сервера, если доступ пользователей с клиентских устройств в интернет осуществляется через прокси-сервер. Приложение Kaspersky Endpoint Security может использовать прокси-сервер для подключения к серверам "Лаборатории Касперского", например, при обновлении баз и модулей или при взаимодействии с Kaspersky Security Network и Kaspersky Endpoint Detection and Response (KATA).

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование прокси-сервера для подключения к Kaspersky Security Network, к SVM и к Серверу интеграции.

Таблица 190. Параметры прокси-сервера

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, прокси-сервер не используется в работе приложения Kaspersky Endpoint Security.
Использовать параметры указанного прокси-сервера	Если выбран этот вариант, Kaspersky Endpoint Security использует указанные параметры прокси-сервера, например для интеграции с Kaspersky Endpoint Detection and Response (KATA).
Адрес	Поле для ввода IP-адреса или доменного имени прокси-сервера. Поле доступно, если выбран вариант **Использовать параметры указанного прокси-сервера**.
Порт	Поле для ввода порта прокси-сервера. Значение по умолчанию: 3128. Поле доступно, если выбран вариант **Использовать параметры указанного прокси-сервера**.

Параметр	Описание
Использовать имя пользователя и пароль	Включает или выключает аутентификацию с помощью имени пользователя и пароля при доступе к прокси-серверу. Флажок доступен, если выбран вариант **Использовать параметры указанного 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 имя пользователя и пароль**.
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 **OK**. 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 имя пользователя и пароль**.
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 Endpoint Security использует Kaspersky Security Center в качестве прокси-сервера при активации приложения. По умолчанию флажок снят. Параметр применяется, только если приложение используется в автономном режиме. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, информацию о лицензии предоставляет Сервер защиты.

kaspersky

Параметры приложения

Вы можете настроить общие параметры приложения Kaspersky Endpoint Security.

Таблица 191. Общие параметры приложения

Параметр	Описание
Обнаруживать легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройствам или данным	Флажок включает или выключает обнаружение легальных программ, через которые злоумышленники могут навредить устройству или данным пользователя. По умолчанию флажок снят.
Уведомления о событиях	По ссылке **Настроить уведомления о событиях** открывается окно **Уведомления о событиях**. В этом окне вы можете выбрать события, уведомления о которых приложение будет записывать в журнал операционной системы (syslog). Для этого установите флажок около каждого типа события, уведомление о котором должно записываться. Также вы можете установить флажок около уровня важности событий (**Отказы функционирования**, **Информационные сообщения**, **Предупреждения**, **Критические события**). В этом случае флажки будут установлены автоматически около каждого типа событий, входящего в группу выбранного уровня важности. По умолчанию все флажки сняты.
Блокировать доступ к файлам во время проверки	Флажок включает или выключает блокировку доступа к файлам во время проверки компонентами Защита от файловых угроз (на стр. 404), Защита от шифрования (на стр. 426), Контроль устройств (на стр. 439) и задачей Проверка съемных дисков (на стр. 447). Если флажок снят, включается информирующий режим работы компонентов Защита от файловых угроз и Контроль устройств. *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 программ, а только информируют пользователя об обнаружении угрозы. По умолчанию флажок установлен.
Исключение памяти процессов из проверки	По ссылке **Настроить исключение памяти процессов из проверки** открывается окно **Исключение памяти процессов из проверки** (см. раздел "**Окно Исключение памяти процессов из проверки**" на стр. 339), в котором вы можете сформировать список процессов, исключаемых из проверки памяти процессов.
Ограничить потребление ресурсов процессора для задач проверки	Флажок включает или выключает ограничение на использование ресурсов процессора для задач Поиск вредоносного ПО, Инвентаризация, Проверка контейнеров и Выборочная проверка контейнеров. По умолчанию флажок снят.

Параметр	Описание
Максимальная нагрузка (в процентах)	Поле для ввода максимального значения нагрузки на все ядра процессора (в процентах) при работе задач Поиск вредоносного ПО, Инвентаризация, Проверка контейнеров и Выборочная проверка контейнеров. Доступные значения: 10–100. Значение по умолчанию – 100% Поле доступно, если установлен флажок **Ограничить потребление ресурсов процессора для задач проверки**.
Дополнительные параметры приложения	По ссылке **Настроить параметры записи дампов** открывается окно **Параметры записи дампов** (см. раздел "**Окно Параметры записи дампов**" на стр. 451).

Окно Исключение памяти процессов из проверки

Список содержит пути к процессам, которые Kaspersky Endpoint Security исключает из проверки памяти процессов. Для указания пути вы можете использовать маски. По умолчанию список пуст.

Элементы в списке можно добавлять, изменять и удалять.

Окно Параметры записи дампов

В этом окне вы можете настроить параметры записи дампов.

Таблица 192. Параметры записи дампов

Параметр	Описание
Создавать файл дампа при сбое в работе приложения	Флажок включает или выключает создание файла дампа (см. раздел "Содержимое файлов дампа и их хранение" на стр. 515) при сбое в работе приложения. По умолчанию флажок снят. Для применения параметров записи дампов требуется перезапустить приложение.
Путь к директории с файлами дампа	Поле ввода пути к директории, в которой хранятся файлы дампа. Размер поля ввода ограничен 128 символами. Допустимо использовать только символы `0-9`, `a-z`, `A-Z`, а также `_-./` для указания пути. Значение по умолчанию: /var/opt/kaspersky/kesl/common/dumps.

Параметры проверки контейнеров

Вы можете настроить параметры проверки пространств имен и контейнеров приложением Kaspersky Endpoint Security.

Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен. При этом в свойствах устройства в разделе **Программы**, в свойствах приложения в разделе **Компоненты** для проверки контейнеров отображается статус *Остановлена*.

Таблица 193. Параметры проверки контейнеров

Параметр	Описание
Проверка пространств имен и контейнеров включена / выключена	Переключатель включает или выключает проверку пространств имен и контейнеров. 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** – 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** (значение по умолчанию) – если не удалось вылечить зараженный объект, приложение останавливает контейнер. Этот параметр доступен при использовании приложения по лицензии, которая включает эту функцию.
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.

Параметр	Описание
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.

Managed Detection and Response

Интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response (MDR) обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.

Эта функциональность не поддерживается в сертифицированной версии приложения. Включение интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response приводит к выходу приложения из сертифицированного состояния.

Таблица 194. Параметры Managed Detection and Response

Параметр	Описание
Managed Detection and Response включен / выключен	Переключатель включает или выключает интеграцию приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response. По умолчанию переключатель выключен. Включение переключателя приводит к выходу приложения из сертифицированного состояния.
Загрузить	По нажатию на кнопку открывается стандартное окно Microsoft Windows, в котором вы можете выбрать конфигурационный файл BLOB.

Параметры сети

Вы можете настроить параметры проверки зашифрованных соединений. Эти параметры используются в работе компонента Защита от веб-угроз (на стр. 420).

При изменении параметров проверки зашифрованных соединений приложение формирует событие *Параметры сети изменены (Network settings changed)*.

Таблица 195. Параметры сети

Параметр	Описание
Проверка зашифрованных соединений включена / выключена	Переключатель включает или выключает проверку зашифрованных соединений. По умолчанию переключатель включен.
Доверенные сертификаты	По ссылке **Настроить список доверенных сертификатов** открывается окно (см. раздел "Окно Доверенные сертификаты" на стр. 455), в котором вы можете настроить список доверенных сертификатов. Доверенные сертификаты используются при проверке зашифрованных соединений.
Действие при обнаружении недоверенного сертификата	Вы можете выбрать действие, которое приложение будет выполнять при обнаружении недоверенного сертификата: • **Разрешить соединение** с доменом с недоверенным сертификатом (значение по умолчанию). • **Блокировать соединение** с доменом с недоверенным сертификатом.
Действие при ошибках во время проверки зашифрованных соединений	Вы можете выбрать действие, которое приложение будет выполнять при возникновении ошибки во время проверки зашифрованных соединений: • **Добавить веб-сайт 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. • **Отключиться от веб-сайта** – заблокировать сетевое подключение.
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 список доверенных доменов** открывается окно **Доверенные домены** (см. раздел "**Окно Доверенные домены**" на стр. 455).
Сетевые порты	По ссылке **Настроить параметры сетевых портов** открывается окно **Сетевые порты** (см. раздел "**Окно Сетевые порты**" на стр. 455), в котором вы можете указать, какие сетевые порты будет проверять приложение.
Отслеживать все сетевые порты	Если выбран этот вариант, приложение проверяет все сетевые порты.
Отслеживать только указанные порты	Если выбран этот вариант, приложение проверяет только сетевые порты, указанные в окне **Сетевые порты** (см. раздел "**Окно Сетевые порты**" на стр. 455). Этот вариант выбран по умолчанию.

Окно Доверенные сертификаты

Вы можете настроить список сертификатов, которые приложение Kaspersky Endpoint Security 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 SHA-256.

По умолчанию список сертификатов пуст.

Вы можете добавлять (см. раздел "Окно добавления доверенного сертификата" на стр. 455) и удалять сертификаты.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно добавления доверенного сертификата

В этом окне вы можете добавить сертификат, который приложение Kaspersky Endpoint Security 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. По умолчанию список пуст. Вы можете добавлять, изменять и удалять домены в списке доверенных доменов.

Пример: `*example.com`. Например, `*example.com/*` – это неправильное значение, так как требуется указывать адрес домена, а не веб-страницы.

Окно Сетевые порты

Таблица содержит сетевые порты, которые будет проверять приложение, если в окне **Параметры сети** (на стр. 453) выбран вариант **Отслеживать 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, настраивать и удалять.

Глобальные исключения

Таблица содержит точки монтирования, которые будут исключены из проверки компонентами приложения, использующими перехватчик файловых операций (Защита от файловых угроз и Защита от шифрования).

В столбце **Путь** отображается путь к исключенным точкам монтирования. По умолчанию таблица пустая.

Элементы в таблице можно добавлять, изменять (см. раздел "Окно добавления исключения точки монтирования" на стр. 456) и удалять.

Окно добавления исключения точки монтирования

Таблица 196. 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**.

Параметр	Описание
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**.
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**.

Параметры Хранилища

Хранилище – это список резервных копий файлов, которые были удалены или изменены в процессе лечения. Резервная копия – копия файла, которая создается при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности. По умолчанию Хранилище расположено в директории /var/opt/kaspersky/kesl/common/objects-backup/.

Файлы в Хранилище могут содержать персональные данные. Для доступа к файлам в Хранилище требуются root-права.

Таблица 197. Параметры Хранилища

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 управляемом клиентском устройстве. По умолчанию переключатель включен.
Информирование о файлах в Хранилище включено / выключено	Переключатель включает или выключает отправку уведомлений о файлах в Хранилище на Сервер администрирования. По умолчанию переключатель включен.
Хранить объекты не более (дней)	Поле ввода для указания периода хранения объектов в Хранилище. Доступные значения: 0–3653. Значение по умолчанию: 90. Если задано значение 0, период хранения объектов в Хранилище не ограничен.
Максимальный размер Хранилища (МБ)	Поле ввода для указания максимального размера Хранилища (в мегабайтах). Доступные значения: 0–999999. Значение по умолчанию: 0 (размер Хранилища не ограничен).

Интеграция с Kaspersky Endpoint Detection and Response (KATA)

Kaspersky Endpoint Detection and Response (KATA) (далее также EDR (KATA)) – компонент в составе решения Kaspersky Anti Targeted Attack Platform, которое предназначено для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats (далее также "APT"). Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform https://support.kaspersky.com/help/KATA/5.1/ru-RU/246841.htm.

При взаимодействии с EDR (KATA) приложение Kaspersky Endpoint Security может отправлять на сервер Kaspersky Anti Targeted Attack Platform с компонентом Central Node (далее также сервер KATA) данные о событиях на устройствах (телеметрию) и выполнять задачи, полученные от Kaspersky Anti Targeted Attack Platform, направленные на обеспечение функций безопасности.

Для интеграции с EDR (KATA) должен быть включен компонент Анализ поведения.

Интеграция приложения Kaspersky Endpoint Security с EDR (KATA) возможна, только если этот компонент включен. В противном случае необходимые данные телеметрии не передаются.

Дополнительно EDR (KATA) может использовать данные, полученные от следующих компонентов:

- Защита от файловых угроз.
- Защита от сетевых угроз.
- Защита от веб-угроз.

Во время интеграции с EDR (KATA) устройства с Kaspersky Endpoint Security устанавливают защищенные соединения с сервером KATA по протоколу HTTPS. Для обеспечения безопасности соединения используются следующие сертификаты, выданные сервером KATA:

- Сертификат сервера KATA. Соединение шифруется с помощью TLS-сертификата сервера. Вы можете повысить уровень безопасности соединения, включив проверку сертификата сервера на стороне Kaspersky Endpoint Security. Для этого вам нужно добавить сертификат сервера (см. раздел "Окно настройки параметров подключения к серверам" на стр. 460) во время настройки параметров интеграции.
- Сертификат клиента. Этот сертификат используется для дополнительной защиты подключения с помощью двусторонней аутентификации (проверки устройств с Kaspersky Endpoint Security сервером KATA). Один и тот же сертификат клиента может использоваться несколькими устройствами. По умолчанию сервер KATA не выполняет проверку сертификатов клиентов, но проверка может быть включена на стороне сервера KATA. В этом случае вам нужно включить двустороннюю аутентификацию и добавить сертификат клиента (см. раздел "Окно настройки параметров подключения к серверам" на стр. 460) в параметрах интеграции (криптоконтейнер с сертификатом и закрытым ключом).

Сертификаты для защиты соединения с сервером KATA предоставляет администратор Kaspersky Anti Targeted Attack Platform.

Для подключения к серверу KATA используется прокси-сервер, если использование прокси-сервера настроено (см. раздел "Параметры прокси-сервера" на стр. 448) в общих параметрах приложения Kaspersky Endpoint Security.

Таблица 198. Параметры интеграции с Kaspersky Endpoint Detection and Response (KATA)

Параметр	Описание
Интеграция с Endpoint Detection and Response (KATA) включена / выключена	Включает или выключает интеграцию приложения Kaspersky Endpoint Security с EDR (KATA). По умолчанию интеграция выключена.
Параметры подключения к серверам	По ссылке **Настроить** в блоке открывается окно (см. раздел "Окно настройки параметров подключения к серверам" на стр. 460), в котором вы можете настроить общие параметры подключения к серверам KATA, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверам KATA.
Серверы KATA	Таблица содержит список серверов KATA, к которым настроено подключение. По кнопке **Добавить** открывается окно (см. раздел "Окно добавления параметров подключения к серверу KATA" на стр. 461), в котором вы можете настроить подключение к серверу KATA. 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 KATA в секундах. Значение по умолчанию: `30`.
Включить регулирование количества событий	Включает или выключает регулирование количества событий, отправляемых на сервер KATA.
Максимальное количество событий в час	Максимальное количество событий в час. Значение по умолчанию: `3000`.

Параметр	Описание
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`.

Окно настройки параметров подключения к серверам

В этом окне вы можете настроить общие параметры подключения к серверам KATA, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверам KATA.

Таблица 199. Параметры подключения к серверу KATA

Параметр	Описание
Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)	Периодичность отправки запросов на синхронизацию на сервер KATA в минутах. Значение по умолчанию: `5`.
Максимальное время ожидания соединения с сервером (сек.)	Максимальное время ожидания соединения с сервером KATA в секундах. Значение по умолчанию: `10`.
Максимальное время ожидания ответа от сервера (сек.)	Максимальное время ожидания ответа от сервера KATA в секундах. Значение по умолчанию: `10`.
Разрешить отправку телеметрии	Включает или выключает отправку данных о событиях на устройствах (телеметрии) на сервер KATA. По умолчанию отправка телеметрии включена.
Сертификат сервера	После добавления сертификата сервера 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 KATA. Если сертификат сервера добавлен, выполняется проверка сертификата сервера на стороне Kaspersky Endpoint Security, это позволяет повысить уровень безопасности соединения.
Удалить	Удаляет ранее добавленный сертификат сервера. Кнопка отображается только если сертификат сервера добавлен.
Дополнительная защита подключения	Блок параметров позволяет включить или выключить двустороннюю аутентификацию при подключении к серверу KATA и добавить сертификат клиента.

Параметр	Описание
Использовать двустороннюю аутентификацию	Включает или выключает использование двусторонней аутентификации для дополнительной защиты соединения с сервером KATA. Двусторонняя аутентификация должна быть включена на стороне сервера KATA. 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**.
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 **OK**. 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 добавления параметров подключения к серверу KATA

В этом окне вы можете указать параметры подключения к серверу KATA.

Таблица 200. Параметры подключения к серверу KATA

Параметр	Описание
Адрес	Адрес сервера KATA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером KATA 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 KATA. Значение по умолчанию: `443`.

kaspersky

Режим Легкого агента

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Для работы приложения Kaspersky Endpoint Security в режиме Легкого агента требуется постоянное взаимодействие между Легким агентом и Сервером защиты, установленным на SVM. Если соединение с Сервером защиты отсутствует, Легкий агент не может передавать фрагменты файлов на проверку Серверу защиты, проверка не выполняется. Для взаимодействия с Сервером защиты Легкий агент устанавливает и поддерживает подключение к SVM, на которой установлен этот Сервер защиты.

Вы можете настраивать следующие параметры подключения Легкого агента к SVM:

- Способ обнаружения SVM (см. раздел "Параметры обнаружения SVM" на стр. 462). Вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM. Легкий агент может обнаруживать SVM, работающие в сети, одним из следующих способов:
  - С помощью Сервера интеграции. SVM передают информацию о себе на Сервер интеграции. Сервер интеграции формирует список доступных для подключения SVM и предоставляет его Легким агентам.

    Для использования этого способа обнаружения SVM требуется подключение SVM и Легких агентов к Серверу интеграции.
  - С использованием списка адресов SVM. Вы можете задать список адресов SVM, к которым могут подключаться Легкие агенты.
- Алгоритм выбора SVM (на стр. 465) для подключения. После получения информации о доступных SVM Легкий агент выбирает оптимальную для подключения SVM в соответствии с алгоритмом выбора SVM. Вы можете указать, какой алгоритм должны использовать Легкие агенты при выборе SVM для подключения.
- Теги для подключения (на стр. 465). Вы можете регулировать подключение Легких агентов к SVM с помощью тегов для подключения. Если вы используете теги для подключения, Легкий агент может подключаться только к тем SVM, на которых настроено использование этого тега для подключения.
- Защита соединения (на стр. 467) между Легким агентом и Сервером защиты. Вы можете защищать соединение между Легкими агентами и Серверами защиты с помощью шифрования.

Подробнее о параметрах подключения Легкого агента к SVM см. в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254867.htm.

Параметры обнаружения SVM

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

В этом окне вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM.

Таблица 201. Параметры обнаружения SVM

Параметр	Описание
Использовать Сервер интеграции	Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них. Если вы хотите использовать Сервер интеграции, вам нужно настроить параметры подключения Легких агентов к Серверу интеграции (см. раздел "Подключение к Серверу интеграции" на стр. 345).
Использовать список адресов SVM, заданный вручную	Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.
Список SVM	Список IP-адресов в формате IPv4 или полных доменных имен (FQDN) SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением политики. По нажатию на кнопку **Добавить** открывается окно, в котором вы можете указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM. Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения. Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**. Список адерсов SVM отображается, если выбран вариант **Использовать список адресов SVM, заданный вручную**.

Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/index.htm), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** (на стр. 465) требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

Параметры подключения к Серверу интеграции

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Подключение к Серверу интеграции требуется, если вы хотите, чтобы Легкие агенты получали информацию об SVM через Сервер интеграции, или если вы хотите защищать соединение между Сервером защиты и Легким агентом.

В этом окне отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. По нажатию на кнопку **Изменить** открывается окно **Подключение к Серверу**, в котором вы можете настроить подключение к Серверу интеграции.

Окно Подключение к Серверу интеграции

В этом окне вы можете настроить параметры подключения Легких агентов к Серверу интеграции.

Таблица 202. Параметры подключения к Серверу интеграции

Параметр	Описание
Адрес	IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции. Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.
Порт	Порт для подключения к Серверу интеграции. По умолчанию указан порт 7271.
Проверить	По нажатию на кнопку веб-плагин проверяет SSL-сертификат, полученный от Сервера интеграции. Кнопка доступна после ввода адреса и порта для подключения к Серверу интеграции. Если сертификат содержит ошибку или не является доверенным, в окне **Подключение к Серверу интеграции** отображается сообщение об этом.
Посмотреть полученный сертификат	По нажатию на строку вы можете посмотреть информацию о сертификате, полученном от Сервера интеграции.
Игнорировать	Выберите этот вариант, чтобы сохранить полученный сертификат и продолжить подключение к Серверу интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.
Отменить	Выберите этот вариант, чтобы прервать подключение к Серверу интеграции.
Пароль	Пароль учетной записи администратора Сервера интеграции (учетной записи admin). Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев.
Проверить	По нажатию на кнопку веб-плагин выполняет подключение к Серверу интеграции. После подключения к Серверу интеграции с правами администратора в политику передается пароль учетной записи agent, которая используется для подключения Легких агентов к Серверу интеграции. Пароль хранится в зашифрованном виде.

kaspersky

Тег для подключения к SVM

В этом окне вы можете включить использование тегов Легким агентом и назначить тег, который Легкий агент будет использовать для подключения.

Убедитесь, что использование тегов для подключения также настроено в параметрах Сервера защиты. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254886.htm. Легкие агенты, которым назначен тег, могут подключаться только к SVM, для которых разрешено подключение Легких агентов с этим тегом.

Таблица 203. Параметры использования тегов для подключения

Параметр	Описание
Использовать теги для подключения Легких агентов	Флажок включает или выключает использование Легким агентом тегов для подключения к SVM.
Тег	Тег, который назначается Легким агентам. В качестве тега вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа `;`. Поле доступно, если установлен флажок **Использовать теги для подключения Легких агентов**.

Алгоритм выбора SVM

В этом окне вы можете указать, какой алгоритм выбора SVM должны использовать Легкие агенты для Linux, и настроить параметры применения расширенного алгоритма выбора SVM.

Таблица 204. Алгоритм выбора SVM

Параметр	Описание
Использовать стандартный алгоритм выбора SVM	Если выбран этот вариант, после установки и запуска на виртуальной машине Легкий агент выбирает для подключения SVM, которая является локальной для Легкого агента. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254869.htm. Если нет доступных для подключения локальных SVM, Легкий агент выбирает SVM, к которой подключено наименьшее количество Легких агентов, независимо от расположения SVM в виртуальной инфраструктуре. Этот вариант выбран по умолчанию.
Использовать расширенный алгоритм выбора SVM	Если выбран этот вариант, вы можете указать с помощью ползунка **Расположение SVM**, как расположение SVM в виртуальной инфраструктуре будет учитываться при определении локальности SVM относительно Легкого агента. Легкий агент сможет подключаться только к тем SVM, которые являются локальными. Также вы можете указать, что расположение SVM в виртуальной инфраструктуре не должно учитываться при выборе SVM для подключения. При выборе SVM Легкие агенты учитывают количество Легких агентов, подключенных к этой SVM, чтобы обеспечить равномерное распределение Легких агентов между доступными для подключения SVM.

Расположение SVM	Позволяет указать тип расположения SVM в виртуальной инфраструктуре, который учитывается при выборе SVM для подключения:
	• **Гипервизор**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):
	  • SVM развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V®, Citrix Hypervisor, VMware vSphere™, KVM, Proxmox VE, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации или Astra Linux).
	  • SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением Облачной платформы ТИОНИКС или платформы OpenStack®).
	Если на том же гипервизоре или в той же Группе серверов, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
	• **Кластер**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):
	  • SVM развернута в том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, Citrix Hypervisor, VMware vSphere, KVM, Proxmox VE, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации или Astra Linux).
	  • SVM развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением Облачной платформы ТИОНИКС или платформы OpenStack).
	Если в том же кластере гипервизоров или в рамках того же проекта OpenStack, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
	• **Дата-центр**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):
	  • SVM развернута в том же дата-центре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, Citrix Hypervisor, VMware vSphere, KVM, Proxmox VE, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis или Альт Сервер Виртуализации).
	  • SVM расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением Облачной платформы ТИОНИКС или платформы OpenStack).
	Если в том же дата-центре или в той же Зоне доступности, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
	Не учитывать расположение SVM. Легкий агент не учитывает при выборе SVM

Параметр	Описание
	ее расположение. По умолчанию выбрано значение **Гипервизор**. Параметр доступен, если выбран вариант **Использовать расширенный алгоритм выбора SVM**.

Если для Легкого агента применяется расширенный алгоритм выбора SVM и в качестве способа обнаружения SVM (см. раздел "Параметры обнаружения SVM" на стр. 462) выбран список адресов SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/index.htm), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. Требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

Защита соединения

В этом окне вы можете включить шифрование канала передачи данных между Легким агентом и Сервером защиты.

Убедитесь, что шифрование канала передачи данных между Легким агентом и Сервером защиты включено в параметрах Сервера защиты на SVM. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/6.0/ru-RU/254886.htm.

Таблица 205. Параметры защиты соединения

Параметр	Описание
Шифровать канал передачи данных между Легким агентом и Сервером защиты	Защитить соединение между Легкими агентами и Сервером защиты с помощью шифрования. Если флажок установлен, между Легким агентом, находящимся под управлением политики, и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается защищенное соединение. Легкий агент, для которого включена защита соединения, может подключиться только к SVM, на которой также включена защита соединения или разрешено незащищенное соединение с Сервером защиты. Если флажок снят, между Легким агентом и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается незащищенное соединение. По умолчанию флажок снят.

kaspersky

Управление задачами в Web Console

Задачи выполняются, только если на устройствах запущено приложение Kaspersky Endpoint Security (см. раздел "Запуск и остановка приложения на клиентском устройстве" на стр. 392).

Вы можете создавать следующие задачи для управления приложением Kaspersky Endpoint Security через Web Console:

- локальные задачи, определенные для отдельного устройства;
- групповые задачи, определенные для устройств, входящих в группы администрирования;
- задачи для наборов устройств, не входящих 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 локальных задачи, групповых задач и задач для наборов устройств.

Задачи Добавление ключа, Обновление и Откат обновления баз неприменимы, если приложение используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23).

Вы можете выполнять следующие действия с задачами:

- Создавать задачу (см. раздел "Создание задачи" на стр. 469).
- Изменять параметры задачи (см. раздел "Изменение параметров задачи" на стр. 469).
- Управлять запуском и остановкой задачи (см. раздел "Действия с задачами" на стр. 470).
- Экспортировать и импортировать задачу (см. раздел "Действия с задачами" на стр. 470).
- Удалять задачу (см. раздел "Удаление задачи" на стр. 470).

Общая информация о задачах в Web Console приведена в документации Kaspersky Security Center.

В этом разделе

Создание задачи

► *Чтобы создать задачу:*

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. В окне **Новая задача** настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Security 12.0 для Linux**.

   b. В раскрывающемся списке **Тип задачи** выберите тип задачи, которую вы хотите создать.

   c. В поле **Название задачи** введите короткое описание, например, `Обновление приложения для бухгалтерии`.

   d. В блоке **Выбор устройств, которым будет назначена задача** выберите способ указания устройств.

   e. Нажмите на кнопку **Далее**.

4. В окне **Область действия задачи** выберите устройства и нажмите на кнопку **Далее**.

5. Завершите работу мастера.

   В списке задач отобразится новая задача. Задача будет иметь параметры по умолчанию. Для настройки параметров задачи (см. раздел "Изменение параметров задачи" на стр. 469) вам нужно перейти в окно свойств задачи. Для запуска выполнения задачи требуется установить флажок напротив задачи и нажать на кнопку **Запустить**.

В списке задач вы можете контролировать результат выполнения 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 задачи также сохраняются локально и в отчетах Kaspersky Security Center.

Изменение параметров задачи

► *Чтобы изменить параметры задачи:*

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. В списке задач выберите задачу, параметры которой вы хотите изменить, и по ссылке с названием задачи откройте окно свойств задачи.

3. Измените параметры задачи.

4. Нажмите на кнопку **Сохранить**.

   Задача будет сохранена с обновленными параметрами.

Действия с задачами

► *Чтобы запустить, приостановить, возобновить, остановить, экспортировать или импортировать задачу:*

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. В списке задач установите флажок рядом с названием нужной задачи и нажмите на кнопку нужного действия над списком задач.

Удаление задачи

► *Чтобы удалить задачу:*

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. В списке задач установите флажок рядом с названием задачи, которую вы хотите удалить.

   Вы можете одновременно выбрать несколько задач для удаления.

3. Нажмите на кнопку **Удалить** над списком задач.
4. Подтвердите удаление задачи.

Параметры задач

Для управления приложением Kaspersky Endpoint Security в Web Console предусмотрены задачи следующих типов:

- **Добавление ключа** (на стр. 471). Во время выполнения задачи приложение добавляет ключ, в том числе резервный, для активации приложения.
- **Инвентаризация** (на стр. 473). Во время выполнения задачи приложение получает информацию обо всех исполняемых файлах приложений, хранящихся на устройствах.
- **Обновление** (на стр. 476). Во время выполнения задачи приложение обновляет базы в соответствии с настроенными параметрами обновления.
- **Откат обновления баз** (на стр. 478). Во время выполнения задачи приложение откатывает последнее обновление баз.
- **Поиск вредоносного ПО** (на стр. 478). Во время выполнения задачи приложение проверяет области устройства, указанные в параметрах задачи, на наличие вирусов и других вредоносных программ.
- **Проверка важных областей** (на стр. 485). Во время выполнения задачи приложение проверяет загрузочные секторы, объекты автозапуска, память процессов и память ядра.
- **Проверка контейнеров** (на стр. 491). Во время выполнения задачи приложение проверяет контейнеры и образы на наличие вирусов и других вредоносных программ.

- **Проверка целостности системы** (на стр. 495). 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.

Набор параметров и значения по умолчанию для параметров задач зависят от типа лицензии. Задачи Добавление ключа, Обновление и Откат обновления баз неприменимы, если приложение используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23).

В этом разделе

Добавление ключа

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), активация приложения с помощью задачи Добавление ключа не поддерживается.

С помощью задачи Добавление ключа вы можете добавить ключ для активации приложения Kaspersky Endpoint Security.

Таблица 206. Параметры задачи Добавление ключа

Параметр	Описание
Использовать ключ в качестве резервного	Флажок включает или выключает использование ключа в качестве резервного. Если флажок установлен, приложение использует ключ в качестве резервного. Если флажок снят, приложение использует ключ в качестве активного. По умолчанию флажок снят. Флажок недоступен, если вы добавляете ключ для пробной лицензии или ключ по подписке. Ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве резервного ключа.

Параметр	Описание
Информация о лицензии	В этом блоке приведены данные о ключе и связанной с ним лицензии: • **Лицензионный ключ** – уникальная буквенно-цифровая последовательность. • **Тип лицензии** – пробная, коммерческая или коммерческая (подписка). • **Срок действия лицензии** – количество дней, в течение которых возможно использование приложения, активированного путем добавления этого ключа (например, 365 дней). Информация не отображается, если вы используете приложение по подписке. • **Действует до** – дата и время окончания срока использования приложения, активированного путем добавления этого ключа, в формате UTC. Если вы используете приложение по неограниченной подписке, дата окончания срока действия лицензии не указывается. • **Ограничение** – максимальное количество устройств, которые приложение может защищать. • **Описание** – описание лицензии.
Выбрать ключ	При нажатии на кнопку открывается окно **Хранилище ключей Kaspersky Security Center** (см. раздел "**Окно Хранилище ключей Kaspersky Security Center**" на стр. 472). В этом окне вы можете выбрать ключ, ранее добавленный в хранилище ключей Kaspersky Security Center, а также добавить ключ в хранилище ключей Kaspersky Security Center.

Окно Хранилище ключей Kaspersky Security Center

В этом окне вы можете выбрать ключ, ранее добавленный в хранилище ключей Kaspersky Security Center, а также добавить ключ в хранилище ключей Kaspersky Security Center.

Таблица 207. Параметры окна Хранилище ключей Kaspersky Security Center

Параметр	Описание
Таблица ключей	Таблица содержит ключи, добавленные в хранилище ключей Kaspersky Security Center, и состоит из следующих столбцов: • **Тип лицензии** – тип лицензии: пробная, коммерческая или коммерческая (подписка). • **Действует до** – дата окончания срока использования приложения, активированного путем добавления этого ключа. • **Срок действия лицензии** – количество дней, в течение которых возможно использование приложения, активированного путем добавления этого ключа (например, 365 дней). Информация не отображается, если вы используете приложение по подписке. • **Ограничение** – максимальное количество устройств, которые приложение может защищать. • **Описание** – описание лицензии. • **Лицензионный ключ** – уникальная буквенно-цифровая последовательность.
Добавить ключ	При нажатии на кнопку запускается мастер добавления лицензионного ключа. Ключ будет добавлен в хранилище ключей Kaspersky Security Center. После добавления ключа информация о нем будет отображаться в таблице ключей.

kaspersky

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. 244).

Для использования задачи требуется лицензия, которая включает эту функцию.

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 Endpoint Security файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

Раздел Параметры проверки (Инвентаризация)

Таблица 208. 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. 244) 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 pyc). 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 209. Параметры области инвентаризации

Параметр	Описание
Название области проверки	Поле ввода названия области инвентаризации. Это название будет отображаться в таблице раздела **Параметры проверки** (см. раздел "**Раздел Параметры проверки (Инвентаризация)**" на стр. 473). 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 (Инвентаризация)

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 210. 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 из проверки для задачи Инвентаризация.

Таблица 211. 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. 410). 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, /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.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Вы можете добавлять, изменять и удалять маски.

Обновление

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), не поддерживается обновление баз и модулей приложения с помощью задачи, созданной в Kaspersky Security Center. Обновление выполняется с помощью локальной предустановленной задачи.

Обновление баз и модулей приложения Kaspersky Endpoint Security обеспечивает актуальность защиты устройства. Каждый день в мире появляются новые вирусы 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 приложения.

Раздел Источники обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей приложения Kaspersky Endpoint Security. Источником обновлений могут быть HTTP-, HTTPS- или FTP-серверы (например, серверы обновлений Kaspersky Security Center и "Лаборатории Касперского"), а также локальные или сетевые директории, смонтированные пользователем.

Таблица 212. Параметры источников 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 (этот вариант доступен только для Web Console). • **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.

Параметр	Описание
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.

Раздел Параметры

В разделе **Параметры** вы можете указать время ожидания ответа и параметры загрузки обновлений приложения.

Таблица 213. 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**.

kaspersky

Откат обновления баз

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23), откат обновления баз с помощью задачи не поддерживается.

После первого обновления баз приложения становится доступна функция отката баз приложения к их предыдущей версии.

Каждый раз, когда пользователь запускает процесс обновления, приложение Kaspersky Endpoint Security 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 Endpoint Security.

Задача Откат обновления баз не имеет параметров.

Поиск вредоносного ПО

Поиск вредоносного ПО – это однократная полная или выборочная проверка файлов на устройстве, выполняемая приложением. Приложение может выполнять несколько задач поиска вредоносного ПО одновременно.

По умолчанию в приложении создается одна стандартная задача поиска вредоносного ПО – полная проверка. Во время выполнения полной проверки 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.

Во время полной проверки диска процессор будет занят. Рекомендуется запускать задачу полной проверки в нерабочее время.

Раздел Параметры проверки (Поиск вредоносного ПО)

Таблица 214. 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.

Параметр	Описание
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. 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.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.

Параметр	Описание
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. 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. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.
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 сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
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 сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в 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.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Таблица 215. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области 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.

Параметр	Описание
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. 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 (Поиск вредоносного ПО)

Вы можете настроить параметры области проверки для задачи Поиск вредоносного ПО. Приложение позволяет проверять файлы, загрузочные секторы, память клиентского устройства и объекты автозапуска.

Таблица 216. 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 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 (Поиск вредоносного ПО)

В разделе **Области исключения** для задачи Поиск вредоносного ПО вы можете настроить области исключения (см. раздел "Окно Области исключения" на стр. 410), исключения по маске (см. раздел "Окно Исключения по маске" на стр. 413) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 413).

kaspersky

Проверка важных областей

Задача Проверка важных областей позволяет проверять файлы, загрузочные секторы, объекты автозапуска, память процессов и память ядра.

Раздел Параметры проверки (Проверка важных областей)

Таблица 217. 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 *самораспаковывающихся архивов*. 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.

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 событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных файлах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. 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. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. 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 устройств.
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
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 сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в 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.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Таблица 218. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области 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. 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 (Проверка важных областей)

Таблица 219. 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 (Проверка важных областей)

В разделе **Области исключения** для задачи Проверка важных областей вы можете настроить области исключения (см. раздел "Окно Области исключения" на стр. 410), исключения по маске (см. раздел "Окно Исключения по маске" на стр. 413) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 413).

kaspersky

Проверка контейнеров

Во время работы задачи Проверка контейнеров приложение Kaspersky Endpoint Security проверяет контейнеры и образы на наличие вирусов и других вредоносных программ. Вы можете одновременно запустить несколько задач Проверка контейнеров.

Поддерживается интеграция с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Для использования задачи требуется лицензия, которая включает эту функцию.

Раздел Параметры проверки (Проверка контейнеров)

Таблица 220. 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 *самораспаковывающихся архивов*. 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.

Параметр	Описание
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.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.

Параметр	Описание
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. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование технологии iChecker. Оптимизация проверки реализована средствами Сервера защиты.
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.
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.

Параметр	Описание
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 сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в 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**.
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.

Параметр	Описание
Проверять каждый слой	Флажок включает или выключает проверку всех слоев образов и запущенных контейнеров. По умолчанию флажок снят.

Раздел Области исключения (Проверка контейнеров)

В разделе **Области исключения** для задачи Проверка контейнеров вы можете настроить исключения по маске (см. раздел "Окно Исключения по маске" на стр. 413) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 413).

Проверка целостности системы

В процессе выполнения задачи Проверка целостности системы (ODFIM) изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве *снимка состояния системы*.

Для использования задачи требуется лицензия, которая включает эту функцию.

Снимок состояния системы создается во время первого выполнения задачи ODFIM на устройстве. Вы можете создать несколько задач ODFIM. Для каждой задачи ODFIM создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы относится к области мониторинга. Если снимок состояния системы не соответствует области мониторинга, приложение Kaspersky Endpoint Security формирует событие о нарушении целостности системы.

Снимок состояния системы создается заново после завершения задачи ODFIM. Вы можете заново создать снимок состояния системы для задачи с помощью соответствующего параметра. Снимок состояния системы также создается при изменении параметров задачи, например, при добавлении новой области мониторинга. При следующем выполнении задачи снимок состояния системы формируется заново. Вы можете удалить снимок состояния системы, удалив соответствующую задачу ODFIM.

Раздел Параметры проверки (Проверка целостности системы)

Таблица 221. 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.

Параметр	Описание
Использовать хеш (SHA-256) для проверки	Флажок включает или выключает использование хеша SHA-256 для задачи Проверка целостности системы. SHA-256 – это криптографическая хеш-функция, которая формирует 256-разрядное хеш-значение. 256-разрядное хеш-значение представляет собой последовательность из 64 шестнадцатеричных цифр. Если флажок снят, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром). По умолчанию флажок снят.
Следить за директориями в областях мониторинга	Флажок включает или выключает проверку указанных директорий во время выполнения задачи Проверка целостности системы. По умолчанию флажок снят.
Следить за временем последнего доступа к файлу	Флажок включает или выключает отслеживание времени доступа к файлу во время выполнения задачи Проверка 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/kesl/). 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 222. Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице раздела **Параметры проверки** (см. раздел "**Раздел Параметры проверки (Проверка целостности системы)**" на стр. 495). 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.

Параметр	Описание
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, /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 работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Раздел Области исключения (Проверка целостности системы)

В разделе **Области исключения** для задачи Проверка целостности системы вы можете настроить области исключения (см. раздел "Окно Области исключения" на стр. 497) из проверки и исключения по маске (см. раздел "Окно Исключения по маске" на стр. 321).

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 223. 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 224. 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. 497). 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.

Настройка удаленной диагностики клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения на клиентских устройствах следующих операций:

- включения и выключения трассировки;
- изменения уровня трассировки;
- загрузки файла трассировки;
- загрузки журнала удаленной установки приложения;
- загрузки системных журналов событий (syslog);
- запуска, остановки и перезапуска приложений.

Удаленная диагностика клиентского устройства выполняется с использованием Сервера администрирования в окне удаленной диагностики.

Подробнее об удаленной диагностике см. в документации Kaspersky Security Center Web Console https://support.kaspersky.com/KSC/14.2/ru-RU/197041.htm.

► *Чтобы открыть окно удаленной диагностики устройства:*

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.

   Откроется список управляемых устройств.
2. В списке управляемых устройств выберите устройство, для которого вы хотите выполнить удаленную диагностику, и по ссылке с названием устройства откройте 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 разделе **Файлы трассировки** нажмите на ссылку **Журналы удаленной установки**.

   Откроется окно **Журналы событий трассировки устройства**.

kaspersky

Управление приложением с помощью графического пользовательского интерфейса

Вы можете управлять работой приложения Kaspersky Endpoint Security с помощью графического пользовательского интерфейса.

В этом разделе

Интерфейс приложения

Значок приложения в области уведомлений

После установки пакета графического пользовательского интерфейса приложения Kaspersky Endpoint Security значок приложения появляется справа в области уведомлений панели задач.

Значок приложения обеспечивает доступ к контекстному меню и главному окну приложения. Вы можете открыть контекстное меню значка приложения, нажав на значок правой кнопкой мыши.

Контекстное меню значка приложения содержит следующие пункты:

- **Kaspersky Endpoint Security 12.0 для Linux**. Открывает главное окно приложения, в котором отображается состояние защиты вашего устройства и находятся элементы интерфейса, предоставляющие доступ к функциям приложения.
- **Выход**. Выполняет выход из графического пользовательского интерфейса приложения.

Главное окно приложения

Главное окно приложения разделено на несколько частей:

- В центральной части главного окна приложения отображается статус защиты вашего устройства. При нажатии кнопкой мыши на этой области окна открывается окно **Центр защиты**. В этом окне отображается информация о состоянии защиты вашего 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. 503)

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 задач обновления" на стр. 504) **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 задач и различные отчеты (см. раздел "Просмотр отчетов" на стр. 505).
  - Кнопка **Хранилище**. При нажатии на эту кнопку открывается окно **Хранилище**, в котором содержится информация об объектах в Хранилище (см. раздел "Просмотр объектов в Хранилище" на стр. 507).
  - Кнопка **Настройка**. При нажатии на эту кнопку открывается окно **Настройка**, в котором вы можете включить или выключить мониторинговые задачи приложения (см. раздел "Включение и выключение мониторинговых задач приложения" на стр. 503), а также использование Kaspersky Security Network.
  - Кнопка **Поддержка**. При нажатии на эту кнопку открывается окно **Поддержка**, в котором содержится информация о текущей версии приложения, лицензионном ключе, состоянии баз приложения, операционной системе, а также ссылки на информационные ресурсы "Лаборатории Касперского".
- 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 этом окне отображается подробная информация о лицензии (см. раздел "Просмотр информации о лицензии" на стр. 507). Также вы можете открыть это окно из окна **Поддержка** по ссылке с лицензионным ключом.

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.

Управление задачами

Графический пользовательский интерфейс приложения позволяет включать и выключать следующие мониторинговые задачи приложения (см. раздел "Включение и выключение мониторинговых задач приложения" на стр. 503):

- Защита от файловых угроз (см. раздел "Задача Защита от файловых угроз (File_Threat_Protection, ID:1)" на стр. 133).
- Контроль целостности системы (см. раздел "Задача Контроль целостности системы (System_Integrity_Monitoring, ID:11)" на стр. 182).
- Управление сетевым экраном.
- Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 200).

- Защита от веб-угроз (см. раздел "Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)" на стр. 206).
- Контроль устройств (см. раздел "Задача Контроль устройств (Device_Control, ID:15)" на стр. 209).
- Проверка съемных дисков (см. раздел "Задача Проверка съемных дисков (Removable_Drives_Scan, ID:16)" на стр. 220).
- Защита от сетевых угроз. (см. раздел "Задача Защита от сетевых угроз (Network_Threat_Protection, ID:17)" на стр. 222)
- Анализ поведения (см. раздел "Задача Анализ поведения (Behavior_Detection, ID:20)" на стр. 242).
- Контроль приложений (см. раздел "Задача Контроль приложений (Application_Control, ID:21)" на стр. 243).

Графический пользовательский интерфейс приложения позволяет также запускать следующие задачи по требованию:

- Поиск вредоносного ПО (см. раздел "Задача Поиск вредоносного ПО (Scan_My_Computer, ID:2)" на стр. 148).
- Выборочная проверка (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 156) (запускается при нажатии кнопкой мыши на файле или директории, которые вы хотите проверить).
- Проверка важных областей (см. раздел "Задача Проверка важных областей (Critical_Areas_Scan, ID:4)" на стр. 164).
- Проверка целостности системы (см. раздел "Контроль целостности системы по требованию (ODFIM)" на стр. 183).
- Проверка контейнеров (см. раздел "Задача Проверка контейнеров (Container_Scan, ID:18)" на стр. 224).
- Обновление (см. раздел "Задача Обновление (Update, ID:6)" на стр. 172).
- Откат обновления баз (см. раздел "Задача Откат обновления баз (Rollback, ID:7)" на стр. 176).

Кроме того, следующие задачи могут работать в информирующем режиме и в этом случае для них в интерфейсе 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 программ, а только информируют пользователя об обнаружении угрозы.

- Защита от файловых угроз (см. раздел "Задача Защита от файловых угроз (File_Threat_Protection, ID:1)" на стр. 133).
- Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 200).
- Защита от веб-угроз (см. раздел "Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)" на стр. 206).
- Контроль устройств (см. раздел "Задача Контроль устройств (Device_Control, ID:15)" на стр. 209).
- Защита от сетевых угроз. (см. раздел "Задача Защита от сетевых угроз (Network_Threat_Protection, ID:17)" на стр. 222)
- Анализ поведения (см. раздел "Задача Анализ поведения (Behavior_Detection, ID:20)" на стр. 242).
- Контроль приложений (см. раздел "Задача Контроль приложений (Application_Control, ID:21)" на стр. 243).

- Поиск вредоносного ПО (см. раздел "Задача Поиск вредоносного ПО (Scan_My_Computer, ID:2)" на стр. 148).
- Выборочная проверка (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 156), запущенная из консоли командой kesl-control --scan-file.
- Проверка важных областей (см. раздел "Задача Проверка важных областей (Critical_Areas_Scan, ID:4)" на стр. 164).
- Проверка контейнеров (см. раздел "Задача Проверка контейнеров (Container_Scan, ID:18)" на стр. 224).
- Выборочная проверка контейнеров (см. раздел "Задача Выборочная проверка контейнеров (Custom_Container_Scan, ID:19)" на стр. 234), запущенная из консоли командой kesl-control --scan-container.

Включение и выключение мониторинговых задач приложения

Вы можете включать и выключать мониторинговые задачи (см. раздел "Управление задачами" на стр. 501) приложения. Если задача включена, доступна кнопка **Выключить**. По умолчанию включены задачи Защита от файловых угроз, Защита от веб-угроз, Контроль устройств и Анализ поведения.

Если задача выключена, доступна кнопка **Включить**.

► *Чтобы включить или выключить мониторинговую задачу приложения:*

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Настройка**.

   Откроется окно **Настройка**.
3. Выполните следующие действия для нужной задачи:
   - Если вы хотите включить задачу, нажмите на кнопку **Включить**.
   - Если вы хотите выключить задачу, нажмите на кнопку **Выключить**.

Запуск и остановка задач проверки

С помощью графического пользовательского интерфейса приложения вы можете запускать и останавливать задачи **Поиск вредоносного ПО**, **Проверка важных областей** и **Проверка контейнеров**.

► *Чтобы запустить или остановить задачу проверки:*

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на раздел **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 выполнения и результат работы временных задач Scan_Boot_Sectors_{идентификатор} и Scan_File_{идентификатор}. Вы можете скрыть информацию о выполненных временных задачах, нажав на крестик или закрыв окно **Проверка** (при переходе в главное окно (см. раздел "Интерфейс приложения" на стр. 500) или при выходе из приложения (см. раздел "Интерфейс приложения" на стр. 500)).

Запуск и остановка задач обновления

С помощью графического пользовательского интерфейса приложения вы можете запускать задачи **Обновление** и **Откат обновления баз**.

► *Чтобы запустить или остановить задачу обновления:*

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на раздел **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 баз:*

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**.

kaspersky

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

Информация о работе задач приложения записывается в отчеты 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 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.

В приложении доступны следующие отчеты, перечисленные в окне **Отчеты** слева:

- **Статистика**. Этот отчет содержит статистические данные о задаче Защита от файловых угроз и 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 мониторинговых задач приложения:
  - Защита от шифрования.
  - Контроль целостности системы.
  - Управление сетевым экраном.
  - Защита от веб-угроз.
  - Контроль приложений.
  - Контроль устройств.
  - Проверка съемных дисков.
  - Защита от сетевых угроз.
  - Анализ поведения.
  - Защита от файловых угроз.
- **Задачи по требованию**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы следующих задач приложения:
  - Задачи проверки.
  - Обновление.
  - Проверка 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 отчета, представленную в отдельном блоке, 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 в Хранилище

► *Чтобы просмотреть объекты в Хранилище:*

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Хранилище**.

   Откроется окно **Хранилище**.

В окне отображается следующая информация об объектах в Хранилище:

- название объекта;
- полный путь к объекту;
- дата добавления объекта в Хранилище;
- дата удаления объекта из Хранилища (это поле отображается, если задан параметр DaysToLive (см. раздел "Параметры задачи Управление Хранилищем" на стр. 179));
- размер объекта.

Вы можете восстановить объекты из Хранилища в их исходные директории. Вы также можете удалить объекты из Хранилища. Удаленные объекты восстановить невозможно. Информация об этих действиях записывается в журнал событий.

Просмотр информации о лицензии

► *Чтобы просмотреть информацию о лицензии:*

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 с уникальной буквенно-цифровой последовательностью, которая отображается в поле **Ключ**.

Откроется окно **Лицензия**.

В окне отображается следующая информация о лицензии:

- **Активный ключ** – уникальная буквенно-цифровая последовательность.
- **Статус ключа** – статус ключа или сообщение о каких-либо проблемах, связанных с ключом (при их наличии).
- **Действует с** – дата активации приложения путем добавления этого ключа.
- **Срок действия лицензии истекает** – количество дней до истечения срока действия лицензии и дата окончания срока действия лицензии в формате UTC.
- Сводная информация о лицензии или сообщение о каких-либо проблемах, связанных с лицензированием, и рекомендации о действиях, которые вам нужно выполнить для устранения проблем (при их наличии).

По ссылке **Подробнее** отображается следующая информация:

- **Название приложения** – название приложения, для которой предназначена лицензия, связанная с ключом.
- **Защита** – информация о доступной функциональности приложения и список доступных компонентов приложения (доступность функциональности и компонентов приложения зависит от лицензии).

Создание файла 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 специалиста из 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/kesl/. В файлах трассировки содержится информация об операционной системе, а также могут содержаться персональные данные (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 514).

Обновление баз программы 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.

kaspersky

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/).

kaspersky

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.

kaspersky

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 Endpoint Security.

Kaspersky предоставляет поддержку приложения Kaspersky Endpoint Security в течение жизненного цикла (см. страницу жизненного цикла приложений (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).

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас прислать *файл трассировки* (см. раздел "*Содержимое файлов трассировки и их хранение*" на стр. 514) или *файл дампа* (см. раздел "*Содержимое файлов дампа и их хранение*" на стр. 515).

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

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).

kaspersky

Содержимое файлов трассировки и их хранение

Файл трассировки позволяет отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка.

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".

По умолчанию файлы трассировки хранятся в директории /var/log/kaspersky/kesl/. Для доступа к заданной по умолчанию директории хранения файлов трассировки требуются root-права.

Во всех файлах трассировки хранятся 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.

Kaspersky Endpoint Security сохраняет пароли пользователей в файл трассировки только в зашифрованном виде.

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).

kaspersky

Содержимое файлов дампа и их хранение

Файл дампа содержит всю информацию о рабочей памяти процессов приложения Kaspersky Endpoint Security и его дочерних процессов на момент создания файла дампа. Если требуется, вы можете включить создание файлов дампа при сбое в работе приложения.

Вы можете настроить создание файлов дампов с помощью конфигурационного файла kesl.ini (см. раздел "Конфигурационные файлы параметров приложения" на стр. 523), а также в параметрах политики Kaspersky Endpoint Security с помощью Консоли администрирования Kaspersky Security Center (см. раздел "Окно Дополнительные параметры приложения" на стр. 333) и Kaspersky Security Center Web Console (см. раздел "Окно Параметры записи дампов" на стр. 451). По умолчанию файлы дампа хранятся в директориях /var/opt/kaspersky/kesl/common/dumps и /var/opt/kaspersky/kesl/common/dumps-user. Для доступа к файлам дампа требуются root-права. Максимальное количество файлов дампов ограничено.

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".

► *Чтобы включить создание файла дампа с помощью конфигурационного файла kesl.ini:*

1. Остановите Kaspersky Endpoint Security (см. раздел "Запуск и остановка приложения" на стр. 92).
2. Откройте файл /var/opt/kaspersky/kesl/common/kesl.ini на редактирование.
3. Добавьте следующий параметр в секцию **[General]**:

   ```
   CoreDumps=yes
   ```

4. Запустите Kaspersky Endpoint Security (см. раздел "Запуск и остановка приложения" на стр. 92).

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 225. 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

kaspersky

Приложения

Этот раздел содержит информацию, которая дополняет основной текст справки.

В этом разделе

Приложение 1. Оптимизация потребления ресурсов

При проверке объектов Kaspersky Endpoint Security использует ресурсы процессора, ввод-вывод дисковой подсистемы и оперативную память.

► *Чтобы посмотреть потребление ресурсов приложением, выполните следующую команду:*

```
top -bn1|grep kesl
```

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 kesl
```

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 Endpoint Security при проверке объектов критически замедляет работу системы, требуется провести настройку приложения для оптимизации потребления ресурсов системы.

В этом разделе

kaspersky

Определение задачи, которая занимает ресурсы

Для того, чтобы определить, какая задача или задачи приложения (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118) занимают ресурсы системы, требуется разделить потребление ресурсов задачей Защита от файловых угроз (см. раздел "Анализ работы задачи Защита от файловых угроз" на стр. 518) (тип OAS) и задачами проверки по требованию (см. раздел "Анализ работы задач проверки по требованию" на стр. 520) (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

► *Чтобы проанализировать работу задачи Защита от файловых угроз:*

1. Остановите (см. раздел "Запуск и остановка задачи" на стр. 123) все задачи проверки и мониторинга (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118).
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:

      ```
      kesl-control --get-task-list
      ```

   b. Получите параметры расписания задачи поиска вредоносного ПО, выполнив следующую команду:

      ```
      kesl-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:

      ```
      kesl-control --set-schedule <ID задачи> RuleType=Manual
      ```

3. Включите создание файлов трассировки приложения с высоким уровнем детализации, выполнив следующую команду:

   ```
   kesl-control --set-app-settings TraceLevel=Detailed
   ```

4. Запустите задачу Защита от файловых угроз, если она не была запущена, выполнив следующую команду:

   ```
   kesl-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. 520).

6. Выключите создание файлов трассировки приложения, выполнив следующую команду:

   ```
   kesl-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/kesl/kesl.* | 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.

   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/kesl/kesl.* | 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/kesl/kesl.* | awk '{print
       $7}' | 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. 520).

Анализ работы задач проверки по требованию

Также большое потребление ресурсов может быть вызвано использованием задач с типами ODS и ContainerScan (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118). 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. 518)) 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. 518) 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:*

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

► *Чтобы исключить конкретный файл или файлы по маске в директории /tmp/logs, выполните следующую команду:*

```
kesl-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:*

```
kesl-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:

   ```
   kesl-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. 518) было выявлено слишком много записываемых файлов, вы можете перевести файловый перехватчик в режим работы только при открытии файлов, выполнив следующую команду:

```
kesl-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

Настройка задач проверки по требованию с типами ODS и ContainerScan (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118) выполняется аналогично настройке исключений из проверки для задачи Защита от файловых угроз (см. раздел "Настройка задачи Защита от файловых угроз" на стр. 520), но для задач проверки по требованию с типами ODS и ContainerScan неприменима настройка исключения точек монтирования.

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. Это особенно актуально для серверов, имеющих сотни гигабайт оперативной памяти.

► *Чтобы указать ограничение на использование памяти при проверке:*

1. Остановите Kaspersky Endpoint Security (см. раздел "Запуск и остановка приложения" на стр. 92).
2. Откройте файл /var/opt/kaspersky/kesl/common/kesl.ini на редактирование.
3. Добавьте параметр `ScanMemoryLimit` с нужным значением в секцию `[General]`:

   `ScanMemoryLimit=8192`
4. Запустите Kaspersky Endpoint Security (см. раздел "Запуск и остановка приложения" на стр. 92).

Параметр `ScanMemoryLimit` ограничивает не общее количество памяти, которое использует приложение, а количество памяти, которое используется при проверке файлов, то есть общее количество памяти может быть больше значения, заданного этим параметром.

Приложение 2. Конфигурационные файлы приложения

В приложении предусмотрены конфигурационные файлы, содержащие параметры приложения, заданные при установке приложения, а также конфигурационные файлы, содержащие параметры по умолчанию для задач приложения.

Вы можете редактировать значения параметров конфигурационных файлов приложения из командной строки.

В этом разделе

Конфигурационные файлы параметров приложения

После первоначальной настройки в приложении создаются следующие конфигурационные файлы:

- /var/opt/kaspersky/kesl/common/agreements.ini

  Конфигурационный файл agreements.ini содержит параметры, связанные с Лицензионным соглашением, Политикой конфиденциальности и Положением о Kaspersky Security Network.

- /var/opt/kaspersky/kesl/common/kesl.ini

  Конфигурационный файл kesl.ini содержит параметры, приведенные в таблице ниже.

Если требуется, вы можете изменять значения параметров (см. раздел "Правила редактирования конфигурационных файлов задач приложения" на стр. 530) в этих файлах.

Изменять значения по умолчанию в этих файлах рекомендуется под руководством специалистов Службы технической поддержки по полученным от них инструкциям.

Таблица 226. Параметры конфигурационного файла kesl.ini

Параметр	Описание	Значения
Секция **[General]** содержит следующие параметры:		
ScanMemoryLimit	Ограничение на использование памяти приложением (см. раздел "Установка ограничения на использование памяти приложением" на стр. 106) в мегабайтах.	Значение по умолчанию: 8192.
ExecArgMax	Количество аргументов, которые приложение будет захватывать из вызова exec.	Значение по умолчанию: 50.
RevealSensitiveInfoInTraces	Отображение в файлах трассировки (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 514) информации, которая может содержать персональные данные (например, пароли).	`true/yes` – отображать информацию, которая может содержать персональные данные, в файлах трассировки приложения. `false/no` (значение по умолчанию) – не отображать информацию, которая может содержать персональные данные, в файлах трассировки.

Параметр	Описание	Значения
PackageType	Формат установленного пакета приложения (см. раздел "Установка приложения с помощью командной строки" на стр. 32). Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения.	`rpm` – установлен пакет формата RPM. `deb` – установлен пакет формата DEB.
Locale	Языковой стандарт, используемый для локализации событий приложения, отправляемых в Kaspersky Security Center. 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 Endpoint Security, то графический интерфейс и командная строка отображаются в английской локализации.	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`.
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. 37).	`true/yes` – операционная система поддерживает технологию fanotify. `false/no` – операционная система не поддерживает технологию fanotify.
CoreDumps	Включение создания файла дампа (см. раздел "Содержимое файлов дампа и их хранение" на стр. 515) при сбое в работе приложения.	`true/yes` – создавать файл дампа при сбое в работе приложения. `false/no` (значение по умолчанию) – не создавать файл дампа при сбое в работе приложения.
CoreDumpsPath	Путь к директории, в которой хранятся файлы дампа (см. раздел "Содержимое файлов дампа и их хранение" на стр. 515).	Значение по умолчанию: /var/opt/kaspersky/kesl/common/dumps. 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.

Параметр	Описание	Значения
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 kesl-control.	Значение по умолчанию: /var/run/bl4control.
KsvlaMode	Режим использования приложения Kaspersky Endpoint Security (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23). Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения (см. раздел "Выбор режима использования приложения" на стр. 34).	`true/yes` – приложение используется в режиме Легкого агента для защиты виртуальных сред. `false/no` – приложение используется в автономном режиме.
StartupTraces	Включение создания файлов трассировки (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 514) при запуске приложения.	`true/yes` – создавать файлы трассировки при запуске приложения. `false/no` (значение по умолчанию) – не создавать файлы трассировки при запуске приложения.
MaxInotifyWatches	Ограничение количества подписок на изменения в файлах и директориях (user watches), указанное в файле /proc/sys/fs/inotify/max_user_watches.	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
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). 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.	`true/yes` – использовать публичный DNS для доступа к серверам "Лаборатории Касперского". `false/no` (значение по умолчанию) – не использовать публичный DNS для доступа к серверам "Лаборатории Касперского".
Секция **[Network]** содержит следующие параметры:		
WtpFwMark	Метка в правилах утилиты iptables для перенаправления трафика в приложение для обработки задачей Защита от веб-угроз (см. раздел "Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)" на стр. 206). 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 десятеричным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 0x100.

Параметр	Описание	Значения
NtpFwMark	Метка в правилах утилиты iptables для перенаправления трафика в приложение для обработки задачей Защита от сетевых угроз (см. раздел "Задача Защита от сетевых угроз (Network_Threat_Protection, ID:17)" на стр. 222). 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 десятеричным 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 десятеричным 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 десятеричным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 0x800.
ProxyRouteTable	Номер таблицы маршрутизации.	Значение по умолчанию: 101.
Секция **[Virtualization]** содержит следующие параметры:		
ServerMode	Роль защищенной виртуальной машины (см. раздел "Определение роли виртуальной машины" на стр. 34), на которой приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23): сервер или рабочая станция. Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения (см. раздел "Определение роли виртуальной машины" на стр. 34).	`true/yes` – виртуальная машина используется как сервер. `false/no` – виртуальная машина используется как рабочая станция.

Параметр	Описание	Значения
VdiMode	Включение режима защиты инфраструктуры VDI (на стр. 35) в случае использования приложения в режиме Легкого агента для защиты виртуальных сред (см. раздел "О режимах использования приложения Kaspersky Endpoint Security" на стр. 23). Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения (см. раздел "Включение режима защиты инфраструктуры VDI" на стр. 35).	`true/yes` – режим защиты инфраструктуры VDI включен. `false/no` – режим защиты инфраструктуры VDI выключен.
Секция **[Watchdog]** содержит следующие параметры:		
TimeoutAfterHeadshot	Максимальное время ожидания завершения управляемого процесса от момента отправки сигнала HEADSHOT Watchdog-сервером управляемому процессу.	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.
TimeoutAfterKill	Максимальное время ожидания завершения управляемого процесса от момента отправки сигнала SIGKILL Watchdog-сервером управляемому процессу. Если по истечении этого времени управляемый процесс 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 мсек.
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 управляемого процесса.	Значение по умолчанию: 2 мин.

Параметр	Описание	Значения
ConnectTimeout	Максимальный интервал времени от момента запуска управляемого процесса до момента установления приложением соединения с Watchdog-сервером. Если приложение не успевает создать соединение за этот интервал времени, Watchdog-сервер начнет процедуру завершения управляемого процесса.	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 мсек.
TimeoutAfterShutdown	Максимальное время ожидания завершения управляемого процесса от момента отправки сигнала SHUTDOWN Watchdog-сервером управляемому процессу.	Значение по умолчанию: 2 мин.
MaxVirtualMemory	Ограничение на использование виртуальной памяти управляемого процесса. Если виртуальная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения управляемого процесса.	`Off` (значение по умолчанию) – использование виртуальной памяти не ограничено. `<значение>MB` – значение в мегабайтах.
MaxSwapMemory	Ограничение на размер swap-файла управляемого процесса. Если swap-файл управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения управляемого процесса.	`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.

Параметр	Описание	Значения
MaxMemory	Ограничение на использование резидентной памяти управляемого процесса. Если резидентная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения управляемого процесса.	`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`.

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 (см. раздел "Управление задачами приложения с помощью командной строки" на стр. 118).
- Если параметр принадлежит к какой-либо секции, укажите его только в этой секции. В пределах одной секции вы можете указывать параметры в любом порядке.
- Заключайте 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`.
- Заключайте 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.

Конфигурационный файл задачи Защита от файловых угроз

```
ScanArchived=No
ScanSfxArchived=No
ScanMailBases=No
ScanPlainMail=No
SkipPlainTextFiles=No
TimeLimit=60
SizeLimit=0
FirstAction=Recommended
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=*
```

Конфигурационный файл задачи Поиск вредоносного ПО

```
ScanFiles=Yes
ScanBootSectors=Yes
ScanComputerMemory=Yes
ScanStartupObjects=Yes
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
```

```
HeuristicLevel=Recommended
UseIChecker=Yes
DeviceNameMasks.item_0000=/**
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Выборочная проверка

```
ScanFiles=Yes
ScanBootSectors=No
ScanComputerMemory=No
ScanStartupObjects=No
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
DeviceNameMasks.item_0000=/**
```

```
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Проверка важных областей

```
ScanFiles=No
ScanBootSectors=Yes
ScanComputerMemory=Yes
ScanStartupObjects=Yes
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
DeviceNameMasks.item_0000=/**
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
```

```
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Обновление

```
SourceType="KLServers"
UseKLServersWhenUnavailable=Yes
ApplicationUpdateMode=DownloadOnly
ConnectionTimeout=10
```

Конфигурационный файл задачи Управление Хранилищем

```
DaysToLive=90
BackupSizeLimit=0
BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

Конфигурационный файл задачи Контроль целостности системы

```
UseExcludeMasks=No
[ScanScope.item_0000]
AreaDesc=Kaspersky internal objects
UseScanArea=Yes
Path=/opt/kaspersky/kesl/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Управление сетевым экраном

```
DefaultIncomingAction=Allow
DefaultIncomingPacketAction=Allow
OpenNagentPorts=Yes
[NetworkZonesTrusted]
[NetworkZonesLocal]
[NetworkZonesPublic]
```

Конфигурационный файл задачи Защита от шифрования

```
UseHostBlocker=Yes
BlockTime=30
UseExcludeMasks=No
[ScanScope.item_0000]
AreaDesc=All shared directories
UseScanArea=Yes
Path=AllShared
AreaMask.item_0000=*
```

Конфигурационный файл задачи Защита от веб-угроз

```
UseTrustedAddresses=Yes
ActionOnDetect=Block
CheckMalicious=Yes
CheckPhishing=Yes
UseHeuristicForPhishing=Yes
CheckAdware=No
CheckOther=No
```

Конфигурационный файл задачи Контроль устройств

```
RulesAction=ApplyRules
[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
```

Конфигурационный файл задачи Проверка съемных дисков

```
ScanRemovableDrives=NoScan
ScanOpticalDrives=NoScan
BlockDuringScan=No
```

Конфигурационный файл задачи Защита от сетевых угроз

```
ActionOnDetect=Block
BlockAttackingHosts=Yes
BlockDurationMinutes=60
UseExcludeIPs=No
```

Конфигурационный файл задачи Проверка контейнеров

```
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
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
```

Вы можете использовать параметры этого конфигурационного файла также для задачи Выборочная проверка контейнеров (см. раздел "Задача Выборочная проверка контейнеров (Custom_Container_Scan, ID:19)" на стр. 234).

Конфигурационный файл задачи Анализ поведения

```
UseTrustedPrograms=No
TaskMode=Block
```

Конфигурационный файл задачи Контроль приложений

```
AppControlMode=DenyList
AppControlRulesAction=ApplyRules
```

Конфигурационный файл задачи Инвентаризация

```
ScanScripts=Yes
ScanBinaries=Yes
ScanAllExecutable=Yes
CreateGoldenImage=No
```

```
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/usr/bin
AreaMask.item_0000=*
```

Конфигурационный файл задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA)

```
UseClientPinnedCertificate=No
SynchronizationPeriod=5
ConnectionTimeout=10
RequestTimeout=10
EnableTelemetry=Yes
[Endpoints.item_0000]
Address=
Port=443
[EventTransferSettings]
MaximumDataTransferTime=30
UseRequestCountLimits=Yes
MaximumNumberOfEventsInHour=3000
EventLimitExceededPercentage=15
```

Приложение 3. Коды возврата командной строки

В приложении Kaspersky Endpoint Security 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 Endpoint Security не запущено;

66 – базы приложения не загружены (используется только командой `kesl-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 (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 156) или Выборочная проверка контейнеров (см. раздел "Задача Выборочная проверка контейнеров (Custom_Container_Scan, ID:19)" на стр. 234) обнаружены угрозы;

73 – попытка задать параметры задачи Контроль приложений (см. раздел "Задача Контроль приложений (Application_Control, ID:21)" на стр. 243), влияющие на работу приложения, без их подтверждения с помощью флага `--accept`.

74 – требуется перезапуск приложения Kaspersky Endpoint Security 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 4. 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 227. Параметры и их безопасные значения для приложения в сертифицированной конфигурации

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. Если первым действием выбрано `Remove`, то `SecondAction` указывать не нужно. • `Recommended` (выполнять рекомендуемое действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе.

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
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.
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.

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
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.
ScanByAccessType	задача Защита от файловых угроз	Одно из следующих значений: • `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.

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
SourceType	задача Обновление	Одно из следующих значений: • `KLServers` – 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. • `Custom` – приложение загружает обновления из пользовательского источника, указанного в секции `[CustomSources.item_#]`. 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	`Disabled` – не загружать и не устанавливать обновления приложения.
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.
RulesAction	задача Контроль устройств	`ApplyRules` (значение по умолчанию) – приложение применяет правила доступа и выполняет заданное в правилах действие.
AppControlRulesAction	задача Контроль приложений	`ApplyRules` (значение по умолчанию) – Kaspersky Endpoint Security применяет правила контроля приложений и выполняет заданное в правилах действие.
ScanRemovableDrives	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).

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
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.
CloudMode	общие параметры приложения	`No` – использовать полную версию баз вредоносного ПО.
UseMDR	общие параметры приложения	`No` – выключить Managed Detection and Response.

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

kaspersky

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.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Ubuntu и LTS являются зарегистрированными товарными знаками Canonical Ltd.

Citrix – товарный знак Citrix Systems, Inc. и / или дочерних компаний, зарегистрированный в патентном офисе США и других стран.

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 Public DNS – товарный знак Google LLC.

HUAWEI, EulerOS, FusionSphere являются товарными знаками 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, Hyper-V, Outlook, Visual C++ и Windows являются товарными знаками группы компаний Microsoft.

OpenStack – зарегистрированный товарный знак OpenStack Foundation в США и других странах.

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.

VMware vSphere – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.