KASPERSKY lab

Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 10.1.1.6421

Уважаемый пользователь!

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

Дата редакции документа: 27.03.2019

Обозначение документа: 643.46856491.00049-07 90 01

https://www.kaspersky.ru

https://help.kaspersky.com/ru

https://support.kaspersky.ru

Содержание

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux" (далее также "Kaspersky Endpoint Security", "программа").

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

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

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка и администрирование Kaspersky Endpoint Security, а также поддержка организаций, использующих Kaspersky Endpoint Security. Документ адресован техническим специалистам, которые имеют опыт с системой удаленного централизованного управления программами "Лаборатории Касперского" Kaspersky Security Center.

В этом разделе

В этом документе

Это руководство содержит следующие разделы.

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

О программе

Этот раздел содержит описание возможностей программы, а также краткую информацию о функциях и компонентах программы. Вы узнаете о том, из чего состоит комплект поставки и какие услуги доступны зарегистрированным пользователям программы.

Требования

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

Подготовка к установке программы

Этот раздел содержит инструкции по установке и удалению Kaspersky Endpoint Security.

Установка программы

Этот раздел содержит информацию о том, как установить Kaspersky Endpoint Security на компьютер.

Удаление программы

Этот раздел содержит информацию о том, как удалить программу с компьютера.

Обновление старой версии программы

Этот раздел содержит информацию о том, как обновить программу.

Процедура приемки

Этот раздел содержит информацию о подготовке программы к работе и проверке ее работоспособности.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

Запуск и остановка программы

Этот раздел содержит информацию о том, как запускать, перезапускать и завершать работу программы из командной строки.

Общие параметры Kaspersky Endpoint Security

Этот раздел содержит информацию об общих параметрах программы.

Управление задачами Kaspersky Endpoint Security с помощью командной строки

Этот раздел содержит информацию о типах задач Kaspersky Endpoint Security и инструкции о том, как управлять задачами.

Задача Защита от файловых угроз (File_Monitoring ID:1)

Этот раздел содержит информацию о Защите от файловых угроз и описание ее параметров.

Задача антивирусной проверки (Scan_My_Computer ID:2)

Этот раздел содержит информацию о задаче антивирусной проверки и описание ее параметров.

Задача выборочной проверки (Scan_File ID:3)

Этот раздел содержит информацию о задаче выборочной проверки и описание ее параметров.

Задача проверки загрузочных секторов (Boot_Scan ID:4)

Этот раздел содержит информацию о задаче проверки загрузочных секторов и описание ее параметров.

Задача проверки памяти процессов (Memory_Scan ID:5)

Этот раздел содержит информацию о задаче проверки памяти процессов и описание ее параметров.

Задача обновления (Update ID:6)

Этот раздел содержит информацию об обновлении антивирусных баз и модулей программы (далее также "обновления") и инструкции, как настроить параметры обновления.

Задача отката обновления (Rollback ID:7)

Этот раздел содержит информацию о задаче отката обновления.

Задача копирования обновлений (Retranslate ID:8)

Этот раздел содержит информацию о задаче копирования обновлений и описание ее параметров.

Задача реализации сервера лицензий (License ID:9)

Этот раздел содержит информацию о задаче реализации сервера лицензий.

Задача управления Хранилищем (Backup ID:10)

Этот раздел содержит инструкции, как настроить параметры Хранилища, и информацию о том, какие действия можно выполнять над объектами в Хранилище.

Задача мониторинга файловых операций (Integrity_Monitoring ID:11)

Этот раздел содержит информацию о задаче Мониторинг файловых операций и описание ее параметров.

Задача Управление сетевым экраном (Firewall ID:12)

Этот раздел содержит информацию о задаче Управление сетевым экраном и описание ее параметров.

Задача Защита от шифрования (AntiCryptor ID:13)

Этот раздел содержит информацию о задаче Защита от шифрования и описание ее параметров.

Участие в Kaspersky Security Network

Этот раздел содержит информацию об участии в Kaspersky Security Network и инструкции о том, как включить и выключить использование Kaspersky Security Network.

Управление программой через Kaspersky Security Center

Этот раздел содержит информацию об управлении Kaspersky Endpoint Security с помощью Kaspersky Security Center.

Управление программой через Kaspersky Security Center Web Console

Этот раздел содержит информацию об управлении Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console.

Использование графического пользовательского интерфейса Kaspersky Endpoint Security

Этот раздел содержит описание работы в Kaspersky Endpoint Security с использованием графического пользовательского интерфейса.

Устранение уязвимостей и установка критических обновлений в программе

Этот раздел содержит информацию об устранении уязвимости и установке критических обновлений в программе.

Действия после сбоя или неустранимой ошибки в работе программы

Этот раздел содержит информацию о работе программы после сбоя.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Приложения

Этот раздел содержит информацию о параметрах конфигурационных файлов по умолчанию, коды возврата командной строки, инструкции по настройке совместной работы программы с Linux Mail Server, а также описание значений параметров программы в сертифицированном состоянии.

Глоссарий

Этот раздел содержит список терминов, которые встречаются в тексте документа, а также определения этих терминов.

АО "Лаборатория Касперского"

Этот раздел содержит информацию об АО "Лаборатория Касперского".

Информация о стороннем коде

Этот раздел содержит информацию о стороннем коде.

Уведомления о товарных знаках

Этот раздел содержит информацию о товарных знаках, упомянутых в документе.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком "Пример".

Пример текста	Описание условного обозначения
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком "стрелка".
В командной строке введите текст `help` Появится следующее сообщение: Укажите дату в формате `ДД:ММ:ГГ`.	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

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

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

В этом разделе

Источники для самостоятельного поиска информации

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);
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. стр. 182).

Для использования источников информации на веб-сайтах требуется подключение к интернету.

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

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

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

Страница Kaspersky Endpoint Security в Базе знаний

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

На странице Kaspersky Endpoint Security в Базе знаний (https://support.kaspersky.ru/kes10linux) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

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

Документация

В состав документации к программе входят файлы руководства администратора.

В руководстве администратора вы можете найти информацию для выполнения следующих задач:

- подготовка к установке, установка и активация Kaspersky Endpoint Security;
- настройка и использование Kaspersky Endpoint Security;
- удаленное управление Kaspersky Endpoint Security через Kaspersky Security Center.

Обсуждение программ "Лаборатории Касперского" на форуме

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

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

О программе

Программное изделие Kaspersky Endpoint Security представляет собой средство антивирусной защиты типа "Б" второго класса защиты и предназначено для применения на серверах информационных систем.

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).

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия
- сигнализация программы;
- идентификация и аутентификация.

Требования

В этой главе

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Минимальные общие требования:

- процессор Core™ 2 Duo 1.86 GHz;
- 1 GB оперативной памяти для 32-битных операционных систем;
- 2 GB оперативной памяти для 64-битных операционных систем;
- раздел подкачки не менее 1 GB;
- 1 GB свободного места на жестком диске.

Программные требования:

- Поддерживаемые 32-битные операционные системы:
  - Ubuntu 16.04 LTS;
  - Red Hat® Enterprise Linux® 6.7;
  - Red Hat Enterprise Linux 7.2;
  - CentOS-6.7;
  - Debian GNU / Linux 8.6;
  - Debian GNU / Linux 9.4;
  - Linux Mint 18.2;
  - Linux Mint 19;
  - Альт Линукс СПТ 7.0 (работа с графическим пользовательским интерфейсом не поддерживается);
  - Альт 8 СП Рабочая станция;
  - Альт 8 СП Сервер;
  - Альт Линукс 8.2 Рабочая станция;
  - Альт Линукс 8.2 Рабочая станция К;
  - Альт Линукс 8.2 Сервер;
  - Альт Линукс 8.2 Образование;

  - Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6)
  - Лотос;
  - РЕД ОС.
- Поддерживаемые 64-битные операционные системы:
  - Ubuntu 16.04 LTS;
  - Ubuntu 18.04 LTS;
  - Red Hat Enterprise Linux 6.7;
  - Red Hat Enterprise Linux 7.2;
  - CentOS-6.7;
  - CentOS-7.2;
  - Debian GNU / Linux 8.6;
  - Debian GNU / Linux 9.4;
  - OracleLinux 7.3;
  - SUSE® Linux Enterprise Server 15;
  - openSUSE® 15;
  - Альт Линукс СПТ 7.0 (работа с графическим пользовательским интерфейсом не поддерживается);
  - Альт 8 СП Рабочая станция;
  - Альт 8 СП Сервер;
  - Альт Линукс 8.2 Рабочая станция;
  - Альт Линукс 8.2 Рабочая станция К;
  - Альт Линукс 8.2 Сервер;
  - Альт Линукс 8.2 Образование;
  - Amazon Linux AMI;
  - Linux Mint 18.2;
  - Linux Mint 19;
  - Micro Focus Open Enterprise Server 2018;
  - Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды);
  - Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды);
  - Astra Linux Common Edition 2.12;
  - программный комплекс терминального доступа «Циркон 36КТ»;
  - программный комплекс терминального доступа «Циркон 36СТ»;
  - ОС РОСА «КОБАЛЬТ» (версия 7.3 для клиентских систем);
  - ОС РОСА «КОБАЛЬТ» (версия 7.3 для серверных систем);
  - ЕМИАС 1.0;

  - Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6);
  - Лотос;
  - РЕД ОС.
- Интерпретатор языка Perl версии 5.10 или выше.
- Установленная утилита which.
- Установленные пакеты для компиляции программ и запуска задач (gcc, binutils, glibc, glibc-devel, make, ld, rpcbind).
- исходный код ядра операционной системы – для компиляции модулей Kaspersky Endpoint Security на операционных системах, не поддерживающих технологию fanotify.

До установки программы и Агента администрирования на операционной системе SUSE Linux Enterprise Server 15 должен быть установлен пакет insserv-compat.

Kaspersky Endpoint Security 10 SP1 MR1 для Linux совместим с Kaspersky Security Center 10 и Kaspersky Security Center 11.

Для работы плагина управления Kaspersky Endpoint Security должен быть установлен Microsoft® Visual C++ 2015 Redistributable Update 3 RC.

Инсталляционный комплект

В комплект поставки входит дистрибутив Kaspersky Endpoint Security, содержащий следующие файлы:

- `kesl-10.1.1-<номер сборки>.i386.rpm`

  `kesl_10.1.1-<номер сборки>_i386.deb`

  Содержат основные файлы Kaspersky Endpoint Security. Пакеты могу быть установлены на 32-битные операционные системы в соответствии с типом пакетного менеджера.
- `kesl-10.1.1-<номер сборки>.x86_64.rpm`

  `kesl_10.1.1-<номер сборки>_amd64.deb`

  Содержат основные файлы Kaspersky Endpoint Security. Пакеты могу быть установлены на 64-битные операционные системы в соответствии с типом пакетного менеджера.
- `kesl.zip`

  Содержит файлы, используемые в процедуре удаленной установки Kaspersky Endpoint Security с помощью Kaspersky Security Center.
- `klnagent-<номер сборки>.i386.rpm`

  `klnagent_<номер сборки>_i386.deb`

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

  `klnagent64_<номер сборки>_amd64.deb`

  Содержат Агент Администрирования (утилиту связи Kaspersky Endpoint Security с Kaspersky Security Center.

- `klnagent-rpm.tar.gz`

  `klnagent-deb.tar.gz`

  Содержат файлы klnagent.kpd и akinstall.sh, используемые в процедуре удаленной установки Агента Администрирования с помощью Kaspersky Security Center.

- Файл `ksn_license.<ID языка>`, с помощью которого вы можете ознакомиться с условиями участия в Kaspersky Security Network.

- Файл `license.<ID языка>`, с помощью которого вы можете ознакомиться с Лицензионным соглашением. В Лицензионном соглашении указано, на каких условиях вы можете пользоваться программой.

Указания по эксплуатации

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

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

Подготовка к установке программы

Перед установкой программы убедитесь, что программные и аппаратные ресурсы компьютера, на который будет произведена установка, удовлетворяют требованиям, приведенным в разделе "Аппаратные и программные требования".

Также нужно убедиться, 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.

Установка программы

Этот раздел содержит инструкции о том, как установить пакет установки (далее «пакет») Kaspersky Endpoint Security и Агента администрирования.

В этой главе

Об установке Kaspersky Endpoint Security

Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM.

► *Для работы с Kaspersky Endpoint Security вам требуется выполнить следующие операции:*

1. Установить пакет Kaspersky Endpoint Security.
2. Запустить скрипт обновления параметров.
3. Установить пакет Агента администрирования и плагин управления Kaspersky Endpoint Security, если вы планируете управлять Kaspersky Endpoint Security с помощью Kaspersky Security Center.

   Плагин управления Kaspersky Endpoint Security Service Pack 1 и плагин управления Kaspersky Endpoint Security Service Pack 1 Maintenance Release 1 можно устанавливать одновременно. Таким образом, можно управлять программой с помощью политик, созданных с помощью обеих версий плагина управления. Можно также преобразовать политики и задачи, созданные с помощью плагина управления Kaspersky Endpoint Security Service Pack 1, в новые версии.

Для доступа к файлам и директориям программы во время установки, а также во время загрузки и применения обновления программы требуются root-права.

Установка пакета Kaspersky Endpoint Security

Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM.

► *Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 32-битную операционную систему, выполните следующую команду:*

```
# rpm -i kesl-10.1.1-<номер сборки>.i386.rpm
```

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

```
# rpm -i kesl-10.1.1-<номер сборки>.x86_64.rpm
```

- *Чтобы установить Kaspersky Endpoint Security из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:*

```
# dpkg -i kesl_10.1.1-<номер сборки>_i386.deb
```

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

```
# dpkg -i kesl_10.1.1-<номер сборки>_amd64.deb
```

Установка Kaspersky Endpoint Security с помощью Kaspersky Security Center

Вы можете установить Kaspersky Endpoint Security на компьютер с помощью Kaspersky Security Center. Подробнее об этом типе установки программы вы можете прочитать в документации для Kaspersky Security Center.

Установка Агента администрирования

Установка Агента администрирования требуется, если вы планируете управлять Kaspersky Endpoint Security с помощью Kaspersky Security Center.

Запускать процесс установки Агента администрирования требуется с root-правами.

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

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

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

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

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

```
# dpkg -i klnagent_<номер сборки>_i386.deb
```

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

```
# dpkg -i klnagent64_<номер сборки>_amd64.deb
```

► *После установки пакета запустите скрипт послеустановочной настройки Kaspersky Endpoint Security, выполнив следующую 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
  ```

Удаление программы

Этот раздел содержит инструкции о том, как удалить Kaspersky Endpoint Security локально или через Kaspersky Security Center.

В этой главе

Локальное удаление Kaspersky Endpoint Security

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

- *Чтобы удалить Kaspersky Endpoint Security, установленный из пакета формата RPM, выполните следующую команду:*

  ```
  # rpm -e kesl
  ```

- *Чтобы удалить Kaspersky Endpoint Security, установленный из пакета формата DEB, выполните следующую команду:*

  ```
  # dpkg -r kesl
  ```

- *Чтобы удалить Агент администрирования, установленный из пакета формата RPM, выполните следующую команду:*

  ```
  # rpm -e klnagent
  ```

- *Чтобы удалить Агент администрирования, установленный из пакета формата DEB, выполните следующую команду:*

  ```
  # dpkg -r klnagent
  ```

Программа автоматически выполняет процедуру удаления. По завершении программа выводит сообщение о результатах удаления.

После удаления Kaspersky Endpoint Security база данных лицензии сохраняется, и ее можно использовать для повторной установки программы.

Удаление Kaspersky Endpoint Security через Kaspersky Security Center

Вы можете удалить Kaspersky Endpoint Security через Kaspersky Security Center. Для этого вам нужно создать и запустить задачу удаления Kaspersky Endpoint Security.

Подробнее о создании и запуске задачи удаления Kaspersky Endpoint Security вы можете прочитать в документации для Kaspersky Security Center.

Обновление старой версии программы

В этой главе

Kaspersky Endpoint Security 10 Service Pack 1 для Linux можно обновить до Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux.

Вне зависимости от того, была ли запущена программа до начала процесса обновления, при успешном обновлениии запускается новая версия программы. При неуспешном обновлении запускается предыдущая версия.

Вы можете обновить предыдущую версию программы следующими способами:

- локально из командной строки (см. стр. 28);
- удаленно с помощью пакета Kaspersky Security Center (см. документацию для Kaspersky Security Center).

Доступно только обновление Kaspersky Endpoint Security 10 Service Pack 1 для Linux до Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux.
Чтобы обновить Kaspersky Endpoint Security 10 для Linux, сначала необходимо обновить программу до версии Kaspersky Endpoint Security 10 Service Pack 1.

Перед началом обновления предыдущей версии программы рекомендуется закрыть все работающие программы.

Обновление программы с помощью командной строки

Kaspersky Endpoint Security 10 Service Pack 1 для Linux можно обновить до Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux локально, выполнив приведенную ниже процедуру.

После завершения процедуры обновления может потребоваться перезагрузка операционной системы или программы.

► *Чтобы обновить программу, выполните следующие действия:*

1. Запустите требуемый пакет установки Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux.

   - для 32-битной операционной системы:

     ```
     # rpm -i kesl-10.1.1-<номер сборки>.i386.rpm
     ```

   - для 64-битной операционной системы:

     ```
     # rpm -i kesl-10.1.1-<номер сборки>.x86_64.rpm
     ```

   Kaspersky Endpoint Security 10 Service Pack 1 для Linux будет остановлен, и будет выполнен экспорт параметров программы и журнала событий.

2. Запустите скрипт послеустановочной настройки (см. стр. 24).

   Скрипт послеустановочной настройки пошагово запрашивает значения параметров Kaspersky Endpoint Security.

   > Согласие с условиями Лицензионного соглашения и Политики конфиденциальности является обязательным. Если вы не принимаете условия Лицензионного соглашения и Политики конфиденциальности, процесс обновления программы будет прерван.

   Параметры программы и журнал событий передаются в обновленную версию программы; для новых параметров устанавливаются значения по умолчанию. Программа останавливается во время переноса ее параметров.

3. При необходимости перезагрузите операционную систему или программу.

Если во время процедуры обновления программы произошла ошибка, программу невозможно автоматически вернуть к предыдущей версии. Отображается сообщение об ошибке.

Если во время переноса параметров по какой-либо причине происходит ошибка, для программы устанавливаются значения по умолчанию.

Обновление программы с помощью Kaspersky Security Center

Kaspersky Endpoint Security 10 Service Pack 1 для Linux можно удаленно обновить до Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux с помощью Kaspersky Security Center, выполнив приведенную ниже процедуру.

► *Чтобы обновить программу, управляемую с помощью политики Kaspersky Security Center, выполните следующие действия:*

1. Обновите Агента администрирования (см. стр. 39).

   Если Агент администрирования не обновлен, программой невозможно управлять через Kaspersky Security Center.

   Программа работает корректно во время обновления Агента администрирования.

2. Удаленно установите Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux.

Если программу необходимо перезапустить, и зарегистрировано событие *NeedToRestart*, дождитесь полного завершения задачи удаленной установки. После этого перезапустите Kaspersky Endpoint Security средствами Kaspersky Security Center. Если пакет успешно установлен после перезапуска, будет запущена новая версия программы. Если установка пакета завершается с ошибкой, обновление откатывается, и запускается предыдущая версия программы. Тем не менее, в пакетном менеджере (rpm/dpkg) будет указана новая версия.

Подробнее об этом типе обновления программы вы можете прочитать в документации для Kaspersky Security Center.

Процедура приемки

После успешной установки программы перед ее вводом в эксплуатацию проводится процедура приемки установленной программы, включающая проверку ее работоспособности, подготовку программы к работе и приведение конфигурации программы в соответствие сертифицируемой конфигурации.

В этой главе

Подготовка программы к работе

Этот раздел содержит инструкции о первоначальной настройке Kaspersky Endpoint Security.

О первоначальной настройке Kaspersky Endpoint Security

После установки Kaspersky Endpoint Security требуется запустить скрипт послеустановочной настройки Kaspersky Endpoint Security. Скрипт послеустановочной настройки Kaspersky Endpoint Security входит в пакет Kaspersky Endpoint Security.

Если вы не выполнили процедуру первоначальной настройки Kaspersky Endpoint Security, антивирусная защита компьютера не будет работать.

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

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

Скрипт послеустановочной настройки пошагово запрашивает значения параметров Kaspersky Endpoint Security.

Скрипт послеустановочной настройки необходимо запустить с root-правами после завершения установки пакета Kaspersky Endpoint Security.

Только Kaspersky Endpoint Security 10 Service Pack 1 для Linux можно обновить до Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux (см. стр. 39).

Антивирус Касперского 8.0 для Linux File Server и Kaspersky Endpoint Security 10 для Linux нельзя обновить до Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux. Вам необходимо удалить предыдущую версию программы и установить Kaspersky Endpoint Security 10 Service Pack 1 для Linux.

Шаг 1. Выбор языкового стандарта

На этом шаге вам нужно задать обозначение языкового стандарта, который будет использоваться при работе Kaspersky Endpoint Security.

Вы можете задать языковой стандарт в формате, определенном в RFC 3066.

► *Чтобы получить полный список обозначений языковых стандартов, выполните следующую команду:*

```
# locale -a
```

По умолчанию программа предлагает использовать языковой стандарт, установленный для root.

Шаг 2. Принятие Лицензионного соглашения

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

Вы можете просмотреть текст с помощью утилиты `less`. Для перемещения по тексту используйте клавиши управления курсором или клавиши **B** (для перемещения назад на один экран) и **F** (для перемещения вперед на один экран). Для получения справки используйте клавишу **H**. Для завершения просмотра используйте клавишу **Q**.

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы согласны с условиями Лицензионного соглашения;
- `no` (или `n`), если вы не согласны с условиями Лицензионного соглашения.

Если вы не согласны с условиями Лицензионного соглашения, программа прерывает процесс настройки Kaspersky Endpoint Security.

Шаг 3. Принятие Политики конфиденциальности

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

Вы можете просмотреть текст с помощью утилиты `less`. Для перемещения по тексту используйте клавиши управления курсором или клавиши **B** (для перемещения назад на один экран) и **F** (для перемещения вперед на один экран). Для получения справки используйте клавишу **H**. Для завершения просмотра используйте клавишу **Q**.

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы принимаете Политику конфиденциальности;

- `no` (или `n`), если вы не принимаете Политику конфиденциальности.

Если вы не согласны с условиями Политики конфиденциальности, программа прерывает процесс настройки Kaspersky Endpoint Security.

Шаг 4. Участие в Kaspersky Security Network

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

Введите одно из следующих значений:

- `yes` (или `y`), если вы согласны с условиями Положения о Kaspersky Security Network; будет включен расширенный режим Kaspersky Security Network;
- `no` (или `n`), если вы не согласны с условиями Положения о Kaspersky Security Network.

Отказ от участия в Kaspersky Security Network не прерывает процесс установки Kaspersky Endpoint Security. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент (см. стр. 145).

Шаг 5. Определение типа перехватчика файловых операций

На этом этапе определяется тип перехватчика файловых операций для используемой операционной системы. Для операционных систем, не поддерживающих технологию fanotify, будет запущена компиляция модуля ядра. Модуль ядра требуется для работы задачи постоянной защиты.

Для компиляции модуля ядра требуется наличие файла System.map-<версия ядра> в директории /boot.

Если скрипт обнаруживает исходные коды модуля ядра операционной системы в директории по умолчанию, программа будет использовать путь к этой директории. В противном случае вам нужно указать путь к исходным кодам модуля ядра.

Если в процессе компиляции модуля ядра не обнаружены необходимые пакеты, Kaspersky Endpoint Security пытается скачать их самостоятельно. Если скачать пакеты не удается, выводится сообщение об ошибке.

Вы можете выполнить компиляцию модуля ядра позже, после завершения первоначальной настройки Kaspersky Endpoint Security.

Шаг 6. Настройка источников обновлений

На этом шаге вам нужно указать источники обновлений баз и модулей программы Kaspersky Endpoint Security.

Введите одно из следующих значений:

- KLServers – Kaspersky Endpoint Security получает обновления с одного из серверов обновлений "Лаборатории Касперского".
- SCServer – Kaspersky Endpoint Security загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновления, если вы используете программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации.
- <Url> – Kaspersky Endpoint Security загружает обновления из пользовательского источника. Вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.

Шаг 7. Настройка параметров прокси-сервера

На этом шаге вам нужно указать параметры прокси-сервера, если вы используете прокси-сервер для доступа в интернет. Подключение к интернету требуется для загрузки антивирусных баз Kaspersky Endpoint Security с серверов обновлений (см. стр. 34).

► *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:порт, если при подключении к прокси-серверу не требуется аутентификация;
  - имя_пользователя:пароль@IP-адрес_прокси_сервера:порт, если при подключении к прокси-серверу требуется аутентификация;
- Если при подключении к интернету вы не используете прокси-сервер, введите ответ no.

По умолчанию программа предлагает ответ no.

Вы можете настроить параметры прокси-сервера без использования скрипта первоначальной настройки.

Шаг 8. Загрузка антивирусных баз Kaspersky Endpoint Security

На этом шаге вы можете загрузить на компьютер антивирусные базы Kaspersky Endpoint Security. Антивирусные базы содержат описания сигнатур угроз и методов борьбы с ними. Kaspersky Endpoint Security использует эти записи при поиске и обезвреживании угроз. Вирусные аналитики "Лаборатории Касперского" регулярно пополняют записи о новых угрозах.

Чтобы загрузить антивирусные базы Kaspersky Endpoint Security на компьютер, вам нужно ввести ответ yes.

Введите no, если вы хотите отказаться от немедленной загрузки антивирусных баз.

По умолчанию предлагается ответ yes.

Программа будет обеспечивать антивирусную защиту компьютера только после загрузки антивирусных баз Kaspersky Endpoint Security.

Задачу обновления можно запустить без использования скрипта первоначальной настройки.

Шаг 9. Включение автоматического обновления антивирусных баз

На этом шаге вы можете включить автоматическое обновление антивирусных баз.

Введите ответ `yes`, чтобы включить автоматическое обновление антивирусных баз. По умолчанию Kaspersky Endpoint Security проверяет наличие обновлений для антивирусных баз каждые 60 минут. Если обновления есть, Kaspersky Endpoint Security загружает обновленные антивирусные базы.

Введите ответ `no`, если вы не хотите, чтобы Kaspersky Endpoint Security автоматически обновлял антивирусные базы.

Вы можете включить автоматическое обновление антивирусных баз без помощи скрипта первоначальной настройки путем управления расписанием задачи обновления (см. стр 72).

Шаг 10. Активация программы

На этом шаге вам нужно активировать программу с помощью кода активации или файла ключа.

Чтобы активировать программу с помощью кода активации, вам нужно ввести код активации.

Чтобы активировать программу с помощью файла ключа, вам нужно указать полный путь к файлу ключа.

Если код активации или файл ключа не указаны, программа будет активирована с помощью пробного ключа на один месяц.

Вы можете установить файл ключа без использования скрипта первоначальной настройки.

Шаг 11. Настройка графического пользовательского интерфейса

На этом шаге можно включить использование графического пользовательского интерфейса (GUI).

Введите одно из следующих значений:

- `yes` (или `y`), если вы хотите включить использование графического пользовательского интерфейса. Kaspersky Endpoint Security проверит наличие всех нужных библиотек и при необходимости попробует установить отсутствующие.
- `no` (или `n`), если вы не хотите включать использование графического пользовательского интерфейса.

Вы можете включить или выключить использование графического пользовательского интерфейса в любой момент (см. стр. 171).

Автоматический режим первоначальной настройки Kaspersky Endpoint Security

Вы можете выполнить первоначальную настройку Kaspersky Endpoint Security в автоматическом режиме. Программа установит значения параметров, указанные в конфигурационном файле первоначальной настройки.

► *Чтобы запустить первоначальную настройку Kaspersky Endpoint Security в автоматическом режиме, выполните следующую команду:*

```
kesl-setup.pl --autoinstall=<полный путь к конфигурационному файлу
превоначальной настройки>
```

Параметры конфигурационного файла первоначальной настройки Kaspersky Endpoint Security

Конфигурационный файл первоначальной настройки Kaspersky Endpoint Security содержит параметры, приведенные в таблице ниже.

Таблица 2. Параметры конфигурационного файла первоначальной настройки

Параметр	Описание	Возможные значения
EULA_AGREED	Обязательный параметр Согласие с условиями Лицензионного соглашения	`yes` – согласие с условиями Лицензионного соглашения необходимо для продолжения процедуры установки программы; `no` – не принимать Лицензионное соглашение. Установка программы будет прервана.
PRIVACY_POLICY_AGREED	Обязательный параметр Принятие Политики конфиденциальности	`yes` – принять Политику конфиденциальности, чтобы продолжить процедуру установки программы; `no` – не принимать Политику конфиденциальности. Установка программы будет прервана.
USE_KSN	Согласие с Положением о Kaspersky Security Network	`yes` – принять Положение о Kaspersky Security Network; `no` – не принимать Положение о Kaspersky Security Network. Для сохранения сертифицированной конфигурации программы допустимо использование исключительно Локального KSN (KPSN). В противном случае использование KSN должно быть отключено.

Параметр	Описание	Возможные значения
LOCALE	Дополнительный параметр Языковой стандарт, используемый при работе Kaspersky Endpoint Security	Языковой стандарт в формате, определенном в RFC 3066. Если параметр `LOCALE` не указан, устанавливается языковой стандарт системы по умолчанию.
INSTALL_LICENSE	Код активации или файл ключа	Нет значения
UPDATER_SOURCE	Источник обновлений	• `SCServer` – использовать в качестве источника обновлений Сервер администрирования Kaspersky Security Center; • `KLServers` – использовать в качестве источника обновлений серверы "Лаборатории Касперского"; • адрес источника обновлений.
PROXY_SERVER	Адрес прокси-сервера, используемого для подключения к интернету	• адрес прокси-сервера; • `no` – не использовать прокси-сервер.
UPDATE_EXECUTE	Запуск задачи обновления баз во время процедуры настройки	• `yes` – запускать задачу обновления; • `no` – не запускать задачу обновления.
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра	• `yes` – компилировать модуль ядра; • `no` – не компилировать модуль ядра.

Параметр	Описание	Возможные значения
USE_GUI	Включение использования графического пользовательского интерфейса	• `yes` – включить использование графического пользовательского интерфейса; • `no` – выключить использование графического пользовательского интерфейса. Чтобы изменения значений параметров вступили в силу, требуется перезапуск программы. Для сохранения сертифицированной конфигурации программы использование графического пользовательского интерфейса должно быть отключено.
IMPORT_SETTINGS	Использование параметров программы из конфигурационного файла	• `yes` – использовать параметры программы из конфигурационного файла; • `no` – не использовать параметры программы из конфигурационного файла.
ScanMemoryLimit	Дополнительный параметр Ограничение на использование памяти программой Kaspersky Endpoint Security во время выполнения задач антивирусной проверки (для типов ODS и OAS), в МБ	• Минимальное значение – 2048. • Значение по умолчанию: 8192. Если указанное значение меньше 2048, будет использоваться минимальное значение (2048). Если указанное значение превышает размер оперативной памяти, будет использоваться до 40% оперативной памяти. Это процентное значение нельзя изменить. Чтобы изменения значений параметров вступили в силу, требуется перезапуск программы.

Если вы хотите изменить параметры в конфигурационном файле первоначальной настройки Kaspersky Endpoint Security, вводите значения параметров в формате `имя параметра=значение_параметра` (программа не обрабатывает пробелы между именем параметра и его значением).

Начальная настройка параметров Агента администрирования

Если вы планируете управлять Kaspersky Endpoint Security с помощью Kaspersky Security Center, вам нужно настроить параметры Агента администрирования.

► *Чтобы настроить параметры Агента администрирования, выполните следующие действия:*

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. Укажите DNS-имя или IP-адрес Сервера администрирования.
3. Укажите номер порта Сервера администрирования.

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

   По умолчанию используется порт 13000.
5. Выполните одно из следующих действий:
   - Введите `yes`, если вы хотите использовать SSL-соединение.
   - Введите `no`, если вы не хотите использовать SSL-соединение.

   По умолчанию SSL-соединение включено.
6. При необходимости укажите режим шлюза для соединения:
   - `0` – не использовать шлюз для соединения;
   - `1` – использовать Агент администрирования в качестве шлюза для соединения;
   - `2` – подключаться к Серверу администрирования через шлюз для соединения.

Для получения подробной информации о настройке Агента администрирования обратитесь к документации Kaspersky Security Center.

Настройка разрешающих правил в системе SELinux

► *Чтобы создать модуль SELinux с правилами, необходимыми для работы Kaspersky Endpoint Security, выполните следующие действия:*

1. Переведите SELinux в разрешающий 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. Запустите следующие задачи:
   - задачу Защита от файловых угроз:

     ```
     kesl-control --start-t 1
     ```

   - задачу проверки загрузочных секторов:

     ```
     kesl-control --start-t 4 -W
     ```

   - задачу проверки памяти процессов:

     ```
     kesl-control --start-t 5 -W
     ```

3. Создайте модуль правил на основе блокирующих записей:

   ```
   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   ```

   Убедитесь, что созданный список содержит только правила, относящиеся к Kaspersky Endpoint Security.

4. Загрузите полученный модуль правил:

   ```
   # semodule -i kesl.pp
   ```

5. Переведите SELinux в принудительный режим:

   ```
   # setenforce Enforcing
   ```

В случае появления новых audit-сообщений, связанных с Kaspersky Endpoint Security, следует обновлять файл модуля правил.

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

Настройка разрешающих правил в системе AppArmor

► *Чтобы обновить профили AppArmor, необходимые для работы Kaspersky Endpoint Security, выполните следующие действия:*

1. Убедитесь, что модуль AppArmor загружен с помощью одной из следующих команд командной строки:

- `systemctl status apparmor`
- `/etc/init.d/apparmor status`

2. Создайте профиль Kaspersky Endpoint Security:
   a. В первой консоли выполните команды:

      ```
      cd /etc/apparmor.d
      aa-genprof /opt/kaspersky/kesl/libexec/kesl
      ```

   b. Чтобы создать полный профиль, рекомендуется выполнить все операции, которые вы планируете выполнять при использовании Kaspersky Endpoint Security. Например, запускать задачи на второй консоли:
      - задачу Защита от файловых угроз:

        ```
        kesl-control --start-t 1
        ```

      - задачу проверки загрузочных секторов:

        ```
        kesl-control --start-t 4 -W
        ```

      - задачу проверки памяти процессов:

        ```
        kesl-control --start-t 5 -W
        ```

      - задачу обновления:

        ```
        kesl-control --start-t 6 -W
        ```

   c. В первой консоли нажмите **S**. После завершения сканирования событий нажмите **F**.

      После этого будет сформирован профиль Kaspersky Endpoint Security для системы AppArmor в директории /etc/apparmor.d/. Имя файла профиля является уникальным для каждой установки (например, `var.opt.kaspersky.kesl.10.1.1.5960_1537783807.opt.kaspersky.kesl.libexec.kesl`).

      Созданные профиль можно определить вручную или с помощью команды:

      ```
      basename /etc/apparmor.d/*kesl*
      ```

3. Переведите созданный профиль Kaspersky Endpoint Security в режим показа сообщений:

   ```
   aa-complain <имя файла профиля Kaspersky Endpoint Security>
   ```

4. Через несколько дней работы программы обновите профиль, запустив команду:

   ```
   aa-logprof
   ```

   Укажите разрешения `Allow` или `Glob` на все файлы, которые Kaspersky Endpoint Security использовал в течение этого периода.

5. Переведите профиль Kaspersky Endpoint Security в блокирующий режим:

   ```
   aa-enforce <имя файла профиля Kaspersky Endpoint Security>
   ```

В случае появления новых audit-сообщений, связанных с Kaspersky Endpoint Security, следует обновлять файл модуля правил.

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

Сертифицированное состояние программы

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

- Программа установлена на компьютере (см. раздел "Установка программы").
- Проведена первоначальная настройка параметров программы (см. раздел "О первоначальной настройке параметров Kaspersky Endpoint Security").
- Антивирусные базы обновлены (см. раздел "Задача обновления (Update ID:6)").
- Настроена и запущена задача постоянной защиты (см. раздел "Задача постоянной защиты (File_Monitoring ID:1)").
- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к данному документу (см. раздел "Значения параметров программы в сертифицированном состоянии").

Проверка работоспособности. EICAR

Чтобы проверить работоспособность программы, вы можете использовать тестовый вирус Eicar. Тестовый вирус предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

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

Файл, который содержит тестовый вирус, называется eicar.com. Вы можете загрузить его со страницы сайта **EICAR** http://www.eicar.org/anti_virus_test_file.htm.

Перед сохранением файла в директории на диске компьютера убедитесь, что постоянная защита файлов в этой директории отключена.

Перед началом проверки убедитесь, что выполнены следующие условия:

- Программа готова к работе (см. раздел "Подготовка программы к работе").
- Программа находится в сертифицированном состоянии (см. раздел "Сертифицированное состояние программы").

Проверка работоспособности программы

1. Установите программу (см. раздел "Установка пакета Kaspersky Endpoint Security").

2. Выполните первоначальную настройку программы (см. раздел "О первоначальной настройке Kaspersky Endpoint Security").

3. Убедитесь, что программа активирована и антивирусные базы обновлены, выполнив команду:

   ```
   kesl-control --app-info
   ```

   Ожидаемый результат: программа выводит на экран следующую информацию:

   ```
   Key status : Valid
   Anti-virus databases loaded : Yes
   Protection status : OAS enabled
   ```

4. Убедитесь, что задача постоянной защиты (*File_Monitoring*) запущена, выполнив команду:

   ```
   kesl-control --get-task-list
   ```

   Ожидаемый результат: задача *File_Monitoring* присутствует в списке задач, статус задачи `Started`.

5. Остановите задачу постоянной защиты (*File_Monitoring*), выполнив следующую команду:

   ```
   kesl-control --stop-task File_Monitoring
   ```

6. Скачайте EICAR-файл сайте http://www.eicar.org/anti_virus_test_file.htm в разделе **Download**.

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

7. Запустите задачу постоянной защиты (*File_Monitoring*), выполнив следующую команду:

   ```
   kesl-control --start-task File_Monitoring
   ```

8. Попытайтесь открыть файл eicar.com, выполнив следующую команду:

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

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

9. Убедитесь, что заражённый файл был удален из директории компьютера.

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

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

Разделение доступа к функциям программы по пользовательским ролям

Доступ к функциям программы Kaspersky Endpoint Security предоставляется пользователю в соответствии с его ролью. Существуют две роли: *Администратор* и *Пользователь*.

После установки программы роль Администратора выдается только root-пользователю. Администратор имеет доступ ко всем функциям программы.

Для пользователей, которые не обладают правами роли "Администратор", доступ к функциям программы Kaspersky Endpoint Security ограничен или запрещен.

Роль пользователя позволяет:

- Управлять временными задачами выборочной проверки (Scan_File) и запускать или останавливать задачу обновления (Update).
- Просматривать в списке запущенных задач только собственные задачи Scan_File_xxx и задачи обновления.
- Просматривать отчеты только по собственным задачам.
- Просматривать события, которые являются общими для всех пользователей Kaspersky Endpoint Security.
- Иметь доступ только к тем файлам, к которым разрешен доступ конкретному пользователю.

Роль пользователя не позволяет:

- Управлять параметрами и задачами программы.
- Применять к Хранилищу какие-либо действия.
- Управлять лицензированием программы.
- Запускать локально графический пользовательский интерфейс, если в конфигурационном файле первоначальной настройки Kaspersky Endpoint Security указано `UseGUI=no`.

Лицензирование программы

В этом разделе описаны основные аспекты лицензирования программы.

В этой главе

О лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Endpoint Security.
- Прочитав файл license.<ID языка>. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на условиях Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок действия зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

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

  У пробной лицензии обычно короткий срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Security прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать программу по пробной лицензии только один раз.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы.

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Endpoint Security). Чтобы продолжить использование Kaspersky Endpoint Security в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от всех 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:

- номер заказа;
- информация о пользователе, которому предоставлена лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение количества лицензионных единиц (например, устройств, на которых можно использовать программу с предоставленной лицензией);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или условия лицензии;
- тип лицензии.

О ключе

Ключ – последовательность битов, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Ключи генерируют специалисты "Лаборатории Касперского".

Вы можете добавить ключ в программу одним из следующих способов: применить *файл ключа* или ввести *код активации*. После добавления в программу ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности.

Ключ может быть заблокирован "Лабораторией Касперского" в случае нарушения условий Лицензионного соглашения. Если ключ был заблокирован, вам понадобится добавить другой ключ, если вы хотите использовать программу.

Ключ может быть активным и дополнительным.

Активный ключ – ключ, используемый в текущий момент для работы программы. Активный ключ можно добавить для пробной или коммерческой лицензии. В программе не может быть больше одного активного ключа.

Дополнительный ключ – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом. Дополнительный ключ может быть добавлен только после добавления активного ключа.

В качестве активного может быть добавлен ключ для пробной лицензии. Ключ для пробной лицензии не может быть добавлен в качестве дополнительного ключа.

О коде активации

Код активации – уникальная последовательность из 20 букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Endpoint Security. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Security или после заказа пробной версии Kaspersky Endpoint Security.

Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если вы потеряли код активации после установки программы, его можно восстановить. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации необходимо связаться со Службой технической поддержки "Лаборатории Касперского".

Использование кода активации для добавления ключа в хранилище ключей Kaspersky Security Center может привести к выходу программы из сертифицированного состояния.

О файле ключа

Файл ключа – это файл с расширением .key, который вам предоставляет "Лаборатория Касперского". Файлы ключей предназначены для активации программы путем добавления ключа.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Security или после заказа пробной версии Kaspersky Endpoint Security.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" (https://keyfile.kaspersky.com/ru/) на основе имеющегося кода активации.

О подписке

Подписка на Kaspersky Endpoint Security – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Endpoint Security можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме или отказаться от нее. Управление подпиской доступно на веб-сайте поставщика услуг.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Endpoint Security после окончания ограниченной подписки ее требуется продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность программы сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Endpoint Security по подписке, требуется применить код активации, предоставленный поставщиком услуг. После применения кода активации устанавливается активный ключ. Активный ключ определяет лицензию для использования программы по подписке. При этом дополнительный ключ может быть установлен только с помощью кода активации и не может быть установлен с помощью файла ключа или по подписке.

Функциональность программы, доступная по подписке, может соответствовать функциональности программы для следующих видов коммерческой лицензии: Стандартная, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Лицензии этих видов предназначены для защиты файловых серверов, рабочих станций и мобильных устройств и позволяют использовать компоненты контроля на рабочих станциях и мобильных устройствах.

В зависимости от поставщика услуг, набор возможных действий для управления подпиской может различаться. Поставщик услуг может не предоставлять льготный период для продления подписки, в течение которого функциональность программы сохраняется.
Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Endpoint Security.

О предоставлении данных

Принимая условия Лицензионного соглашения, вы соглашаетесь передавать в автоматическом режиме информацию об используемой программе, а также тип, версию и языковую локализацию установленной программы, уникальный идентификатор установки программы и тип установки, данные об активном и дополнительном ключах (включая тип лицензии, срок действия, дату активации программы и дату окончания

срока действия лицензии, ключ, текущий статус лицензионного ключа, версию протокола взаимодействия с сервером активации).

Также, принимая условия Положения о Kaspersky Security Network, вы соглашаетесь передавать в автоматическом режиме следующую информацию об участии в Kaspersky Security Network:

- идентификатор и версию Положения о Kaspersky Security Network, принятого или отклоненного пользователем;
- информацию о принятии/отклонении Положения о Kaspersky Security Network;
- дату и время принятия/отклонения Положения о Kaspersky Security Network;
- информацию о выборе варианта KSN без отправки статистических данных;
- информацию о выборе варианта KSN с отправкой статистических данных;
- уникальные идентификаторы персонального компьютера и пользователя, полную версию и тип программы.

В случае активации программы с помощью кода активации, для целей получения статистической информации о распространении и использовании программ Правообладателя вы соглашаетесь предоставлять в автоматическом режиме версию используемой программы (в том числе информацию об установленных обновлениях программы, идентификаторе установки программы, информацию об используемой лицензии), версию операционной системы, идентификаторы компонентов программы, активных на момент предоставления информации.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского".

"Лаборатория Касперского" использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных и иных конфиденциальных данных. Исходная полученная информация уничтожается по мере накопления (один раз в год). Данные общей статистики хранятся бессрочно.

Более подробную информацию о получении, обработке, хранении и уничтожении информации об использовании программы после принятия Лицензионного соглашения и согласия с Положением о Kaspersky Security Network вы можете узнать, прочитав тексты этих документов, а также на веб-сайте "Лаборатории Касперского". Файлы license.<ID языка> и ksn_license.<ID языка> с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки программы.

Запуск и остановка программы

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

Если вы остановите Kaspersky Endpoint Security, все выполняющиеся задачи будут прерваны. После повторного запуска Kaspersky Endpoint Security прерванные пользовательские задачи не будут автоматически возобновлены. Только те пользовательские задачи, в параметрах расписания которых задан режим запуска `PS`, будут запущены снова.

- *Чтобы запустить Kaspersky Endpoint Security, выполните следующую команду:*

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

- *Чтобы остановить Kaspersky Endpoint Security, выполните следующую команду:*

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

- *Чтобы перезапустить Kaspersky Endpoint Security, выполните следующую команду:*

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

- *Чтобы вывести статус Kaspersky Endpoint Security, выполните следующую команду:*

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

- *Чтобы запустить Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

  ```
  systemctl start kesl-supervisor
  ```

- *Чтобы остановить Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

  ```
  systemctl stop kesl-supervisor
  ```

- *Чтобы перезапустить Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

  ```
  systemctl restart kesl-supervisor
  ```

- *Чтобы вывести статус Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

  ```
  systemctl status kesl-supervisor
  ```

Мониторинг состояния программы

Мониторинг состояния программы выполняет контрольная служба. Контрольная служба автоматически запускается при запуске программы.

В случае сбоя программы генерируется файл дампа, и программа автоматически перезапускается. Создается резервная копия директории /var/opt/kaspersky/kesl за исключением файлов дампа.

Общие параметры Kaspersky Endpoint Security

В этом разделе описаны общие параметры Kaspersky Endpoint Security.

Общие параметры конфигурационного файла имеют следующие значения:

SambaConfigPath

Директория, в которой хранится конфигурационный файл Samba. Конфигурационный файл Samba нужен для обеспечения работы значений `AllShared` или `Shared:SMB` для опции `Path`.

По умолчанию указана стандартная директория конфигурационного файла Samba на компьютере.

После изменения значения этого параметра требуется перезапуск программы.

Значение по умолчанию: `/etc/samba/smb.conf`

NfsExportPath

Директория, в которой хранится конфигурационный файл NFS. Конфигурационный файл NFS нужен для обеспечения работы значений `AllShared` или `Shared:NFS` для опции `Path`.

По умолчанию указана стандартная директория конфигурационного файла NFS на компьютере.

После изменения значения этого параметра требуется перезапуск программы.

Значение по умолчанию: `/etc/exports`

TraceFolder

Директория, в которой хранятся файлы трассировки программы.

Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, с правами которой работает Kaspersky Endpoint Security.

После изменения значения этого параметра требуется перезапуск программы.

Значение по умолчанию: `/var/log/kaspersky/kesl`

TraceLevel

Уровень детализации журнала трассировки.

Доступные значения:

`Detailed` – наиболее детализированный журнал трассировки.

`NotDetailed` – журнал трассировки содержит оповещения об ошибках.

`None` – не создает журнал трассировки.

Значение по умолчанию: `None`.

TraceMaxFileCount

Максимальное количество файлов трассировки программы.

Файлы трассировки для текущего и для завершенных процессов трассировки считаются отдельно. Например, если для параметра `TraceMaxFileCount` указано значение 2, то максимально может

храниться 4 файла трассировки: два файла для текущего процесса трассировки и два файла для завершенных процессов.

После изменения значения этого параметра требуется перезапуск программы.

Доступные значения: `1 – 99`.

Значение по умолчанию: `2`.

TraceMaxFileSize

Максимальный размер файла трассировки программы (в мегабайтах).

После изменения значения этого параметра требуется перезапуск программы.

Доступные значения: `1 – 1000`.

Значение по умолчанию: `250`.

BlockFilesGreaterMaxFileNamePath

Блокирование 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 антивирусной проверки пропускают такой файл при проверке.

Этот параметр недоступен для операционных систем, в которых используется технологи fanotify.

Доступные значения: `4096 – 33554432`.

Значение по умолчанию: `16384`.

DetectOtherObjects

Включает или выключает обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Доступные значения:

`Yes`. Включить обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

`No`. Выключить обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Значение по умолчанию: `No`.

UseKSN

Включает или выключает участие в Kaspersky Security Network.

Доступные значения:

`No`. Выключить участие в Kaspersky Security Network.

`Basic`. Включить участие в Kaspersky Security Network без отправки статистики.

`Extended`. Включить участие в Kaspersky Security Network с отправкой статистики.

Значение по умолчанию: `No`.

UseProxy

Включает или выключает использование прокси для Kaspersky Security Network, активации программы и обновлений.

Доступные значения:

`Yes`. Включить использование прокси.

`No`. Выключить использование прокси.

Значение по умолчанию: `No`.

ProxyServer

Параметры прокси-сервера в формате `[пользователь[:пароль]@]узел[:порт]`.

MaxEventsNumber

Максимальное количество событий, которые будет хранить Kaspersky Endpoint Security. При превышении заданного количества событий Kaspersky Endpoint Security удаляет наиболее давние события.

Значение по умолчанию: `500000`.

LimitNumberOfScanFileTasks

Максимальное количество задач типа `Scan_File`, которые непривилегированный пользователь может запустить на компьютере одновременно. Этот параметр не ограничивает количество задач, которые запускает пользователь с root-правами. Если задано значение `0`, непривилегированный пользователь не может запускать задачи типа `Scan_File`.

Доступные значения: `0 – 4294967295`.

Значение по умолчанию: `0`.

Если во время установки программы для параметра `USE_GUI` установлено значение `yes`, для параметра `LimitNumberOfScanFileTasks` по умолчанию используется значение `5`.

UseSysLog

Включает или выключает запись информации о событиях в syslog. В некоторых случаях программа не может создать и сохранить событие. В этом случае информация сохраняется в syslog.

Доступные значения:

`Yes`. Включить запись информации о событиях в syslog.

`No`. Выключить запись информации о событиях в syslog.

Значение по умолчанию: `No`.

UIReportsForRootOnly

Включает или выключает просмотр отчетов для пользователей из графического пользовательского интерфейса.

Для сохранения сертифицированной конфигурации программы значение параметра `UIReportsForRootOnly` должно быть `Yes`.

Доступные значения:

`Yes`. Разрешить просмотр отчетов из графического пользовательского интерфейса только пользователю с root-правами.

`No`. Разрешить просмотр отчетов из графического пользовательского интерфейса непривилегированным пользователям. Непривилегированные пользователи также смогут создавать и запускать до 5 пользовательских задач проверки.

Значение по умолчанию: `No`

EventsStoragePath

Файл базы данных, в которой Kaspersky Endpoint Security сохраняет информацию о событиях.

Значение по умолчанию: `/var/opt/kaspersky/kesl/events.db`.

ExcludedMountPoint

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

Доступные значения:

`AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`Mounted:NFS` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протокола NFS;

`Mounted:SMB` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протокола NFS;

`/Mnt` – исключать из проверки объекты, находящиеся в директории `/mnt` (включая вложенные директории), используемой в качестве временной точки монтирования съемных дисков;

`<путь с применением маски /mnt/user* или /mnt/**/user_share>` – исключать из проверки объекты, находящиеся в директориях, имена которых содержат указанную маску.

Можно использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включая символ /. Например, /dir/**/file*/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

Точки монтирования необходимо указывать точно так же, как они отображаются в выходных данных команды `mount`.

Параметр `ExcludedMountPoint` не указан по умолчанию.

В этой главе

Команды управления параметрами Kaspersky Endpoint Security и задачами

Этот раздел содержит информацию о командах управления параметрами Kaspersky Endpoint Security и задачами.

Получение общих параметров Kaspersky Endpoint Security

Команда `kesl-control --get-app-settings` выводит общие параметры Kaspersky Endpoint Security. Используя эту команду, вы также можете получить общие параметры Kaspersky Endpoint Security, заданные с помощью ключей команды.

Вы можете использовать эту команду для изменения общих параметров Kaspersky Endpoint Security, установленного на компьютере:

1. Сохраните общие параметры Kaspersky Endpoint Security в конфигурационном файле с помощью команды `--get-app-settings`.
2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `--set-app-settings`. Kaspersky Endpoint Security применит новые значения параметров после того, как вы остановите и снова запустите Kaspersky Endpoint Security.

Вы можете использовать созданный конфигурационный файл для импорта параметров в Kaspersky Endpoint Security, установленный на другом компьютере.

Синтаксис команды

```
kesl-control [-T] --get-app-settings [--file <имя конфигурационного файла>]
kesl-control [-T] --get-app-settings
```

Аргументы и ключи

`--file <имя конфигурационного файла>`

Имя конфигурационного файла, в котором будут сохранены параметры Kaspersky Endpoint Security. 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.

Пример:

Экспортировать общие параметры Kaspersky Endpoint Security в файл с именем kesl_config.ini. Сохранить созданный файл в текущей директории:

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

Изменение общих параметров Kaspersky Endpoint Security

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

Для изменения параметров программы необходимо наличие root-прав.

Вы можете использовать эту команду для изменения общих параметров Kaspersky Endpoint Security:

1. Сохраните общие параметры Kaspersky Endpoint Security в конфигурационном файле с помощью команды `--get-app-settings`.
2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды --set-app-settings. Kaspersky Endpoint Security применит новые значения параметров после того, как вы остановите и снова запустите Kaspersky Endpoint Security с помощью команд `--stop-app` и `--start-app` или с помощью команды `--restart-app`.

Синтаксис команды

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

Аргументы и ключи

`--file <имя конфигурационного файла>`

Имя конфигурационного файла, параметры из которого будут импортированы в Kaspersky Endpoint Security; включает полный путь к файлу.

Примеры:

Импортировать в Kaspersky Endpoint Security общие параметры из конфигурационного файла с именем /home/test/kav_config.ini:

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

Установить низкий уровень детализации журнала 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"
```

Вывод справки о командах Kaspersky Endpoint Security

Команда `kesl-control` с ключом `--help <набор команд Kaspersky Endpoint Security>` выводит справку о командах Kaspersky Endpoint Security.

Синтаксис команды

```
kesl-control --help [<набор команд Kaspersky Endpoint Security>]
```

<набор команд Kaspersky Endpoint Security>

Доступные значения:

`[-T]` – команды управления задачами и общими параметрами Kaspersky Endpoint Security;

`[-L]` – команды управления ключами;

`[-B]` – команды управления Хранилищем;

`[-E]` – команды управления событиями Kaspersky Endpoint Security.

`[-F]` – команды для управления задачей Управление сетевым экраном.

`[-H]` – команды для управления задачей Защита от шифрования.

`[-S]` – команды для управления статистикой.

`-W` – мониторинг событий.

Включение вывода событий

Команда `kesl-control-W` включает режим вывода событий Kaspersky Endpoint Security. Вы можете использовать эту команду либо отдельно, чтобы отобразить все события Kaspersky Endpoint Security, либо вместе с командой `kesl-control --start-task`, чтобы отобразить только события, связанные с текущей задачей. Вы можете использовать `--query` с флагом `-W` для вывода только определенных событий.

Команда возвращает название события и дополнительную информацию о событии.

Синтаксис команды

```
kesl-control -W
```

Пример:

Включить режим вывода событий Kaspersky Endpoint Security:

```
kesl-control -W
```

Просмотр информации о программе

Команда `kesl-control --app-info` выводит информацию о Kaspersky Endpoint Security.

Синтаксис команды

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

Результат выполнения команды

Name

Название программы.

Version

Текущая версия программы.

Key status

Статус ключа.

Subscription status

Статус подписки. Это поле отображается, если программа используется по подписке.

License expiration date

Дата окончания срока действия лицензии.

Storage state

Состояние Хранилища. Отображает информацию об ограничениях времени и размера.

Storage space usage

Размер Хранилища.

Last run date of the Scan_My_Computer task

Время последнего запуска задачи Scan_My_Computer.

Last release date of databases

Время последнего выпуска баз.

Anti-virus databases loaded

Отображает, загружены ли антивирусные базы.

Anti-virus databases records

Количество записей в антивирусных базах.

KSN state

Состояние участия в Kaspersky Security Network.

File monitoring

Состояние компонента Мониторинг файлов.

Integrity monitoring

Состояние компонента Мониторинг файловых операций.

Firewall

Состояние компонента Управление сетевым экраном.

Anti-Cryptor

Состояние компонента Защита от шифрования.

Application update state

Отображает наличие обновлений программы.

Команды Kaspersky Endpoint Security

Вы можете менять значения параметров Kaspersky Endpoint Security.

Ниже приведены правила использования команд Kaspersky Endpoint Security.

- Соблюдайте регистр.
- Разделяйте ключи символом "пробел".
- Используя полное название команды или ключа, вводите значение через символ "равно" (=).

Пример:

Указать значение параметра URL для пользовательского источника обновлений для задачи обновления (ID=6) из командной строки:

```
kesl-control --set-settings 6

SourceType=Custom CustomSources.item_0000.URL=http://site.domain/path
CustomSources.item_0000.Enabled=Yes
```

Вывод справки о командах Kaspersky Endpoint Security

`--help`

Выводит справку о командах Kaspersky Endpoint Security.

Вывод событий Kaspersky Endpoint Security

`-W`

Включает вывод событий Kaspersky Endpoint Security.

Команды управления параметрами Kaspersky Endpoint Security и задачами

`-T`

Префикс; указывает на то, что команда принадлежит к группе команд управления параметрами Kaspersky Endpoint Security / управления задачами (необязательный).

`[-S] --app-info`

Выводит общую информацию о Kaspersky Endpoint Security.

`[-T] --get-app-settings --file <имя и директория файла>`

Возвращает общие параметры Kaspersky Endpoint Security.

`[-T] --set-app-settings --file <имя и директория файла>`

Устанавливает общие параметры Kaspersky Endpoint Security.

`[-T] --get-task-list`

Возвращает список существующих задач Kaspersky Endpoint Security.

`[-T] --get-task-state <ID задачи>|<имя задачи>`

Выводит состояние указанной задачи.

`[-T] --create-task <имя задачи> --type <тип задачи> --file <имя и директория файла>`

Создает задачу указанного типа; импортирует в задачу параметры из указанного конфигурационного файла.

`[-T] --delete-task <ID задачи>|<имя задачи>`

Удаляет задачу.

`[-T] --start-task <ID задачи>|<имя задачи> [-W] [--progress] [--file <имя и директория файла>]`

Запускает задачу.

`[-T] --stop-task <ID задачи>|<имя задачи>`

Останавливает задачу.

`[-T] --suspend-task <ID задачи>|<имя задачи>`

Приостанавливает задачу.

`[-T] --resume-task <ID задачи>|<имя задачи>`

Возобновляет задачу.

`[-T] --get-settings <ID задачи>|<имя задачи> --file <имя и директория файла>`

Выводит параметры задачи.

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

Устанавливает параметры задачи.

`[-T] --scan-file <путь> [--action <действие>]`

Создает и запускает временную задачу `Scan_File`.

`[-T] --import-settings <--file файл>`

Импортирует параметры программы в конфигурационный файл.

`[-T] --update-application`

Обновляет программу.

`[-S] --omsinfo --file <путь>`

Создает файл в формате JSON для интеграции с Microsoft Operations Management Suite.

Команды управления ключами

`-L`

Префикс; указывает на то, что команда принадлежит к группе команд управления ключами.

`[-L] --install-active-key <код активации>|<файл ключа>`

Добавляет активный ключ.

`[-L] --install-additional-key <код активации>|<файл ключа>`

Добавляет дополнительный ключ.

`[-L] --revoke-active-key`

Удаляет активный ключ.

`[-L] --revoke-additional-key`

Удаляет дополнительный ключ.

`[-L] --query`

Выводит информацию о ключе.

Команды для задачи Управление сетевым экраном

`[-F] --add-rule [--name <строка>] [--action <действие>] [--protocol <протокол>] [--direction <директория>] [--remote <удаленная>] [--local <локальная>] [--at <индекс>]`

Добавляет новое правило.

`[-F] --del-rule [--name <строка>] [--index <индекс>]`

Удаляет правило.

`[-F] --move-rule [--name <строка>] [--index <индекс>] [--at <индекс>]`

Изменяет приоритетность правила.

`[-F] --add-zone [--zone <зона>] [--address <адрес>]`

Добавляет в зону IP-адрес.

`[-F] --del-zone [--zone <зона>] [--address <адрес>] [--index <индекс>]`

Удаляет из зоны IP-адрес.

`-F --query`

Отображает информацию.

Команды для задачи Защита от шифрования

`[-H] --get-blocked-hosts`

Отображает список заблокированных компьютеров.

`[-H] --allow-hosts`

Разблокирует недоверенные компьютеры.

Команды управления Хранилищем

`-B`

Префикс; указывает на то, что команда принадлежит к группе команд управления Хранилищем.

`[-B] --mass-remove --query`

Очищает Хранилище, полностью или выборочно.

`[-B] --query --limit --offset`

Выводит информацию об объектах в Хранилище.

`--limit`

Максимальное количество объектов, о которых выводится информация.

`--offset`

Количество записей, на которое следует отступить от начала выборки.

`[-B] --restore <ID объекта> --file <имя и директория файла>`

Восстанавливает объект из Хранилища.

Команды управления журналом событий

`-E`

Префикс; указывает на то, что команда принадлежит к группе команд управления журналом событий.

`[-E] --query --limit --offset --file <имя и директория файла> --db <файл БД>`

Максимальное количество событий, о которых выводится информация.

`--query`

Выводит информацию о событиях по фильтру из журнала событий или указанного файла ротации.

`--offset`

Количество записей, на которое следует отступить от начала выборки.

`--db`

Имя файла базы данных.

Команды управления расписанием задач

`[-T] --set-schedule <ID задачи>|<имя задачи> --file <имя и директория файла>`

Устанавливает параметры расписания задачи / импортирует их в задачу из конфигурационного файла.

`[-T] --get-schedule <ID задачи>|<имя задачи> --file <имя и директория файла>`

Выводит параметры расписания задачи.

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

Расписание запуска задачи.

`PS` – запускать задачу после запуска Kaspersky Endpoint Security.

`BR` – запускать задачу после обновления антивирусных баз.

`StartTime=[year/month/month_day] [hh]:[mm]:[ss]; [<month_day>|<week_day>]; [<period>]`

Время запуска задачи.

`RandomInterval=<мин.>`

Интервал запуска задачи, если несколько задач запущены одновременно (в минутах).

`ExecuteTimeLimit=<мин.>`

Ограничение времени выполнения задачи (в минутах).

`RunMissedStartRules`

Включает или выключает запуск пропущенной задачи после запуска Kaspersky Endpoint Security.

Экспорт и импорт параметров программы

Kaspersky Endpoint Security позволяет вам импортировать и экспортировать все параметры программы для диагностики сбоев, проверки параметров или для упрощения настройки программы на компьютерах.

При *экспорте* параметров все параметры программы и задач сохраняются в конфигурационном файле. Этот конфигурационный файл используется, чтобы *импортировать* параметры для настройки программы.

Во время импорта или экспорта параметров Kaspersky Endpoint Security должен быть запущен. После импорта параметров программу необходимо перезапустить.

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

При импорте или экспорте параметров из более старой версии программы для новых параметров устанавливаются значения по умолчанию. При сопоставлении конфигурационных файлов новой и старой версий программы будет возвращен код 1.

Импорт параметров в более старую версию программы недоступен.

При импорте настроек для параметра `UseKSN` устанавливается значение `No`. Чтобы начать или возобновить участие в Kaspersky Security Network, необходимо ввести `UseKSN=Basic` или `UseKSN=Extended` (см. стр. 144).

После импорта параметров программы внутренние идентификаторы задач могут поменяться. Для управления ими мы рекомендуем использовать имена задач.

► *Экспортируйте параметры программы в конфигурационный файл с помощью следующей команды:*

```
kesl-control --export-settings [--file <полный путь к конфигурационному файлу>]
```

► *Чтобы настроить программу с помощью параметров из конфигурационного файла (импортировать параметры), выполните следующую команду:*

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

Управление задачами Kaspersky Endpoint Security с помощью командной строки

Этот раздел содержит информацию о типах задач Kaspersky Endpoint Security и инструкции о том, как управлять задачами.

В этой главе

О задачах Kaspersky Endpoint Security

Вы можете управлять работой Kaspersky Endpoint Security с помощью задач как локально на компьютере (с помощью командной строки или конфигурационных файлов), так и централизованно через Kaspersky Security Center (см. стр. 148).

Для работы с Kaspersky Endpoint Security существует два типа задач:

- *Предустановленная задача* – задача, которая создается во время установки программы. Вы не можете создавать или удалять предустановленные задачи, но вы можете изменять параметры этих задач.
- *Пользовательская задача* – задача, которую вы можете создавать или удалять самостоятельно.

Вы можете управлять следующими задачами:

- `File_Monitoring` – задача Защита от файловых угроз (ID=1, тип – OAS);

- `Scan_My_Computer` – задача антивирусной проверки (ID=2, тип – ODS);
- `Scan_File` – пользовательская задача проверки (ID=3, тип – ODS). По умолчанию параметры этой задачи совпадают с параметрами задачи Scan_My_Computer;
- `Boot_Scan` – задача проверки загрузочных секторов (ID=4, тип – BootScan);
- `Memory_Scan` – задача проверки памяти процессов (ID=5, тип – MemoryScan);
- `Update` – задача обновления (ID=6, тип – Update);
- `Rollback` – задача отката обновлений (ID=7, тип – Rollback). В этой задаче нет параметров. Ее можно только запустить или остановить;
- `Retranslate` – задача копирования обновлений (ID=8, тип – Retranslate);
- `License` – задача, реализующая сервер лицензий (ID=9, тип – License);
- `Backup` – задача, управляющая Хранилищем (ID=10, тип – Backup);
- `Integrity_Monitoring` – задача мониторинга файловых операций (ID=11, тип – OAFIM);
- `Firewall` – задача управления сетевым экраном системы (ID=12, тип – Firewall);
- `Anti-Cryptor` – задача защиты от шифрования (ID=13, тип – AntiCryptor).

ID – номер задачи, который Kaspersky Endpoint Security присваивает задаче при ее создании.

Вы можете выполнять следующие действия над задачами:

- запускать, останавливать, приостанавливать и возобновлять выполнение задач;
- создавать и удалять задачи (только для пользовательских задач);
- изменять параметры задач.

Kaspersky Endpoint Security позволяет просматривать и изменять значения по умолчанию и значения параметров поиска опасных программ только пользователям с правами root.

Просмотр списка задач Kaspersky Endpoint Security

► *Чтобы просмотреть список задач Kaspersky Endpoint Security, выполните следующую команду:*

```
kesl-control [-T] --get-task-list
```

Список, в котором представлены задачи Kaspersky Endpoint Security.

Для каждой задачи отображается следующая информация:

- `Название`. Имя задачи.
- `ID`. Идентификатор задачи (см. стр. 65).

- `Type`. Тип задачи (см. стр. 65).
- `State`. Текущее состояние задачи.

Если пользователю запрещено просматривать и изменять параметры задачи, отображается информация о задачах Scan_File, Backup, License, File_Monitoring, Integrity_Monitor и Anti_Cryptor. Информация о других задачах недоступна.
Если ваша лицензия не покрывает функции Защита от шифрования и Мониторинг файловых операций, информация об этих задачах не отображается.

Более подробную информацию см. в разделе О задачах Kaspersky Endpoint Security (см. стр. 65).

Создание задачи

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

Задачи типов OAS, Firewall, OAFIM, License, Backup и AntiCryptor создать нельзя.

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

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

Здесь:

- `<имя задачи>` – имя, которое вы указываете для новой задачи;
- `<тип задачи>` - предустановленный тип задачи (см. стр. 65).

Задача указанного типа создается с параметрами по умолчанию.

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

```
kesl-control [-T] --create-task <имя задачи> --type <тип задачи> --file
<полный путь к конфигурационному файлу>
```

Здесь:

- `<имя задачи>` – имя, которое вы указываете для новой задачи;
- `<тип задачи>` - предустановленный тип задачи (см. стр. 65).
- `<полный путь к конфигурационному файлу>` - это полный путь к конфигурационному файлу (см. стр. 184)

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

Изменение параметров задачи с помощью конфигурационного файла

► *Чтобы изменить параметры задачи путем изменения конфигурационного файла, выполните следующие действия:*

1. Сохраните параметры задачи в конфигурационный файл:

   ```
   kesl-control --get-settings <имя задачи>|<task ID> --file <полный путь к файлу>
   ```

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 <имя задачи>|<task ID> --file <полный путь к файлу>
   ```

В результате задача выполняется с обновленными параметрами.

Изменение параметров задачи с помощью командной строки

► *Чтобы изменить параметры задачи с помощью командной строки, выполните следующие действия:*

1. Укажите нужное значение параметра:

   ```
   kesl-control --set-settings <имя или идентификатор задачи> setting=value [параметр=значение]
   ```

   Kaspersky Endpoint Security изменит указанный параметр.

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

   ```
   kesl-control --get-settings <имя или идентификатор 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 блок с описанием области проверки для задачи с ID=100:

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

Запуск и остановка задачи

Вы не можете запускать и останавливать задачи типов Backup и License.

- *Чтобы запустить задачу, выполните следующую команду:*

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

- *Чтобы остановить задачу, выполните следующую команду:*

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

Приостановка и возобновление задачи

Вы можете приостанавливать и возобновлять выполнение задач типов ODS, BootScan и MemoryScan.

- *Чтобы приостановить задачу, выполните следующую команду:*

  ```
  kesl-control --suspend-task <ID задачи>|<имя задачи>
  ```

  После выполнения команды выполнение задачи приостанавливается.

- *Чтобы возобновить задачу, выполните следующую команду:*

  ```
  kesl-control --resume-task <ID задачи>|<имя задачи>
  ```

  После выполнения команды выполнение задачи возобновляется.

Управление областями проверки из командной строки

Вы можете добавлять или удалять область проверки с указанным параметром `Path` для задач OAS, ODS, OAFIM, ODFIM и Защита от шифрования из командной строки.

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

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

В конфигурационный файл будет добавлен новый блок `[ScanScope.item_#]`. Kaspersky Endpoint Security будет проверять объекты, расположенные в директории, указанной в параметре `Path`.

Если блок `[ScanScope.item_#]` для указанного параметра `Path` уже существует, дублирующий блок не добавляется в конфигурационный файл. Если для параметра `UseScanArea` установлено значение `No`, после выполнения этой команды значение изменяется на `Yes` и объекты, расположенные в этой директории, проверяются.

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

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

Блок `[ScanScope.item_#]`, содержащий указанный путь, удаляется из конфигурационного файла задачи. Kaspersky Endpoint Security не будет проверять объекты, расположенные в директории, указанной в параметре `Path`.

Управление исключенными областями из командной строки

Вы можете добавлять или удалять область исключения с указанным параметром `Path` для задач OAS, ODS, OAFIM, ODFIM и Защита от шифрования из командной строки.

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

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

В конфигурационный файл будет добавлен новый блок `[ExcludedFromScanScope.item_#]`. Kaspersky Endpoint Security будет исключать объекты, расположенные в директории, указанной в параметре `Path`.

Если блок `[ExcludedFromScanScope.item_#]` для указанного параметра `Path` уже существует, дублирующий блок не добавляется в конфигурационный файл. Если для параметра `UseScanArea` установлено значение `No`, после выполнения этой команды значение изменяется на `Yes` и объекты, расположенные в этой директории, исключаются из проверки.

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

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

Блок `[ExcludedFromScanScope.item_#]`, содержащий указанный путь, удаляется из конфигурационного файла задачи. Kaspersky Endpoint Security не будет исключать объекты, расположенные в директории, указанной в параметре `Path`.

Просмотр состояния задачи

Вы можете просматривать состояние задачи.

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

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

Здесь:

- `<ID задачи>` – идентификатор задачи, который Kaspersky Endpoint Security присваивает задаче при создании.
- `<имя задачи>` – имя, которое вы указываете для новой задачи.

Задачи Kaspersky Endpoint Security могут находиться в одном из следующих состояний:

- `Started` – выполняется;
- `Starting` – запускается;
- `Stopped` – остановлена;
- `Stopping` – останавливается;
- `Suspended` – приостановлена;
- `Suspending` – приостанавливается;
- `Resumed` – возобновлена;
- `Resuming` – возобновляется.

Настройка расписания задачи

► *Чтобы настроить расписание задачи, выполните следующие действия:*

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

   ```
   kesl-control --get-schedule <ID задачи>|<имя задачи>
   ```

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

   ```
   kesl-control --set-schedule <ID задачи>|<имя задачи> --file <полный путь к файлу>
   ```

Получение параметров расписания задачи

Команда `kesl-control --get-schedule` выводит параметры расписания задачи. Используя эту команду, вы также можете получить параметры расписания задачи, заданные с помощью ключей команды.

Вы можете использовать эту команду для изменения расписания задачи:

1. Сохраните параметры расписания в конфигурационном файле с помощью команды `kesl-control --get-schedule`.
2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `kesl-control --set-schedule`. Kaspersky Endpoint Security применит новые значения параметров расписания немедленно.

Синтаксис команды

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

Аргументы и ключи

`<ID задачи>`

Идентификационный номер задачи в Kaspersky Endpoint Security.

`<имя задачи>`

Имя задачи.

`--file <имя конфигурационного файла>`

Имя конфигурационного файла, в котором 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.

Пример:

Сохранить параметры Kaspersky Endpoint Security в файле с именем update_schedule.ini. Сохранить созданный файл в текущей директории:

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

Возвращает расписание задачи Обновление:

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

Изменение параметров расписания задачи

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

Вы можете использовать эту команду для изменения параметров Kaspersky Endpoint Security:

1. Сохраните параметры расписания в конфигурационном файле с помощью команды `kesl-control --get-schedule`.
2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `kesl-control -T --set-schedule`. Kaspersky Endpoint Security применит новые значения параметров расписания немедленно.

Синтаксис команды

```
kesl-control --set-schedule <ID задачи>|<имя задачи> --file <имя конфигурационного файла>
kesl-control --set-schedule <ID задачи>|<имя задачи> <название параметра>=<значение параметра> <название параметра>=<значение параметра>
```

Аргументы и ключи

`<ID задачи>`

Идентификационный номер задачи в Kaspersky Endpoint Security.

`<имя задачи>`

Имя 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
```

Удаление задачи

Вы можете удалять задачи, которые вы создали (пользовательские задачи).

► *Чтобы удалить задачу, выполните следующую команду:*

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

Задача Защита от файловых угроз (File_Monitoring ID:1)

В этом разделе содержится информация о задаче Защита от файловых угроз.

В этой главе

О защите от файловых угроз

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

Во время работы задачи Защита от файловых угроз, Kaspersky Endpoint Security Service Pack 1 Maintenance Release 1 выполняет проверку всех пространств имен во всех поддерживаемых операционных системах. Дополнительно для операционной системы Astra Linux пользовательская задача антивирусной проверки (Scan_File) позволяет проверять файлы из других пространств имен (в рамках обязательной проверки).

Для запуска и остановки задачи Защита от файловых угроз из командной строки необходимы root-права.

Нельзя создавать пользовательские задачи Защита от файловых угроз. Вы можете изменить настройки задачи Защиты от файловых угроз по умолчанию (см. стр. 65).

Параметры постоянной защиты содержатся в конфигурационном файле, который используется в задаче Защита от файловых угроз.

О зараженных файлах

При проверке файлов Kaspersky Endpoint Security использует антивирусные базы. Базы содержат файлы с фрагментами кода угроз и алгоритмы лечения объектов, в которых содержатся эти угрозы. Антивирусные базы позволяют обнаруживать в проверяемых файлах известные угрозы.

Если в файле содержится код, который полностью совпадает с кодом известной угрозы, Kaspersky Endpoint Security присваивает файлу статус Зараженный.

Особенности проверки символических и жестких ссылок

Kaspersky Endpoint Security позволяет проверять символические и жесткие ссылки на файлы.

Проверка символических ссылок

Kaspersky Endpoint Security проверяет символические ссылки, только если файл, на который ссылается символическая ссылка, входит в область защиты задачи Защита от файловых угроз или в область проверки задачи антивирусной проверки.

Если файл, обращение к которому происходит по символической ссылке, не входит в область защиты или в область проверки задачи, программа не проверяет этот файл. Если такой файл содержит вредоносный код, безопасность компьютера окажется под угрозой.

Проверка жестких ссылок

Когда Kaspersky Endpoint Security обрабатывает файл, у которого больше одной жесткой ссылки, программа выбирает действие в зависимости от заданного действия над объектами:

- Если выбрано действие **Выполнять рекомендуемое действие** (Recommended), Kaspersky Endpoint Security 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), Kaspersky Endpoint Security удаляет обрабатываемую жесткую ссылку. Остальные жесткие ссылки на этот файл обработаны не будут.
- Если выбрано действие **Лечить** (Cure), Kaspersky Endpoint Security лечит исходный файл. Если лечение невозможно, программа удаляет жесткую ссылку и создает вместо нее копию исходного файла с именем удаленной жесткой ссылки.

Когда вы восстанавливаете файл с жесткой ссылкой из Хранилища, Kaspersky Endpoint Security 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 этом разделе содержится информация о параметрах, которые вы можете указать для задачи Защита от файловых угроз.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanArchived

Включение или отключение проверки архивов (включая самораспаковывающиеся архивы SFX). Kaspersky Endpoint Security обнаруживает угрозы в архивах, но не лечит их. Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.

Доступные значения:

`Yes` – проверять архивы;

`No` – не проверять архивы.

Значение по умолчанию: `No`

ScanSfxArchived

Включение или отключение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы;

`No` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `No`

ScanMailBases

Включение или отключение проверки почтовых баз приложений Microsoft Outlook®, Outlook Express, The Bat и других.

Доступные значения:

`Yes` – проверять файлы почтовых баз;

`No` – не проверять файлы почтовых баз.

Значение по умолчанию: `No`.

ScanPlainMail

Включение или отключение проверки сообщений электронной почты в текстовом формате (plain text).

Доступные значения:

`Yes` – проверять сообщения электронной почты в текстовом формате;

`No` – не проверять сообщения электронной почты в текстовом формате.

Значение по умолчанию: `No`.

SizeLimit

Задает максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, Kaspersky Endpoint Security пропускает объект.

Этот параметр применяется совместно с параметром `UseSizeLimit`.

Доступные значения:

`0 - 999,999.`

`0` – Kaspersky Endpoint Security проверяет объекты любого размера.

Значение по умолчанию: `0`.

TimeLimit

Задает максимальную продолжительность проверки объекта (в секундах). Kaspersky Endpoint Security прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.

Этот параметр применяется совместно с параметром `UseTimeLimit`.

Доступные значения:

`0 – 9999`.

`0` – продолжительность проверки объектов не ограничена.

Значение по умолчанию: `60`.

FirstAction

Выбор первого действия Kaspersky Endpoint Security над зараженными объектами.

В задаче Защита от файловых угроз, перед тем как выполнить над объектом выбранное вами действие, Kaspersky Endpoint Security блокирует доступ к этому объекту для программ, которые к нему обращаются.

Доступные значения:

`Cure` (лечить) – Kaspersky Endpoint Security пытается вылечить объект, сохранив копию объекта в Хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным. Если первым действием выбрано `Cure`, рекомендуется задать второе действие в параметре `SecondAction`.

`Remove` (удалять) – Kaspersky Endpoint Security удаляет зараженный объект, предварительно создав его резервную копию.

`Recommended` (выполнять рекомендуемое действие) – Kaspersky Endpoint Security 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) – Kaspersky Endpoint Security блокирует доступ к зараженному объекту. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию: `Recommended`.

SecondAction

Выбор второго действия Kaspersky Endpoint Security над зараженными объектами. Kaspersky Endpoint Security выполняет второе действие, если не удалось выполнить первое действие.

Значения параметра `SecondAction` такие же, как значения параметра `FirstAction`.

Если в качестве первого действия выбрано `Block` (блокировать) или `Remove` (удалять), то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия. Если вы не указали второе действие, Kaspersky Endpoint Security в качестве второго действия применяет `Block` (блокировать).

Значение по умолчанию: `Block`.

UseExcludeMasks

Включает или отключает исключение из проверки объектов, указанных параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные параметром `ExcludeMasks`.

No – не исключать объекты, указанные параметром ExcludeMasks.

Значение по умолчанию: No.

ExcludeMasks

Исключает из проверки объекты 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 командной оболочки.

Значение по умолчанию не задано.

Пример:

```
UseExcludeMasks=Yes
ExcludeMasks.item_0000=eicar1.*
ExcludeMasks.item_0001=eicar2.*
```

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром ExcludeThreats.

Доступные значения:

Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats;

No – не исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.

Значение по умолчанию: No.

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр UseExcludeThreats.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы Kaspersky Endpoint Security не блокировал ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (https://securelist.ru/). Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

```
UseExcludeThreats=Yes
ExcludeThreats.item_0000=EICAR-Test-*
ExcludeThreats.item_0001=?rojan.Linux
```

ReportCleanObjects

Включает или отключает запись в журнал информации о проверенных объектах, которые Kaspersky Endpoint Security признал незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен Kaspersky Endpoint Security.

Доступные значения:

`Yes` – записывать в журнал информацию о незараженных объектах;

`No` – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: `No`.

ReportPackedObjects

Включает или отключает запись 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 Kaspersky Endpoint Security.

Доступные значения:

`Yes` – записывать в журнал информацию о проверке объектов в составе архивов;

`No` – не записывать в журнал информацию о проверке объектов в составе архивов.

Значение по умолчанию: `No`.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

`Yes` – записывать в журнал информацию о непроверенных объектах;

`No` – не записывать в журнал информацию о непроверенных объектах.

Значение по умолчанию: `No`.

UseAnalyzer

Включает или отключает эвристический анализатор.

Эвристический анализ помогает программе распознавать новые угрозы еще до того, как они станут известны вирусным аналитикам.

Доступные значения:

`Yes` – включить эвристический анализатор;

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`.

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.

Доступные значения:

`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.

Значение по умолчанию: `Recommended`.

UseIChecker

Включает или отключает использование технологии iChecker.

Доступные значения:

`Yes` – включить использование технологии iChecker;

`No` – отключить использование технологии iChecker.

Значение по умолчанию: `Yes`.

ScanByAccessType

С помощью этого параметра можно указать режим задачи Защита от файловых угроз. Параметр `ScanByAccessType` применяется только в задаче Защита от файловых угроз.

Доступные значения:

`SmartCheck` – 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.

Значение по умолчанию: `SmartCheck`.

В блоке `[ScanScope.item_#]` содержатся 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

Этот параметр включает или отключает проверку указанной области. Для выполнения задачи необходимо включить проверку хотя бы одной области.

Доступные значения:

`Yes` – проверять указанную область;

`No` – не проверять указанную область.

Значение по умолчанию: `Yes`.

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

В области проверки Kaspersky Endpoint Security проверяет только файлы, указанные помощью масок в формате командной оболочки.

Если параметр не указан, Kaspersky Endpoint Security проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.

Значение по умолчанию: `*` (проверять все объекты).

Пример:

```
AreaMask=*doc
```

Path

С помощью этого параметра вы можете указать путь к проверяемым объектам.

Значение параметра `Path` включает два элемента: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

`<путь к локальной директории>` – проверять объекты в указанной директории;

`Shared:NFS` – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу NFS;

`Shared:SMB` – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу SMB;

`AllRemoteMounted` – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – проверять все ресурсы файловой системы компьютера, предоставленные для доступа по протоколам SMB и NFS.

В блоке `[ExcludedFromScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Описание области исключения из проверки. Содержит дополнительную информацию об области исключения.

Значение по умолчанию не задано.

Пример:

```
AreaDesc="Исключение разделенных SAMBA"
```

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

С помощью этого параметра вы можете указать путь к исключаемым объектам.

Значение параметра `Path` включает два элемента: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

`<путь к локальной директории>` – исключать из проверки объекты в указанной директории; Для указания пути можно использовать маски

Можно использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включая символ /. Например, /dir/**/file*/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

`Shared:NFS` – исключать из проверки ресурсы файловой системы компьютера, предоставленные для доступа по протоколу NFS;

`Shared:SMB` – исключать из проверки ресурсы файловой системы компьютера, предоставленные для доступа по протоколу Samba;

`AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – исключать из проверки все ресурсы файловой системы компьютера, предоставленные для доступа по протоколам SMB и NFS.

Формирование глобальной области исключения

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

► *Чтобы создать глобальную область исключения, выполните следующие действия:*

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

   ```
   kesl-control --get-settings <имя или идентификатор задачи> --file <полный путь к конфигурационному файлу>
   ```

2. Добавьте в созданный файл блок `[ExcludedFromScanScope.item_#]`. В каждом блоке `[ExcludedFromScanScope.item_#]` содержатся следующие параметры:

   - AreaMask, указывает маски имени файла для файлов, которые следует исключить из области защиты.
   - AreaDesc, задает уникальное имя области исключения.
   - Path, указывает путь к файлам, которые следует исключить из области защиты.

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

   ```
   kesl-control --set-settings <имя или идентификатор задачи> --file <полный путь к конфигурационному файлу>
   ```

Задача антивирусной проверки (Scan_My_Computer ID:2)

В этом разделе содержится информация о задаче антивирусной проверки.

В этой главе

Об антивирусной проверке

Антивирусная проверка – это однократная полная или выборочная проверка файлов на компьютере, выполняемая Kaspersky Endpoint Security. Kaspersky Endpoint Security может выполнять несколько задач антивирусной проверки одновременно.

По умолчанию в Kaspersky Endpoint Security создается одна стандартная задача антивирусной проверки – полная проверка. Программа проверяет все объекты, расположенные на локальных дисках компьютера, а также все смонтированные и разделяемые объекты, доступ к которым предоставляется по протоколам Samba и NFS, с рекомендуемыми параметрами безопасности.

Пользователи могут создавать пользовательские задачи антивирусной проверки.

По умолчанию в Kaspersky Endpoint Security также создается стандартная пользовательская задача антивирусной проверки.

Если программа была перезапущена контрольной службой или вручную пользователем во время антивирусной проверки, выполнение задачи прерывается. В журнале программы сохраняется событие *OnDemandTaskInterrupted*.

Параметры задачи антивирусной проверки

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи антивирусной проверки.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanArchived

Включение или отключение проверки архивов (включая самораспаковывающиеся архивы SFX). Kaspersky Endpoint Security обнаруживает угрозы в архивах, но не лечит их. Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.

Доступные значения:

`Yes` – проверять архивы;

No – не проверять архивы.

Значение по умолчанию: Yes.

ScanSfxArchived

Включение или отключение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).

Доступные значения:

Yes – проверять самораспаковывающиеся архивы;

No – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: Yes.

ScanMailBases

Включение или отключение проверки почтовых баз приложений Microsoft Outlook®, Outlook Express, The Bat и других.

Доступные значения:

Yes – проверять файлы почтовых баз;

No – не проверять файлы почтовых баз.

Значение по умолчанию: No.

ScanPlainMail

Включение или отключение проверки сообщений электронной почты в текстовом формате (plain text).

Доступные значения:

Yes – проверять сообщения электронной почты в текстовом формате;

No – не проверять сообщения электронной почты в текстовом формате.

Значение по умолчанию: No.

UseSizeLimit

Включение или отключение применения параметра SizeLimit (максимальный размер проверяемого объекта).

Доступные значения:

Yes – применять параметр SizeLimit;

No – не применять параметр SizeLimit.

Значение по умолчанию: No.

SizeLimit

Задает максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, Kaspersky Endpoint Security пропускает объект.

Этот параметр применяется совместно с параметром UseSizeLimit.

Доступные значения:

0 – 999,999.

`0` – Kaspersky Endpoint Security проверяет объекты любого размера.

Значение по умолчанию: `0`.

UseTimeLimit

Включение или отключение применения параметра `TimeLimit` (максимальная продолжительность проверки объекта).

Доступные значения:

`Yes` – применять параметр `TimeLimit`;

`No` – не применять параметр `TimeLimit`.

Значение по умолчанию: `No`

TimeLimit

Задает максимальную продолжительность проверки объекта (в секундах). Kaspersky Endpoint Security прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.

Этот параметр применяется совместно с параметром `UseTimeLimit`.

Доступные значения:

0 – 9999.

`0` – продолжительность проверки объектов не ограничена.

Значение по умолчанию: `0`.

FirstAction

Выбор первого действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

`Cure` (лечить) – Kaspersky Endpoint Security пытается вылечить объект, сохранив копию объекта в Хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным. Если первым действием выбрано `Cure`, рекомендуется задать второе действие в параметре `SecondAction`.

`Remove` (удалять) – Kaspersky Endpoint Security удаляет зараженный объект, предварительно создав его резервную копию.

`Recommended` (выполнять рекомендуемое действие) – Kaspersky Endpoint Security 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) – Kaspersky Endpoint Security не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию: `Recommended`.

SecondAction

Выбор второго действия Kaspersky Endpoint Security над зараженными объектами. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security в качестве второго действия применяет `Skip` (пропускать).

Значение по умолчанию: `Skip`.

UseExcludeMasks

Включает или отключает исключение из проверки объектов, указанных параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные параметром `ExcludeMasks`.

`No` – не исключать объекты, указанные параметром `ExcludeMasks`.

Значение по умолчанию: `No`.

ExcludeMasks

Исключает из проверки объекты 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 командной оболочки.

Значение по умолчанию не задано.

Пример:

```
UseExcludeMasks=Yes
ExcludeMasks.item_0000=eicar1.*
ExcludeMasks.item_0001=eicar2.*
```

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Доступные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`.

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы Kaspersky Endpoint Security не блокировал ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (https://securelist.ru/). Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

```
UseExcludeThreats=Yes
ExcludeThreats.item_0000=EICAR-Test-*
ExcludeThreats.item_0001=?rojan.Linux
```

ReportCleanObjects

Включает или отключает запись в журнал информации о проверенных объектах, которые Kaspersky Endpoint Security признал незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен Kaspersky Endpoint Security.

Доступные значения:

`Yes` – записывать в журнал информацию о незараженных объектах;

`No` – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: `No`.

ReportPackedObjects

Включает или отключает запись 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 Kaspersky Endpoint Security.

Доступные значения:

`Yes` – записывать в журнал информацию о проверке объектов в составе архивов;

`No` – не записывать в журнал информацию о проверке объектов в составе архивов.

Значение по умолчанию: `No`.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

`Yes` – записывать в журнал информацию о непроверенных объектах;

`No` – не записывать в журнал информацию о непроверенных объектах.

Значение по умолчанию: `No`.

UseAnalyzer

Включает или отключает эвристический анализатор.

Эвристический анализ помогает программе распознавать новые угрозы еще до того, как они станут известны вирусным аналитикам.

Доступные значения:

`Yes` – включить эвристический анализатор;

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`.

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.

Доступные значения:

`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.

Значение по умолчанию: `Recommended`.

UseIChecker

Включает или отключает использование технологии iChecker.

Доступные значения:

`Yes` – включить использование технологии iChecker;

`No` – отключить использование технологии iChecker.

Значение по умолчанию: `Yes`.

ScanByAccessType

С помощью этого параметра вы можете задать режим постоянной защиты. Параметр `ScanByAccessType` применяется только в задаче Защита от файловых угроз.

Доступные значения:

`SmartCheck` – 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.

Значение по умолчанию: `SmartCheck`.

В блоке `[ScanScope.item_#]` содержатся 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

Включает или выключает проверку указанной области. Для выполнения задачи необходимо включить проверку хотя бы одной области.

Доступные значения:

`Yes` – проверять указанную область;

`No` – не проверять указанную область.

Значение по умолчанию: `Yes`.

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

В области проверки Kaspersky Endpoint Security проверяет только файлы, указанные помощью масок в формате командной оболочки.

Если параметр не указан, Kaspersky Endpoint Security проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.

Значение по умолчанию: `*` (проверять все объекты).

Пример:

```
AreaMask=*doc
```

Path

С помощью этого параметра вы можете указать путь к проверяемым объектам.

Значение параметра `Path` включает два элемента: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

`<путь к локальной директории>` – проверять объекты в указанной директории;

`Shared:NFS` – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу NFS;

`Shared:SMB` – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу SMB;

`AllRemoteMounted` – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – проверять все ресурсы файловой системы компьютера, предоставленные для доступа по протоколам SMB и NFS.

В блоке `[ExcludedFromScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Описание области исключения из проверки. Содержит дополнительную информацию об области исключения.

Значение по умолчанию не задано.

Пример:

```
AreaDesc="Исключение разделенных SAMBA"
```

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

С помощью этого параметра вы можете указать путь к исключаемым объектам.

Значение параметра `Path` включает два элемента: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

`<путь к локальной директории>` – исключать из проверки объекты в указанной директории; Для указания пути можно использовать маски

Можно использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включая символ /. Например, /dir/**/file*/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

`Shared:NFS` – исключать из проверки ресурсы файловой системы компьютера, предоставленные для доступа по протоколу NFS;

`Shared:SMB` – исключать из проверки ресурсы файловой системы компьютера, предоставленные для доступа по протоколу Samba;

`AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – исключать из проверки все ресурсы файловой системы компьютера, предоставленные для доступа по протоколам SMB и NFS.

Задача выборочной проверки (Scan_File ID:3)

В этом разделе содержится информация о задаче выборочной проверки.

В этой главе

О задаче выборочной проверки

Задача выборочной проверки использует параметры, которые применяются командой `kesl-control --scan-file`.

Вы можете проверить файл или директорию с помощью следующей команды:

```
kesl-control --set-settings--scan-file <путь к файлу>
```

Программа создает временную задачу антивирусной проверки (тип=ODS) с параметрами задачи Scan_File. После завершения проверки временная задача автоматически удаляется.

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

Настройка параметров задачи выборочной проверки

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи выборочной проверки.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanArchived

Включение или отключение проверки архивов (включая самораспаковывающиеся архивы SFX). Kaspersky Endpoint Security обнаруживает угрозы в архивах, но не лечит их. Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.

Доступные значения:

`Yes` – проверять архивы;

`No` – не проверять архивы.

Значение по умолчанию: `Yes`.

ScanSfxArchived

Включение или отключение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы;

`No` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `Yes`.

ScanMailBases

Включение или отключение проверки почтовых баз приложений Microsoft Outlook®, Outlook Express, The Bat и других.

Доступные значения:

`Yes` – проверять файлы почтовых баз;

`No` – не проверять файлы почтовых баз.

Значение по умолчанию: `No`.

ScanPlainMail

Включение или отключение проверки сообщений электронной почты в текстовом формате (plain text).

Доступные значения:

`Yes` – проверять сообщения электронной почты в текстовом формате;

`No` – не проверять сообщения электронной почты в текстовом формате.

Значение по умолчанию: `No`.

UseSizeLimit

Включение или отключение применения параметра `SizeLimit` (максимальный размер проверяемого объекта).

Доступные значения:

`Yes` – применять параметр `SizeLimit`;

`No` – не применять параметр `SizeLimit`.

Значение по умолчанию: `No`.

SizeLimit

Задает максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, Kaspersky Endpoint Security пропускает объект.

Этот параметр применяется совместно с параметром `UseSizeLimit`.

Доступные значения:

`0 - 999,999.`

`0` – Kaspersky Endpoint Security проверяет объекты любого размера.

Значение по умолчанию: `0`.

UseTimeLimit

Включение или отключение применения параметра `TimeLimit` (максимальная продолжительность проверки объекта).

Доступные значения:

`Yes` – применять параметр `TimeLimit`;

`No` – не применять параметр `TimeLimit`.

Значение по умолчанию: `No`

TimeLimit

Задает максимальную продолжительность проверки объекта (в секундах). Kaspersky Endpoint Security прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.

Этот параметр применяется совместно с параметром `UseTimeLimit`.

Доступные значения:

`0 - 9999`

`0` – продолжительность проверки объектов не ограничена.

Значение по умолчанию: `0`.

FirstAction

Выбор первого действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

`Cure` (лечить) – Kaspersky Endpoint Security пытается вылечить объект, сохранив копию объекта в Хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным. Если первым действием выбрано `Cure`, рекомендуется задать второе действие в параметре `SecondAction`.

`Remove` (удалять) – Kaspersky Endpoint Security удаляет зараженный объект, предварительно создав его резервную копию.

`Recommended` (выполнять рекомендуемое действие) – Kaspersky Endpoint Security 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) – Kaspersky Endpoint Security не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию: `Recommended`.

SecondAction

Выбор второго действия Kaspersky Endpoint Security над зараженными объектами. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security в качестве второго действия применяет `Skip` (пропускать).

Значение по умолчанию: `Skip`.

UseExcludeMasks

Включает или отключает исключение из проверки объектов, указанных параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные параметром `ExcludeMasks`.

`No` – не исключать объекты, указанные параметром `ExcludeMasks`.

Значение по умолчанию: `No`.

ExcludeMasks

Исключает из проверки объекты 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 командной оболочки.

Значение по умолчанию не задано.

Пример:

```
UseExcludeMasks=Yes
ExcludeMasks.item_0000=eicar1.*
ExcludeMasks.item_0001=eicar2.*
```

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Доступные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`.

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы Kaspersky Endpoint Security не блокировал ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (https://securelist.ru/). Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

```
UseExcludeThreats=Yes
ExcludeThreats.item_0000=EICAR-Test-*
ExcludeThreats.item_0001=?rojan.Linux
```

ReportCleanObjects

Включает или отключает запись в журнал информации о проверенных объектах, которые Kaspersky Endpoint Security признал незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен Kaspersky Endpoint Security.

Доступные значения:

`Yes` – записывать в журнал информацию о незараженных объектах;

`No` – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: `No`.

ReportPackedObjects

Включает или отключает запись 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 Kaspersky Endpoint Security.

Доступные значения:

`Yes` – записывать в журнал информацию о проверке объектов в составе архивов;

`No` – не записывать в журнал информацию о проверке объектов в составе архивов.

Значение по умолчанию: `No`.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

`Yes` – записывать в журнал информацию о непроверенных объектах;

`No` – не записывать в журнал информацию о непроверенных объектах.

Значение по умолчанию: `No`.

UseAnalyzer

Включает или отключает эвристический анализатор. Эвристический анализ помогает программе распознавать новые угрозы еще до того, как они станут известны вирусным аналитикам.

Доступные значения:

`Yes` – включить эвристический анализатор;

No – отключить эвристический анализатор.

Значение по умолчанию: Yes.

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.

Доступные значения:

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.

Значение по умолчанию: Recommended.

UseIChecker

Включает или отключает использование технологии iChecker.

Доступные значения:

Yes – включить использование технологии iChecker;

No – отключить использование технологии iChecker.

Значение по умолчанию: Yes.

ScanByAccessType

С помощью этого параметра вы можете задать режим постоянной защиты. Параметр ScanByAccessType применяется только в задаче Защита от файловых угроз.

Доступные значения:

SmartCheck – 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.

Значение по умолчанию: SmartCheck.

В блоке [ScanScope.item_#] содержатся 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

Включает или выключает проверку указанной области. Для выполнения задачи необходимо включить проверку хотя бы одной области.

Доступные значения:

`Yes` – проверять указанную область;

`No` – не проверять указанную область.

Значение по умолчанию: `Yes`.

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

В области проверки Kaspersky Endpoint Security проверяет только файлы, указанные помощью масок в формате командной оболочки.

Если параметр не указан, Kaspersky Endpoint Security проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.

Значение по умолчанию: `*` (проверять все объекты).

Пример:

```
AreaMask=*doc
```

Path

С помощью этого параметра вы можете указать путь к проверяемым объектам.

Значение параметра `Path` включает два элемента: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

`<путь к локальной директории>` – проверять объекты в указанной директории;

`Shared:NFS` – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу NFS;

`Shared:SMB` – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу SMB;

`AllRemoteMounted` – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – проверять все ресурсы файловой системы компьютера, предоставленные для доступа по протоколам SMB и NFS.

В блоке `[ExcludedFromScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Описание области исключения из проверки. Содержит дополнительную информацию об области исключения.

Значение по умолчанию не задано.

Пример:

```
AreaDesc="Исключение разделенных SAMBA"
```

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

С помощью этого параметра вы можете указать путь к исключаемым объектам.

Значение параметра `Path` включает два элемента: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

`<путь к локальной директории>` – исключать из проверки объекты в указанной директории; Для указания пути можно использовать маски

Можно использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включая символ /. Например, /dir/**/file*/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

`Shared:NFS` – исключать из проверки ресурсы файловой системы компьютера, предоставленные для доступа по протоколу NFS;

`Shared:SMB` – исключать из проверки ресурсы файловой системы компьютера, предоставленные для доступа по протоколу Samba;

`AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – исключать из проверки все ресурсы файловой системы компьютера, предоставленные для доступа по протоколам SMB и NFS.

Задача проверки загрузочных секторов (Boot_Scan ID:4)

В этом разделе содержится информация о задаче проверки загрузочных секторов.

В этой главе

О задаче проверки загрузочных секторов

Задача проверки загрузочных секторов позволяет проверять загрузочные сектора без указания области проверки.

Параметры задачи проверки загрузочных секторов

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи проверки загрузочных секторов.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

UseExcludeMasks

Включает или отключает исключение из проверки объектов, указанных параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные параметром `ExcludeMasks`.

`No` – не исключать объекты, указанные параметром `ExcludeMasks`.

Значение по умолчанию: `No`.

ExcludeMasks

Исключает из проверки объекты 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 командной оболочки.

Значение по умолчанию не задано.

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Доступные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы Kaspersky Endpoint Security не блокировал ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (https://securelist.ru/). Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

ReportCleanObjects

Включает или отключает запись в журнал информации о проверенных объектах, которые Kaspersky Endpoint Security признал незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен Kaspersky Endpoint Security.

Доступные значения:

`Yes` – записывать в журнал информацию о незараженных объектах;

`No` – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: `No`.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о файлах, которые по какой-то причине не были обработаны.

Доступные значения:

`Yes` – записывать в журнал информацию о непроверенных объектах. Не рекомендуется надолго устанавливать значение `Yes` для этого параметра, так как запись большого объема информации может снизить производительность программы.

`No` – не записывать в журнал информацию о необработанных объектах.

Значение по умолчанию: `No`

UseAnalyzer

Включает или отключает эвристический анализатор. Эвристический анализ помогает программе распознавать новые угрозы еще до того, как они станут известны вирусным аналитикам.

Доступные значения:

`Yes` – включить эвристический анализатор;

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`.

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.

Доступные значения:

`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.

Значение по умолчанию: `Recommended`.

Action

Выбор действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

`Cure` (лечить) – Kaspersky Endpoint Security пытается вылечить объект, сохранив копию объекта в Хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным.

`Skip` (пропускать) – Kaspersky Endpoint Security не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию: `Cure`.

Задача проверки памяти процессов (Memory_Scan ID:5)

В этом разделе содержится информация о задаче проверки памяти процессов.

В этой главе

О задаче проверки памяти процессов

Задача проверки памяти процессов позволяет проверять память процессов без указания области проверки.

Параметры задачи проверки памяти процессов

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи проверки памяти процессов.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Доступные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`.

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы Kaspersky Endpoint Security не блокировал ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (https://securelist.ru/). Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

ReportCleanObjects

Включает или отключает запись в журнал информации о проверенных объектах, которые Kaspersky Endpoint Security признал незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен Kaspersky Endpoint Security.

Доступные значения:

`Yes` – записывать в журнал информацию о незараженных объектах;

`No` – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: `No`.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о файлах, которые по какой-то причине не были обработаны.

Доступные значения:

`Yes` – записывать в журнал информацию о непроверенных объектах. Не рекомендуется надолго устанавливать значение `Yes` для этого параметра, так как запись большого объема информации может снизить производительность программы.

`No` – не записывать в журнал информацию о необработанных объектах.

Значение по умолчанию: `No`

Action

Выбор действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

`Cure` (лечить) – Kaspersky Endpoint Security пытается вылечить объект, сохранив копию объекта в Хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным.

`Skip` (пропускать) – Kaspersky Endpoint Security не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию: `Cure`.

Задача обновления (Update ID:6)

В этом разделе содержится информация о задаче обновления.

В этой главе

Об обновлении баз и модулей программы

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

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

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

Для успешной загрузки пакета обновлений с серверов обновлений "Лаборатории Касперского" компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, требуется настроить параметры прокси-сервера.

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

- Базы Kaspersky Endpoint Security. Во время установки Kaspersky Endpoint Security получает актуальные базы с одного из HTTP-серверов обновлений "Лаборатории Касперского". Если для обновления используется предустановленная задача с параметрами по умолчанию (ID=6), Kaspersky Endpoint Security обновляет базы с периодичностью один раз в 60 минут. Вы можете изменять параметры предустановленной задачи обновления баз и модулей программы и создавать пользовательские задачи обновления.

  Kaspersky Endpoint Security продолжает использовать предыдущую установленную версию баз, если загрузка обновлений баз прерывается или завершается с ошибкой. Если отсутствуют установленные ранее доступные базы программы, то программа продолжит работу в режиме "без баз". Обновление баз и модулей программы остается доступным.

  По умолчанию программа записывает в журнал событие *Базы устарели* (AVBasesAreOutOfDate), если последние установленные обновления баз были опубликованы на сервере "Лаборатории Касперского" более семи дней назад. Если базы не обновляются в течение семи дней, Kaspersky Endpoint Security записывает в журнал событие *Базы сильно устарели* (AVBasesAreTotallyOutOfDate). Базы актуальны, если они были загружены менее 24 часов назад.

- Обновления программы Помимо баз Kaspersky Endpoint Security, можно обновлять и саму программу. Обновления программы устраняют уязвимости Kaspersky Endpoint Security или улучшают существующие.

  Обновление программы может быть установлено вне зависимости от состояния программы (запущена или остановлена, управляется политикой Kaspersky Security Center) и расписания обновлений.

  Kaspersky Endpoint Security продолжает защищать ваш компьютер во время процедуры обновления программы.

  Kaspersky Endpoint Security автоматически переносит параметры программы и журналы событий. Параметры предыдущей версии программы экспортируются при запуске обновленной версии.

  Если после обновления программы Kaspersky Endpoint Security работает некорректно, программа автоматически откатывается на предыдущую версию. Отображается сообщение об откате обновления программы. Мы рекомендуем обратиться в службу технической поддержки "Лаборатории Касперского".

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

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

Об источниках обновлений

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

В предустановленной задаче обновления по умолчанию в качестве источника обновлений выбраны серверы обновлений "Лаборатории Касперского". На серверах обновлений выкладываются обновления баз и программных модулей для многих программ "Лаборатории Касперского". Обновления загружаются по протоколам HTTP.

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 вами локальной или сетевой директории (SMB / NFS), примонтированной пользователем, или с FTP- или HTTP-сервера. Вы можете указать пользовательский источник обновлений в конфигурационном файле задачи обновления.

Параметры задачи обновления

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи обновления.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

SourceType

С помощью этого параметра вы можете выбрать источник, из которого Kaspersky Endpoint Security будет получать обновления.

Доступные значения:

KLServers – Kaspersky Endpoint Security получает обновления с одного из серверов обновлений "Лаборатории Касперского". Обновления загружаются по протоколу HTTP.

`SCServer` – Kaspersky Endpoint Security загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновления, если вы используете программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации.

`Custom` – Kaspersky Endpoint Security загружает обновления из пользовательского источника, указанного в блоке `[CommonSettings:CustomSources]`. Вы можете указывать директории HTTP-серверов или директории на любом смонтированном устройстве защищаемого компьютера, включая директории на удаленных компьютерах, смонтированные по протоколам Samba или NFS.

Значение по умолчанию: `KLServers`.

UseKLServersWhenUnavailable

С помощью этого параметра вы можете настроить обращение Kaspersky Endpoint Security к серверам обновлений "Лаборатории Касперского" в случае, если все пользовательские источники недоступны.

Доступные значения:

`Yes` – Kaspersky Endpoint Security обращается к серверам обновлений "Лаборатории Касперского", если все пользовательские источники обновлений недоступны;

`No` – Kaspersky Endpoint Security не обращается к серверам обновлений "Лаборатории Касперского", если все пользовательские источники обновлений недоступны.

Значение по умолчанию: `Yes`.

IgnoreProxySettingsForKLServers

С помощью этого параметра вы можете настроить использование прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского".

Доступные значения:

`Yes` – Kaspersky Endpoint Security не использует прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского";

`No` – Kaspersky Endpoint Security использует прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского".

Значение по умолчанию: `No`.

IgnoreProxySettingsForCustomSources

С помощью этого параметра вы можете настроить использование прокси-сервера для соединения с пользовательскими источниками обновлений. Вам нужно включить этот параметр, если для соединения с каким-либо из пользовательских HTTP-серверов обновлений требуется доступ к прокси-серверу.

Доступные значения:

`Yes` – Kaspersky Endpoint Security не использует прокси-сервер для соединения с пользовательскими источниками обновлений;

`No` – Kaspersky Endpoint Security использует прокси-сервер для соединения с пользовательскими источниками обновлений.

Значение по умолчанию: `No`.

ApplicationUpdateMode

Отображает режим загрузки и установки обновлений программы.

Для сохранения сертифицированной конфигурации программы значение параметра `ApplicationUpdateMode` должно быть `Disabled`.

Доступные значения:

`Disabled` – не загружать и не устанавливать обновления программы;

`DownloadOnly` – загружать обновления программы, но не устанавливать их;

`DownloadAndInstall` – автоматически загружать и устанавливать обновления программы.

Значение по умолчанию: `DownloadOnly`.

ConnectionTimeout

С помощью этого параметра вы можете указать время ожидания (в секундах) ответа от источника обновлений – HTTP-сервера при соединении с ним. Если в течение указанного промежутка времени от источника обновлений не приходит ответ, Kaspersky Endpoint Security обращается к другому указанному источнику обновлений.

Вы можете указывать только целые числа в диапазоне от 0 до 120.

Значение по умолчанию: `10`.

Блок `[CustomSources.item_#]` содержит следующие параметры:

URL

С помощью этого параметра вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.

Значение по умолчанию не задано.

Пример:

```
URL=http://example.com/bases/ – адрес HTTP-сервера, на котором помещается директория с обновлениями.

URL=/home/bases/ – директория на защищаемом компьютере, в которой содержатся базы программы.
```

Enabled

С помощью этого параметра вы можете включить или отключить использование источника обновлений, указанного в параметре `URL`. Для выполнения задачи необходимо, чтобы использование хотя бы одного источника обновлений было включено.

Доступные значения:

`Yes` – Kaspersky Endpoint Security использует источник обновления;

`No` – Kaspersky Endpoint Security не использует источник обновления.

Значение по умолчанию не задано.

Пример:

```
Enabled=Yes
```

Установка обновления программы вручную

Вы можете вручную установить обновление программы из командной строки. Для установки обновления на вашем компьютере должен быть установлен Kaspersky Endpoint Security. Остановка работы программы не требуется: если процесс обновления завершается с ошибкой, программа автоматически откатывается к предыдущей версии.

► *Чтобы установить обновление Kaspersky Endpoint Security из пакета формата RPM, выполните следующую команду:*

```
# rpm –U <имя пакета в формате rpm>.rpm
```

► *Чтобы установить обновление Kaspersky Endpoint Security той же версии из пакета формата RPM, выполните следующую команду:*

```
# rpm –U --replacefiles –replacepkgs <имя пакета в формате rpm>.rpm
```

► *Чтобы установить обновление Kaspersky Endpoint Security из пакета формата DEB, выполните следующую команду:*

```
# dpkg -i <имя пакета в формате deb>.deb
```

Процесс обновления программы запущен.

Может потребоваться перезагрузка программы или операционной системы. Отобразится соответствующее сообщение. После перезапуска программы или операционной системы запускается обновленная версия Kaspersky Endpoint Security.

После обновления программы может потребоваться принять Лицензионное соглашение, условия Политики конфиденциальности или Положение о Kaspersky Security Network, если они были изменены «Лабораторией Касперского» (отображается соответсвующее сообщение).

► *Чтобы принять Лицензионное соглашение,*

1. Прочитайте текст Лицензионного соглашения (/opt/kaspersky/kesl/doc/license.<language ID>) .
2. Если вы согласны с текстом Лицензионного соглашения, укажите переменную среды:
   - # KESL_EULA_AGREED=yes rpm -U <имя пакета в формате rpm>.rpm для пакета в формате rpm.
   - # KESL_EULA_AGREED=yes dpkg -i <имя пакета в формате deb>.deb для пакета в формате deb.

► *Чтобы принять условия Политики конфиденциальности,*

3. Прочитайте текст Политики конфиденциальности (/opt/kaspersky/kesl/doc/license.<language ID>) .
4. Если вы согласны с текстом Лицензионного соглашения, укажите переменную среды:
   - # KESL_ PRIVACY_POLICY_AGREED=yes rpm -U <имя пакета в формате rpm>.rpm для пакета в формате rpm.
   - # KESL_ PRIVACY_POLICY_AGREED=yes dpkg -i <имя пакета в формате deb>.deb для пакета в формате deb.

► *Чтобы принять Положение о Kaspersky Security Network,*

1. Прочитайте текст Положения о Kaspersky Security Network.
2. Если вы согласны с текстом Положения о Kaspersky Security Network, укажите переменную среды:
   - # KESL_USE_KSN=yes rpm -U <имя пакета в формате rpm>.rpm for a rpm package.
   - # KESL_ USE_KSN=yes dpkg -i <имя пакета в формате deb>.deb for a deb package.

Если вы не принимаете Лицензионное соглашение и/или условия Политики конфиденциальности, процесс обновления программы прерывается.

Задача отката обновления (Rollback ID:7)

В этом разделе содержится информация о задаче отката обновления.

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

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

Задача Откат обновлений не имеет параметров.

Подробнее об управлении задачей отката обновления см. в разделе "Управление задачами Kaspersky Endpoint Security с помощью командной строки" (см. стр. 65).

Задача копирования обновлений (Retranslate ID:8)

В этом разделе содержится информация о задаче копирования обновлений.

В этой главе

О задаче копирования обновлений

Задача копирования обновлений позволяет загружать обновления баз и программы в выбранную директорию. Обновления не устанавливаются.

Скопированные обновления баз может использовать только программа с тем же номером сборки.

Параметры задачи копирования обновлений

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи копирования обновлений.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

SourceType

С помощью этого параметра вы можете выбрать источник, из которого Kaspersky Endpoint Security будет получать обновления.

Доступные значения:

KLServers – Kaspersky Endpoint Security получает обновления с одного из серверов обновлений "Лаборатории Касперского". Обновления загружаются по протоколу HTTP.

`SCServer` – Kaspersky Endpoint Security загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновления, если вы используете программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации.

`Custom` – Kaspersky Endpoint Security загружает обновления из пользовательского источника, указанного в блоке `[CommonSettings:CustomSources]`. Вы можете указывать директории HTTP-серверов или директории на любом смонтированном устройстве защищаемого компьютера, включая директории на удаленных компьютерах, смонтированные по протоколам Samba или NFS.

Значение по умолчанию: `KLServers`.

UseKLServersWhenUnavailable

С помощью этого параметра вы можете настроить обращение Kaspersky Endpoint Security к серверам обновлений "Лаборатории Касперского" в случае, если все пользовательские источники недоступны.

Доступные значения:

`Yes` – Kaspersky Endpoint Security обращается к серверам обновлений "Лаборатории Касперского", если все пользовательские источники обновлений недоступны;

`No` – Kaspersky Endpoint Security не обращается к серверам обновлений "Лаборатории Касперского", если все пользовательские источники обновлений недоступны.

Значение по умолчанию: `Yes`.

IgnoreProxySettingsForKLServers

С помощью этого параметра вы можете настроить использование прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского".

Доступные значения:

`Yes` – Kaspersky Endpoint Security не использует прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского";

`No` – Kaspersky Endpoint Security использует прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского".

Значение по умолчанию: `No`.

IgnoreProxySettingsForCustomSources

С помощью этого параметра вы можете настроить использование прокси-сервера для соединения с пользовательскими источниками обновлений. Вам нужно включить этот параметр, если для соединения с каким-либо из пользовательских HTTP-серверов обновлений требуется доступ к прокси-серверу.

Доступные значения:

`Yes` – Kaspersky Endpoint Security не использует прокси-сервер для соединения с пользовательскими источниками обновлений;

`No` – Kaspersky Endpoint Security использует прокси-сервер для соединения с пользовательскими источниками обновлений.

Значение по умолчанию: `No`.

ConnectionTimeout

С помощью этого параметра вы можете указать время ожидания (в секундах) ответа от источника обновлений – HTTP-сервера при соединении с ним. Если в течение указанного промежутка времени от источника обновлений не приходит ответ, Kaspersky Endpoint Security обращается к другому указанному источнику обновлений.

Вы можете указывать только целые числа в диапазоне от 0 до 120.

Значение по умолчанию: `10`.

RetranslationFolder

С помощью этого параметра вы можете указать директорию, в которую будут копироваться обновления. Если указанная директория не существует, Kaspersky Endpoint Security создает ее во время выполнения задачи копирования обновлений.

Блок [CustomSources.item_#] содержит следующие параметры:

URL

С помощью этого параметра вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.

Значение по умолчанию не задано.

Пример:

URL=http://example.com/bases/ – адрес HTTP-сервера, на котором помещается директория с обновлениями.

URL=/home/bases/ – директория на защищаемом компьютере, в которой содержатся базы программы.

Enabled

Включает или выключает использование источника обновлений, указанного в параметре URL. Для выполнения задачи необходимо, чтобы использование хотя бы одного источника обновлений было включено.

Доступные значения:

Yes – Kaspersky Endpoint Security использует источник обновления;

No – Kaspersky Endpoint Security не использует источник обновления.

Значение по умолчанию не задано.

ApplicationUpdateMode

Отображает режим загрузки и установки обновлений программы.

Доступные значения:

Disabled – не загружать и не устанавливать обновления программы;

DownloadOnly – загружать обновления программы, но не устанавливать их;

DownloadAndInstall – автоматически загружать и устанавливать обновления программы.

Значение по умолчанию: Disabled.

Задача реализации сервера лицензий (License ID:9)

В этом разделе содержится информация о задаче, реализующей сервер лицензий.

В этой главе

О задаче реализации сервера лицензий

Задача, реализующая сервер лицензий позволяет управлять ключами и кодами активации Kaspersky Endpoint Security.

Добавление активного ключа

Команда `kesl-control --install-active-key` добавляет активный ключ. Подробнее о ключах см. в разделе "О ключе".

Синтаксис команды

```
kesl-control [-L] --install-active-key <путь к файлу ключа>|<код активации>
```

Аргументы и ключи

`<путь к файлу ключа>`

Путь к файлу ключа; если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

```
Добавить ключ из файла /home/test/00000001.key в качестве активного:

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

Добавление дополнительного ключа

Команда `kesl-control --install-additional-key` добавляет дополнительный ключ. Подробнее о ключах см. в разделе "О ключе".

Если активный ключ не установлен, то дополнительный ключ будет установлен как основной.

Синтаксис команды

```
kesl-control [-L] --install-additional-key <путь к файлу ключа>
```

Аргументы и ключи

`<путь к файлу ключа>`

Путь к файлу ключа; если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

Установить дополнительный ключ из файла /home/test/00000002.key:

```
kesl-control --install-additional-key /home/test/00000002.key
```

Удаление активного ключа

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

Синтаксис команды

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

Удаление дополнительного ключа

Команда `kesl-control --revoke-additional-key` удаляет дополнительный ключ.

Синтаксис команды

```
kesl-control [-L] --revoke-additional-key
```

Ввод дополнительного кода активации

Команда `kesl-control --install-additional-key` вводит дополнительный код активации. Подробнее о кодах активации читайте в разделе "О коде активации".

Синтаксис команды

```
kesl-control [-L] --install-additional-key <код активации>
```

Задача управления Хранилищем (Backup ID:10)

В этом разделе содержится информация о задаче управления Хранилищем.

В этой главе

О Хранилище

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.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, пользователь может попытаться восстановить файл из его вылеченной копии в директорию исходного размещения файла.

Параметры задачи управления Хранилищеми

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи управления Хранилищем.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

DaysToLive

Время хранения объектов в Хранилище (в днях).

Чтобы снять ограничение на время хранения объектов в Хранилище, укажите значение 0.

Значение по умолчанию: 90.

BackupSizeLimit

Максимальный размер Хранилища.

При достижении максимального размера Хранилища Kaspersky Endpoint Security удаляет наиболее давние объекты.

Доступные значения:

0–999 999 (в МБ).

Чтобы снять ограничение на размер Хранилища, укажите значение 0.

Значение по умолчанию: `0`.

BackupFolder

Путь к директории Хранилища вы можете указать пользовательскую директорию Хранилища, отличную от директории, установленной по умолчанию.

Для Хранилища вы можете использовать директории на любых устройствах компьютера. Не рекомендуется указывать директории, расположенные на удаленных компьютерах, например смонтированных по протоколам Samba и NFS.

Kaspersky Endpoint Security начинает помещать объекты в указанную директорию после того, как вы импортируете параметры из файла в задачу для Хранилища и перезапустите Kaspersky Endpoint Security.

Если указанная директория не существует или недоступна, Kaspersky Endpoint Security использует директорию Хранилища по умолчанию.

Значение по умолчанию: `/var/opt/kaspersky/kesl/objects-backup/`

Просмотр идентификаторов объектов в Хранилище

При помещении объекта в Хранилище Kaspersky Endpoint Security присваивает ему числовой идентификатор. Этот идентификатор используется для выполнения действий над объектом, таких как восстановление (см. стр. 120) или удаление (см. стр. 120) объекта из Хранилища.

► *Чтобы просмотреть идентификаторы объектов в Хранилище,*

выполните команду: `kesl-control -B --query`

Идентификатор объекта отображается в строке `ObjectId`.

О восстановлении объектов из Хранилища

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

Вы можете восстанавливать объекты из Хранилища. Восстановление объектов может потребоваться в следующих случаях:

- При лечении зараженного файла Kaspersky Endpoint Security не удалось сохранить его целостность, и в результате информация в файле стала недоступной.
- Если вы считаете, что объект безопасен для сервера, и хотите использовать его, вы можете исключить объект из области проверки, и программа не будет обнаруживать его во время последующих проверок. Для этого вам нужно исключить объект по имени или по названию угрозы, обнаруженной при выполнении задачи Защита от файловых угроз, а также по имени объекта и по названию угрозы, обнаруженной в задаче антивирусной проверки.

Восстановление зараженных объектов может привести к заражению компьютера.

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

Восстановление объектов из Хранилища

► *Чтобы восстановить объект из Хранилища, выполните одно из следующих действий:*

- Чтобы восстановить объект с исходным именем и в исходное местоположение, выполните команду:

  `kesl-control --restore <ID объекта>`

  где `ID объекта` – идентификатор объекта в Хранилище.

- Чтобы восстановить объект с новым именем в указанную директорию, выполните команду:

  `[-B] --restore <ID объекта> --file <имя и директория файла>`

  Если указанная директория не существует, Kaspersky Endpoint Security создает ее.

Удаление объектов из Хранилища

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

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

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

```
kesl-control -B --mass-remove --query "<поле><оператор сравнения>
'<значение>' [и <поле> <оператор сравнения>'<значение>' ]* ]
```

► *Чтобы удалить все объекты из Хранилища, выполните одну из следующих команд:*

```
kesl-control -B --mass-remove
```

или

```
kesl-control -B --mass-remove --query
```

Задача мониторинга файловых операций (Integrity_Monitoring ID:11)

В этом разделе содержится информация о задаче Мониторинг файловых операций.

В этой главе

О мониторинге файловых операций

Задача Мониторинг файловых операций создана 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. Вы также можете настроить отслеживание изменений в файлах в течение времени, когда мониторинг прерывается.

Для использования функции мониторинга файловых операций необходимо приобрести лицензию, которая включает эти функции. По умолчанию мониторинг файловых операций выключен.

Мониторинг файловых операций может выполняться в режиме реального времени при запуске задачи *Мониторинг файловых операций при доступе* (OAFIM) (см. стр. 121). Кроме этого можно создавать и запускать задачи *Мониторинг файловых операций по требованию* (ODFIM). (см. стр 122)

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.

Мониторинг файловых операций при доступе (OAFIM)

Во время работы задачи OAFIM каждое изменение объекта определяется путем перехвата файловых операций в режиме реального времени. При изменении объекта Kaspersky Endpoint Security отправляет событие на Сервер администрирования Kaspersky Security Center. Во время работы задачи контрольная сумма файла не рассчитывается. Задача OAFIM не отслеживает изменения файлов (атрибутов и содержимого) с жесткими ссылками, которые расположены вне области мониторинга.

Kaspersky Endpoint Security отслеживает операции с конкретными файлами или в областях, указанных в параметрах задачи.

Области мониторинга

Области мониторинга для задачи Мониторинг файловых операций всегда должны быть указаны. Администратор может изменять области проверки и мониторинга в режиме реального времени. Если область мониторинга не указана, параметры задачи нельзя сохранить в конфигурационном файле. При добавлении области мониторинга или области исключения программа не проверяет, существует ли такая директория.

Вы можете указать несколько областей мониторинга.

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.

Исключения имеют более высокий приоритет, чем область мониторинга, и не проверяются задачей, даже если указанная папка 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.

Чтобы указать исключения, можно использовать те же маски в формате командной оболочки, которые используются для указания областей мониторинга.

Контролируемые параметры

Во время работы задачи Мониторинг файловых операций 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 компоненту Мониторинг файловых операций определять, какой администратор или процесс внес изменение в файл.

Мониторинг файловых операций по требованию (ODFIM)

В ходе выполнения задачи ODFIM изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве *снимка состояния системы*.

Вы можете создать несколько задач ODFIM.

Снимок состояния системы

Снимок состояния системы задается во время первого запуска задачи ODFIM на компьютере. Для каждой задачи ODFIM создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы соответствует области мониторинга. Если снимок состояния системы не соответствует области мониторинга, Kaspersky Endpoint Security создает событие о нарушении целостности файла.

Вы можете заново создать снимок состояния системы для задачи с помощью соответствующего параметра (см. стр. 123). Снимок состояния системы создается заново после завершения задачи ODFIM.

Снимок состояния системы также создается заново при изменении параметров задачи, например когда добавляется новая область мониторинга. Снимок состояния системы будет создан заново при следующем выполнение задачи.

Задача ODFIM создает хранилище для снимков состояния системы на компьютере с установленным компонентом Мониторинг файловых операций.

Удалить снимок состояния системы можно, только удалив соответствующую задачу ODFIM.

Параметры задачи Мониторинг файловых операций при доступе

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Мониторинг файловых операций при доступе.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

UseExcludeMasks

Включает или выключает исключение из области мониторинга объектов, указанных параметром `ExcludeMasks`.

Параметр `UseExcludeMasks` работает только с указанным параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

`No` – не исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

Значение по умолчанию: `No`

ExcludeMasks

Указывает список масок, которые определяют объекты, исключаемые из области мониторинга.

Прежде чем указать этот параметр, убедитесь, что для параметра `UseExcludeMasks` 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 (`ExcludeMasks.item_0000`, `ExcludeMasks.item_0001`).

Значение по умолчанию: не задано

Блок [ScanScope.item_#]

В блоках `[ScanScope.item_#]` указываются области мониторинга для задачи Мониторинг файловых операций. Для задачи должна быть указана минимум одна область мониторинга.

Вы можете указать в конфигурационном файле несколько блоков `[ScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

В каждом блоке `[ScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Указывает имя области мониторинга.

UseScanArea

Включает или выключает мониторинг указанной области.

Доступные значения:

`Yes` – контролировать указанную область;

`No` – не контролировать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает полный путь к объекту или директориям для мониторинга.

Значение по умолчанию: `/opt/kaspersky/kesl/`

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты для мониторинга.

Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: `*` (будут обработаны все объекты).

Блок [ExcludedFromScanScope.item_#]

В блоках `[ExcludedFromScanScope.item_#]` указываются объекты, которые нужно исключить из всех блоков `[ScanScope.item_#]`.

Все объекты, которые соответствуют правилам любого блока `[ExcludedFromScanScope.item_#]`, будут исключены из области мониторинга. Формат блока `[ExcludedFromScanScope.item_#]` идентичен формату блока `[ScanScope.item_#]`.

Вы можете указать в конфигурационном файле несколько блоков `[ExcludedFromScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

В каждом блоке `[ScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Указывает имя области, которую нужно исключить из мониторинга.

UseScanArea

Указывает, будут ли указанные области исключены из мониторинга.

Доступные значения:

`Yes` – исключать указанные области из мониторинга;

`No` – не исключать указанные области из мониторинга.

Значение по умолчанию: `Yes`.

Path

Указывает путь к объектам или директориям, исключенным из мониторинга. Для указания пути можно использовать маски.

Можно использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включая символ /. Например, /dir/**/file*/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты, исключенные из мониторинга.

Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: `*` (будут контролироваться все объекты).

Параметры задачи Мониторинг файловых операций по требованию

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Мониторинг файловых операций по требованию.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

RebuildBaseline

Включает или выключает повторное создание снимка состояния системы после завершения задачи ODFIM.

Доступные значения:

`Yes` – создавать снимок состояния системы повторно после завершения задачи ODFIM;

`No` – не создавать снимок состояния системы повторно после завершения задачи ODFIM.

Значение по умолчанию: `No`

CheckFileHash

Включает или выключает проверку хеша (SHA-256).

Доступные значения:

`Yes` – включить проверку хеша;

`No` – выключить проверку хеша.

Значение по умолчанию: `No`

TrackDirectoryChanges

Включает или выключает мониторинг директорий.

Доступные значения:

`Yes` – контролировать директории;

`No` – не контролировать директории.

Значение по умолчанию: `No`

TrackLastAccessTime

Включает или выключает проверку времени последнего доступа к файлу. В операционной системе Linux это параметр `noatime`.

Доступные значения:

`Yes` – проверять время последнего доступа к файлу;

`No` – не проверять время последнего доступа к файлу.

Значение по умолчанию: `No`

UseExcludeMasks

Включает или отключает исключение из области мониторинга объектов, указанных параметром `ExcludeMasks`.

Этот параметр работает только с указанным параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

`No` – не исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

Значение по умолчанию: `No`

ExcludeMasks

Указывает список масок, которые определяют объекты, исключаемые из области мониторинга.

Прежде чем указать этот параметр, убедитесь, что для параметра `UseExcludeMasks` 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 (`ExcludeMasks.item_0000`, `ExcludeMasks.item_0001`).

Значение по умолчанию: не задано

Блок [ScanScope.item_#]

В блоках `[ScanScope.item_#]` указываются области мониторинга для задачи Мониторинг файловых операций. Для задачи должна быть указана минимум одна область мониторинга.

Вы можете указать в конфигурационном файле несколько блоков `[ScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

В каждом блоке `[ScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Указывает имя области мониторинга.

UseScanArea

Включает или выключает мониторинг указанной области.

Доступные значения:

`Yes` – контролировать указанную область;

`No` – не контролировать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает полный путь к объекту или директориям для мониторинга.

Значение по умолчанию: `/opt/kaspersky/kesl/`

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты для мониторинга.

Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: `*` (будут обработаны все объекты).

Блок [ExcludedFromScanScope.item_#]

В блоках `[ExcludedFromScanScope.item_#]` указываются объекты, которые нужно исключить из всех блоков `[ScanScope.item_#]`.

Все объекты, которые соответствуют правилам любого блока `[ExcludedFromScanScope.item_#]`, будут исключены из области мониторинга. Формат блока `[ExcludedFromScanScope.item_#]` идентичен формату блока `[ScanScope.item_#]`.

Вы можете указать в конфигурационном файле несколько блоков `[ExcludedFromScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

В каждом блоке `[ScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Указывает имя области, которую нужно исключить из мониторинга.

UseScanArea

Указывает, будут ли указанные области исключены из мониторинга.

Доступные значения:

`Yes` – исключать указанные области из мониторинга;

`No` – не исключать указанные области из мониторинга.

Значение по умолчанию: `Yes`.

Path

Указывает путь к объектам или директориям, исключенным из мониторинга. Для указания пути можно использовать маски.

Можно использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включая символ /. Например, /dir/**/file*/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты, исключенные из мониторинга.

Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: `*` (будут контролироваться все объекты).

Задача Управление сетевым экраном (Firewall ID:12)

В этом разделе содержится информация о задаче Управление сетевым экраном.

В этой главе

Об Управлении сетевым экраном

Для сохранения сертифицированной конфигурации программы задача Управление сетевым экраном должна быть остановлена.

Во время работы в локальных сетях и интернете компьютер подвержен 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 компьютере пользователя. Сетевой экран блокирует большую часть потенциальных угроз для операционной системы, когда компьютер подключен к интернету или локальной сети. Управление сетевым экраном позволяет обнаружить все сетевые соединения на компьютере пользователя и предоставить список их IP-адресов с указанием статуса сетевого соединения по умолчанию.

Компонент Управление сетевым экраном фильтрует всю сетевую активность в соответствии с сетевыми пакетными правилами (см. стр. 130). Настройка сетевых пакетных правил позволяет вам задать нужный уровень защиты компьютера, от полной блокировки доступа в интернет для всех программ до разрешения неограниченного доступа.

Во время работы задачи Управление сетевым экраном Kaspersky Endpoint Security управляет параметрами и правилами сетевого экрана операционной системы. Программа блокирует любую настройку параметров сетевого экрана операционной системы, например когда программа или инструмент добавляют или удаляют

правила. Kaspersky Endpoint Security проверяет сетевой экран операционной системы каждые 60 секунд и при необходимости восстанавливает набор правил сетевого экрана. Периодичность проверки изменить нельзя.

Проверка сетевого экрана операционной системы по-прежнему выполняется, когда задача Управление сетевым экраном остановлена. Это позволяет программе восстанавливать динамические правила (см. стр. 130).

Все исходящие соединения разрешены по умолчанию (параметр действия 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.

Перед включением задачи Управление сетевым экраном мы рекомендуем отключить другие средства управления сетевым экраном операционной системы.

О сетевых пакетных правилах

Сетевое пакетное правило представляет собой разрешающее или запрещающее действие, которое совершает задача Управление сетевым экраном, обнаружив попытку сетевого соединения.

Используются для ввода ограничений на сетевые пакеты независимо от программы. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных.

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 Kaspersky Endpoint Security могут добавлять и удалять *динамические правила* для сетевого экрана, необходимые для правильной работы. Например, Агент администрирования добавляет динамические правила, которые разрешают соединение с Kaspersky Security Center, инициируемые как программой, так и Kaspersky Security Center. Таким образом, правила задачи Защита от шифрования являются динамическими.

Задача Управление сетевым экраном не контролирует динамические правила и не блокирует доступ к сетевым ресурсам для компонентов программы. 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. Kaspersky Endpoint Security восстанавливает набор динамических правил, если какие-либо из них были удалены, например, с помощью утилиты iptables.

Вы можете просматривать набор динамических правил (с помощью команды `kesl-control –F –query`), но не можете изменять их параметры.

О предустановленных именах сетевых зон

Заданная сетевая зона представляет собой конкретную группу IP-адресов или IP-подсетей. С помощью заданной сетевой зоны вы можете использовать одно и то же правило для нескольких IP-адресов или IP-подсетей, не создавая отдельное правило для каждого IP-адреса или IP-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 антивирусной программой, 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 компьютере (таким как локальные или домашние сети).
- **Доверенные**. Эта зона предназначена для безопасных сетей, в которых компьютеры не подвержены атакам или несанкционированным попыткам доступа к данным.

Вы не можете создать или удалить сетевую зону. Вы можете добавить (см. стр. 137) или удалить (см. стр. 137) IP-подсети из сетевой зоны.

Параметры задачи Управление сетевым экраном

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Управление сетевым экраном.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

DefaultIncomingAction

Действие по умолчанию, применяемое к входящему соединению, если другие сетевые правила не применяются к этому виду соединения.

Доступные значения:

`Allow` – разрешать входящие соединения;

`Block` – запрещать входящие соединения.

Значение по умолчанию: `Allow`.

DefaultIncomingPacketAction

Действие по умолчанию, применяемое к входящему пакету, если другие сетевые пакетные правила не применяются к этому виду соединения.

Доступные значения:

`Allow` – разрешать входящие пакеты;

`Block` – запрещать входящие пакеты.

Значение по умолчанию: `Allow`.

Блок [PacketRules.item_xxxx]

В блоках `[PacketRules.item_#]` указываются сетевые пакетные правила для задачи Управление сетевым экраном.

Вы можете указать в конфигурационном файле несколько блоков `[PacketRules.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Каждый блок `[PacketRules.item_#]` содержит следующие параметры:

Name

Имя сетевого пакетного правила.

Значение по умолчанию: `Network rule #<n>`, где `n` является индексом.

FirewallAction

Действие, применяемое к соединениям, указанным в сетевом пакетном правиле.

Доступные значения:

`Allow` – разрешать сетевые соединения;

`Block` – запрещать сетевые соединения.

Значение по умолчанию: `Allow`.

Protocol

Тип протокола, для которого необходим мониторинг сетевой активности.

Доступные значения:

`Any` – задача Управление сетевым экраном контролирует всю сетевую активность.

`TCP`.

`UDP`.

`ICMP`.

`ICMPv6`.

`IGMP`.

`GRE`.

Значение по умолчанию: `Any`.

RemotePorts

Номера портов удаленных компьютеров, соединение между которыми отслеживается.

Этот параметр можно указать, только если для параметра `Protocol` установлено значение `TCP` или `UDP`.

Для этого параметра можно указать значение в виде целого числа или интервала.

Доступные значения:

`Any` – контролировать все удаленные порты.

`0 - 65535`

Значение по умолчанию: `Any`.

LocalPorts

Номера портов локальных компьютеров, соединение между которыми отслеживается.

Этот параметр можно указать, только если для параметра `Protocol` установлено значение `TCP` или `UDP`.

Для этого параметра можно указать значение в виде целого числа или интервала.

Доступные значения:

`Any` – контролировать все локальные порты.

`0 - 65535`

Значение по умолчанию: `Any`.

ICMPType

Тип пакета ICMP.

Этот параметр можно указать, только если для параметра `Protocol` установлено значение `ICMP` или `ICMPv6`.

Доступные значения:

`Any` – контролировать все типы пакетов ICMP.

Целое число согласно спецификации протокола передачи данных.

Значение по умолчанию: `Any`.

ICMPCode

Код пакета ICMP.

Этот параметр можно указать, только если для параметра `Protocol` установлено значение `ICMP` или `ICMPv6`.

Доступные значения:

`Any` – контролировать все коды пакетов ICMP.

Целое число согласно спецификации протокола передачи данных.

Значение по умолчанию: `Any`.

Direction

Направление отслеживаемой сетевой активности.

Доступные значения:

`IncomingOutgoing` – контролируются как входящие, так и исходящие соединения.

`Incoming` – контролировать входящие соединения.

`Outgoing` – контролировать исходящие соединения.

`IncomingPacket` – контролировать входящие пакеты.

`OutgoingPacket` – контролировать исходящие пакеты.

`IncomingOutgoingPacket` – контролировать как входящие, так и исходящие пакеты.

Значение по умолчанию: `IncomingOutgoing`.

RemoteAddress

Сетевые адреса удаленных компьютеров, которые могут передавать и / или получать сетевые пакеты.

Доступные значения:

`Any` – контролируется отправка и / или получение сетевых пакетов удаленными компьютерами 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` – IP-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` – IP-подсеть адресов IPv6, где `p` – число от 0 до 64.

Значение по умолчанию: `Any`.

LocalAddress

Сетевые адреса компьютеров с установленным Kaspersky Endpoint Security, которые могут передавать и/или получать сетевые пакеты.

Доступные значения:

`Any` – контролируется отправка и / или получение сетевых пакетов удаленными компьютерами с любым IP-адресом.

`d.d.d.d` – адреса IPv4, где `d` – десятичное число от 0 до 255.

`d.d.d.d/p` – IP-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` – IP-подсеть адресов IPv6, где `p` – число от 0 до 64.

Значение по умолчанию: `Any`.

LogAttempts

Указывает, следует ли включать в отчет действия сетевого правила.

Доступные значения:

`Yes` – отражать действия в отчете.

`No` – не отражать действия в отчете.

Значение по умолчанию: `No`

Блок [NetworkZonesPublic]

В блоке `[NetworkZonesPublic]` указываются сетевые адреса, связанные с публичными сетями.

Вы можете указать несколько IP-адресов или IP-подсетей.

Address.item_xxxx

Доступные значения:

`d.d.d.d` – адреса IPv4, где `d` – десятичное число от 0 до 255.

`d.d.d.d/p` – IP-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` – IP-подсеть адресов IPv6, где `p` – число от 0 до 64.

Значение по умолчанию: "" (в этой зоне нет сетевых адресов)

Блок [NetworkZonesLocal]

В блоке `[NetworkZonesLocal]` указываются сетевые адреса, связанные с локальными сетями.

Вы можете указать несколько IP-адресов или IP-подсетей.

Address.item_xxxx

Доступные значения:

`d.d.d.d` – адреса IPv4, где `d` – десятичное число от 0 до 255.

`d.d.d.d/p` – IP-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` – IP-подсеть адресов IPv6, где `p` – число от 0 до 64.

Значение по умолчанию: "" (в этой зоне нет сетевых адресов)

Блок [NetworkZonesTrusted]

В блоке `[NetworkZonesTrusted]` указываются сетевые адреса, связанные с доверенными сетями.

Вы можете указать несколько IP-адресов или IP-подсетей.

Address.item_xxxx

Доступные значения:

`d.d.d.d` – адреса IPv4, где `d` – десятичное число от 0 до 255.

`d.d.d.d/p` – IP-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` – IP-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 вручную (см. стр. 130).

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 блок, содержащий параметры нового сетевого пакетного правила. Если вы не указали в команде конкретный параметр, устанавливается значение по умолчанию (см. стр. 187).

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>`

  Сетевое пакетное правило будет удалено по имени. Если список сетевых пакетных правил содержит несколько правил с одинаковым именем, Kaspersky Endpoint Security 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, выводится ошибка.

Изменение приоритета выполнения сетевого пакетного правила

Вы можете вручную изменить приоритетность выполнения сетевого пакетного правила.

► *Чтобы изменить приоритетность выполнения сетевого пакетного правила, выполните следующую команду:*

```
kesl-control -F --move-rule [--name <имя>|--index <индекс>] --at <индекс>
```

Приоритетность сетевого пакетного правила будет изменена в соответствии с указанным индексом.

Добавление сетевого адреса в блок зоны

Вы можете вручную добавить в конфигурационный файл задачи Управление сетевым экраном 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 блок конкретной зоны в конфигурационном файле задачи.

Удаление сетевого адреса из блока зоны

Вы можете вручную удалить из конфигурационного файла задачи Управление сетевым экраном сетевые адреса, связанные с определенным типом сети.

► *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 блока конкретной 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.

Задача Защита от шифрования (AntiCryptor ID:13)

В этом разделе содержится информация о задаче Защита от шифрования.

В этой главе

О задаче Защита от шифрования

Задача Защита от шифрования позволяет защитить ваши файлы в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования.

В ходе выполнения задачи Защита от шифрования Kaspersky Endpoint Security проверяет обращения удаленных компьютеров сети к файлам, расположенным в общих сетевых директориях защищаемого сервера. Если программа расценивает действия удаленного компьютера, получающего доступ к общим сетевым ресурсам, как шифрование, она добавляет этот компьютер в список недоверенных компьютеров и запрещает ему доступ к общим сетевым директориям.

Kaspersky Endpoint Security не расценивает действия как шифрование, если обнаруженная активность шифрования имеет место в директориях, исключенных из области задачи Защита от шифрования (см. стр. 139).

По умолчанию Kaspersky Endpoint Security блокирует доступ недоверенных компьютеров к сетевым файловым ресурсам на 30 минут.

Чтобы задача Защита от шифрования работала корректно необходимо, чтобы в операционной системе была установлена хотя бы одна из служб: Samba или NFS. Для службы NFS необходимо, чтобы был установлен 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. Мы рекомендуем настроить параметры сервера таким образом, чтобы протоколы NFS2 и NFS4 нельзя было использовать для подключения ресурсов.

Задача Защита от шифрования не блокирует доступ к сетевым файловым ресурсам, пока действия компьютера не расцениваются как вредоносные. Таким образом, минимум один файл будет зашифрован, прежде чем программа обнаружит вредоносную активность.

О блокировании доступа к сетевым файловым ресурсам

При обнаружении вредоносного шифрования Kaspersky Endpoint Security создает и включает правило для сетевого экрана операционной системы, которое блокирует сетевой трафик от скомпрометированного компьютера. Скомпрометированный компьютер добавляется в список недоверенных компьютеров. Kaspersky Endpoint Security блокирует доступ к общим сетевым директориям для всех удаленных компьютеров в списке недоверенных компьютеров. Информация обо всех заблокированных компьютерах защищаемого сервера отправляется в Kaspersky Security Center.

Правила управления сетевым экраном, созданные задачей Защита от шифрования, невозможно удалить с помощью утилиты iptables: Kaspersky Endpoint Security восстанавливает набор правил раз в минуту. Используйте команду `--allow-hosts`, чтобы разблокировать компьютер (см. стр. 142).

По умолчанию Kaspersky Endpoint Security удаляет недоверенные компьютеры из списка через 30 минут после добавления в список. Доступ компьютеров к сетевым файловым ресурсам восстанавливается автоматически после удаления недоверенного компьютера из списка. Вы можете изменять список заблокированных компьютеров и указывать период, после которого заблокированные компьютеры автоматически разблокируются.

Параметры задачи Защита от шифрования

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Защита от шифрования.

Описаны все доступные значения и значения по умолчанию для каждого параметра.

UseHostBlocker

Включает или выключает блокирование недоверенных компьютеров.

Если блокирование недоверенных компьютеров выключено, Kaspersky Endpoint Security все равно проверяет действия удаленных компьютеров с сетевыми файловыми ресурсами на наличие вредоносного шифрования, когда работает задача Защита от шифрования. При обнаружении вредоносного шифрования создается событие `EncryptionDetected`, но атакующий компьютер не блокируется.

Доступные значения:

`Yes` – включить блокирование недоверенных компьютеров;

`No` – выключить блокирование недоверенных компьютеров.

Значение по умолчанию: `Yes`.

BlockTime

Указывает длительность блокирования доступа к сетевым файловым ресурсам в минутах.

Изменение параметра `BlockTime` не влияет на длительность блокировки ранее заблокированных скомпрометированных компьютеров. Длительность блокирования не является динамическим значением и рассчитывается на момент блокирования.

Доступные значения:

Целые числа от `1` до `4294967295`

Значение по умолчанию: `30`

UseExcludeMasks

Включает или отключает исключение из области защиты объектов, указанных параметром `ExcludeMasks`.

Этот параметр работает только с указанным параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные в параметре `ExcludeMasks`, из области защиты;

`No` – не исключать объекты, указанные в параметре `ExcludeMasks`, из области защиты.

Значение по умолчанию: `No`

ExcludeMasks

Указывает список масок, которые определяют объекты, исключаемые из области защиты.

Прежде чем указать этот параметр, убедитесь, что для параметра `UseExcludeMasks` 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 (`ExcludeMasks.item_0000`, `ExcludeMasks.item_0001`).

Значение по умолчанию: не задано

Блок [ScanScope.item_#]

В блоках `[ScanScope.item_#]` указываются области, защищаемые Kaspersky Endpoint Security. Для задачи Защита от шифрования должна быть указана минимум одна область защиты.

Для задачи Защита от шифрования можно указывать только общие директории.

Вы можете указать в конфигурационном файле несколько блоков `[ScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

В каждом блоке `[ScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Указывает имя области защиты.

Значение по умолчанию: `AllSharedFolders`.

UseScanArea

Включает или выключает защиту указанной области.

Доступные значения:

`Yes` – защищать указанную область.

`No` – не защищать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает путь к защищаемым объектам.

Доступные значения:

Абсолютный путь, доступный через SMB / NFS (например, `Path=/tmp`)

`AllShared` – защищать все ресурсы, доступные через SMB / NFS;

`Shared:SMB <путь>` – защищать ресурсы, доступные через SMB.

`Shared:NFS <путь>` – защищать ресурсы, доступные через NFS.

Значение по умолчанию: `AllShared`.

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты для защиты.

Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: `*` (будут обработаны все объекты).

Блок [ExcludedFromScanScope.item_#]

В блоках `[ExcludedFromScanScope.item_#]` указываются объекты, которые нужно исключить из всех блоков `[ScanScope.item_#]`.

Все объекты, которые соответствуют правилам любого блока `[ExcludedFromScanScope.item_#]`, будут проверяться. Формат блока `[ExcludedFromScanScope.item_#]` идентичен формату блока `[ScanScope.item_#]`.

Вы можете указать в конфигурационном файле несколько блоков `[ExcludedFromScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

В каждом блоке `[ScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Указывает имя области, которую нужно исключить из проверки.

Значение по умолчанию: `All objects`

UseScanArea

Указывает, будут ли указанные области исключены из защиты.

Доступные значения:

`Yes` – исключать указанные области из защиты.

`No` – не исключать указанные области из защиты.

Значение по умолчанию: `Yes`.

Path

Указывает путь к объектам, исключенным из защиты.

Вы можете указать только абсолютный путь к локальной директории (например, `/root /tmp/123`), которую не будет защищать задача Защита от шифрования.

Для указания пути можно использовать маски.

Можно использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включая символ /. Например, /dir/**/file*/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

Значение по умолчанию: не задано

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты, исключенные из защиты.

Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: `*` (будут обработаны все объекты).

Просмотр списка заблокированных компьютеров

Вы можете просматривать список недоверенных компьютеров, заблокированных задачей Защита от шифрования.

► *Чтобы просмотреть список заблокированных компьютеров, выполните следующую команду:*

```
kesl-control -H --get-blocked-hosts
```

Будут выведены компьютеры, заблокированные задачей Защита от шифрования.

Разблокирование заблокированных компьютеров

Вы можете вручную разблокировать компьютеры, заблокированные задачей Защита от шифрования, и восстановить сетевой доступ для них.

► *Чтобы разблокировать компьютеры, выполните следующую команду:*

```
kesl-control [-H] --allow-hosts <компьютер>
```

где `<компьютер>` может быть списком действительных адресов IPv4 / IPv6 (включая адреса в короткой форме) и/или подсетей. Таким образом, вы можете указать компьютеры в виде списка.

Указанные компьютеры 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 - ::
```

Участие в Kaspersky Security Network

Этот раздел содержит информацию об участии в Kaspersky Security Network и инструкции о том, как включить и выключить использование Kaspersky Security Network.

В этой главе

Об участии в Kaspersky Security Network

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

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

В зависимости от расположения инфраструктуры различают Глобальный KSN (инфраструктура расположена на серверах "Лаборатории Касперского") и Локальный KSN (инфраструктура расположена на сторонних серверах, например внутри сети интернет-провайдера).

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN.

См. подробнее в документации Kaspersky Security Center.

После изменения лицензии для использования Локального KSN требуется предоставить поставщику услуг информацию о новом ключе. В противном случае обмен информацией с Локальным KSN будет невозможен из-за ошибки аутентификации.

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

Есть два способа участвовать в KSN:

- **Kaspersky Security Network со статистикой** – вы можете получать информацию из базы знаний. Программа автоматически отправляет в KSN статистическую информацию, полученную в результате своей работы. Также программа может отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или части файлов), которые злоумышленники могут использовать для нанесения вреда компьютеру или данным.
- **Kaspersky Security Network без статистики** – вы можете получать информацию из базы знаний, но программа не отправляет анонимную статистику и данные о типах и источниках новых угроз.

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" (http://www.kaspersky.ru/privacy). Файл с текстом Положения о Kaspersky Security Network входит в комплект поставки программы.

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

Служба KSN Proxy предоставляет следующие возможности:

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

Подробнее о службе KSN Proxy вы можете прочитать в документации для Kaspersky Security Center.

Настроить параметры KSN Proxy можно в свойствах политики Kaspersky Security Center.

Участие в Kaspersky Security Network является добровольным. Программа предлагает участвовать в KSN во время установки. Начать или прекратить использование KSN можно в любой момент.

Включение и выключение использования Kaspersky Security Network

► *Чтобы включить использование Kaspersky Security Network, выполните одну из следующих команд:*

- Чтобы включить использование Kaspersky Security Network со статистикой, выполните команду:

  ```
  kesl-control --set-app-settings UseKSN=Extended
  ```

- Чтобы включить использование Kaspersky Security Network без статистики, выполните команду:

  ```
  kesl-control --set-app-settings UseKSN=Basic
  ```

► *Чтобы выключить использование Kaspersky Security Network, выполните следующую команду:*

```
kesl-control --set-app-settings UseKSN=No
```

► *Чтобы включить или выключить использование Kaspersky Security Network с помощью конфигурационного файла, выполните следующую команду:*

```
kesl-control --set-app-settings --file <имя конфигурационного файла>
```

Если Kaspersky Endpoint Security, установленный на компьютере, работает под политикой, назначенной в Kaspersky Security Center, изменить значение параметра `UseKSN` можно только с помощью Kaspersky Security Center.

Если Kaspersky Endpoint Security, установленный на компьютере, выходит из-под политики, устанавливается значение параметра `UseKSN=No`.

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

Проверка подключения к Kaspersky Security Network

► *Чтобы проверить подключение к Kaspersky Security Network, выполните следующую команду:*

```
kesl-control --app-info
```

В строке `KSN state` отображается статус подключения к Kaspersky Security Network:

- Если отображается статус `Extended`, Kaspersky Endpoint Security подключен к Kaspersky Security Network, информация из базы знаний доступна, анонимная статистика и данные о типах и источниках новых угроз отправляются.
- Если отображается статус `Basic`, Kaspersky Endpoint Security подключен к Kaspersky Security Network, информация из базы знаний доступна, но анонимная статистика и данные о типах и источниках новых угроз не отправляются.
- Если отображается статус `No`, Kaspersky Endpoint Security не подключен к Kaspersky Security Network.

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Ваш компьютер не подключен к интернету.
- Вы не участвуете в Kaspersky Security Network.
- Программа не активирована, или срок действия лицензии истек.
- Выявлены проблемы, связанные с ключом. Например, ключ попал в черный список ключей.

Дополнительная защита с использованием Kaspersky Security Network

"Лаборатория Касперского" предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков "Лаборатории Касперского" обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте "Лаборатории Касперского".

Управление программой через Kaspersky Security Center

Этот раздел содержит информацию об управлении программой Kaspersky Endpoint Security через Kaspersky Security Center. Описание приведено для Security Center Service Pack 2.

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Security, настраивать параметры работы программы и запускать задачи на управляемых компьютерах.

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

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

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

- просматривать состояние защиты компьютеров;
- настраивать общие параметры защиты компьютеров;
- управлять политиками;
- управлять задачами:
  - добавлять ключи;
  - копировать обновления.
  - обновления;
  - откатывать обновления баз;
  - проверять загрузочные сектора;
  - проверять память процессов;
  - выполнять антивирусную проверку;
  - контролировать целостность файлов.

В этой главе

Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере

► *Чтобы запустить или остановить Kaspersky Endpoint Security на клиентском компьютере, выполните следующие действия:*

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

   Откроется окно свойств компьютера.
6. В окне свойств компьютера выберите раздел **Программы**.

   Справа в окне свойств компьютера отобразится список программ "Лаборатории Касперского", установленных на компьютере.
7. Выберите программу Kaspersky Endpoint Security 10 SP1 для Linux.
8. Выполните следующие действия:

   - Если вы хотите запустить программу, нажмите кнопку  справа от списка программ "Лаборатории Касперского" или выполните следующие действия:

     a. Правой клавишей мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 SP1 для Linux и выберите пункт **Свойства** или нажмите кнопку **Свойства**, расположенную под списком программ «Лаборатории Касперского».

        Откроется окно Параметры программы Kaspersky Endpoint Security 10 SP1 для Linux на закладке Общие.

     b. Нажмите кнопку **Запустить**.

- Если вы хотите остановить работу программы, нажмите кнопку  справа от списка программ "Лаборатории Касперского» или выполните следующие действия:

  a. Правой клавишей мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 SP1 для Linux и выберите пункт **Свойства** или нажмите кнопку **Свойства**, расположенную под списком программ.

     Откроется окно Параметры программы Kaspersky Endpoint Security 10 SP1 для Linux на закладке Общие.

  b. Нажмите кнопку **Остановить**.

Настройка параметров Kaspersky Endpoint Security

► *Чтобы настроить параметры Kaspersky Endpoint Security, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите настроить параметры Kaspersky Endpoint Security.
5. Правой клавишей мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.

   Откроется окно свойств компьютера.
6. В окне свойств компьютера выберите раздел **Программы**.

   Справа в окне свойств компьютера отобразится список программ "Лаборатории Касперского", установленных на компьютере.
7. Выберите программу Kaspersky Endpoint Security 10 SP1 для Linux.
8. Правой клавишей мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 SP1 для Linux и выберите пункт **Свойства**.

   Откроется окно **Параметры программы "Kaspersky Endpoint Security 10 SP1 для Linux"**.
9. В разделе **Дополнительные параметры** настройте параметры работы Kaspersky Endpoint Security, а также параметры отчетов и хранилищ.

Остальные разделы окна **Параметры программы "Kaspersky Endpoint Security 10 SP1 для Linux"** стандартны для программы Kaspersky Security Center, их описание вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

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

10. В окне **Параметры программы "Kaspersky Endpoint Security 10 SP1 для Linux"** нажмите кнопку **OK**, чтобы сохранить внесенные изменения.

Просмотр состояния защиты компьютера

► *Чтобы просмотреть состояние защиты компьютера, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый компьютер.
2. В рабочей области выберите закладку **Устройства**.
3. Правой клавишей мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.
4. В окне **Свойства** выберите закладку **Защита**.

На закладке **Защита** отображается следующая информация о защищаемом компьютере:

- **Статус устройства** – информация об антивирусной безопасности защищаемого компьютера, например: *Базы устарели*, *Срок действия лицензии истек*;
- **Статус постоянной защиты** – состояние задачи Защита от файловых угроз, например: *Выполняется*, *Остановлена*, *Приостановлена*.
- **Последняя антивирусная проверка** – дата и время последнего выполнения задачи антивирусной проверки.
- **Обнаружено вирусов** – общее количество вредоносных программ, обнаруженных на защищаемом компьютере (счетчик обнаруженных угроз) с момента установки Kaspersky Endpoint Security или с момента сброса счетчика. Чтобы сбросить счетчик, нажмите кнопку **Обнулить**;
- **Количество невылеченных объектов** – количество зараженных объектов, которые Kaspersky Endpoint Security не удалось вылечить.

Просмотр параметров Kaspersky Endpoint Security

► *Чтобы просмотреть параметры Kaspersky Endpoint Security, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый компьютер.
2. В рабочей области выберите закладку **Устройства**.
3. Правой клавишей мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.
4. В открывшемся окне **Свойства: <название компьютера>** выберите раздел **Программы**.
5. В разделе **Программы** выберите Kaspersky Endpoint Security 10 для Linux в списке установленных программ и в контекстном меню программы выберите пункт Свойства.

   В результате откроется окно Параметры программы **Kaspersky Endpoint Security 10 SP1 для Linux** в разделе **Общие**.

В окне Параметры программы **Kaspersky Endpoint Security 10 SP1 для Linux** отображается следующая информация о Kaspersky Endpoint Security:

- Раздел **Общие**
  - **Номер версии** – номер версии Kaspersky Endpoint Security;
  - **Установлено** – дата и время установки Kaspersky Endpoint Security на защищаемом компьютере;
  - **Текущее состояние** – состояние задачи Защита от файловых угроз, например: *Выполняется* или *Приостановлена*;
  - **Последнее обновление ПО** – дата и время последнего обновления программных модулей Kaspersky Endpoint Security;
  - **Установленные обновления** – список программных модулей, для которых установлены обновления;
  - **Базы программы** – дата и время последнего обновления антивирусных баз, а также количество записей в базах.
- Раздел **Ключи**
  - **Тип лицензии** – тип лицензии: коммерческая или пробная;
  - **Дата активации** (поле доступно только для активного ключа) – дата добавления активного ключа;
  - **Дата окончания срока действия лицензии** (поле доступно только для активного ключа) – дата окончания срока действия активного ключа;
  - **Срок действия** – количество дней, в течение которых действует ключ;
  - **Ограничение** – количество компьютеров, на которых вы можете использовать ключ.
- Раздел **События**

  В этом разделе вы можете просмотреть события, которые Kaspersky Endpoint Security сохраняет в хранилище событий.
- Раздел **Дополнительно**

  В этом разделе вы можете просмотреть информацию о плагине управления программой.

Управление политиками

Этот раздел содержит информацию о создании и настройке политик для Kaspersky Endpoint Security. Более подробную информацию о концепции управления программой Kaspersky Endpoint Security с помощью политик Kaspersky Security Center вы можете прочитать в документации Kaspersky Security Center.

О политиках

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

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

Возможность изменять параметр программы на клиентском компьютере определяется статусом "замка" у параметра в политике:

- Если параметр закрыт "замком» (), это означает, что вы не можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используется значение параметра, заданное политикой.
- Если параметр не закрыт "замком" (), это означает, что вы можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используются значения параметра, установленные локально. Значение параметра, установленное в политике, не применяется.

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

Вы можете использовать политики для настройки параметров таких задач Kaspersky Endpoint Security, как Защита от файловых угроз, Управление сетевым экраном, Защита от шифрования, Мониторинг файловых операций при доступе и Хранилища.

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

Вы можете выполнять следующие действия над политикой:

- Создавать политику.
- Изменять параметры политики.

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

- Удалять политику.
- Изменять состояние политики.

Информацию о работе с политиками, не касающуюся взаимодействия с Kaspersky Endpoint Security, вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Создание политики

► *Чтобы создать политику, выполните следующие действия:*

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

3. В рабочей области выберите закладку **Политики**.
4. Выполните одно из следующих действий:
   - Нажмите кнопку **Создать политику**.
   - Правой клавишей мыши откройте контекстное меню. Выберите пункт **Создать →политику**.

   Запустится мастер создания политики.
5. Следуйте указаниям мастера создания политики.

Изменение параметров политики

► *Чтобы изменить параметры политики, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием нужной группы администрирования, для которой вы хотите изменить параметры политики.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику.
5. Выполните одно из следующих действий:
   - Правой клавишей мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите кнопку **Изменить политику** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.

   Параметры политики для Kaspersky Endpoint Security включают в себя параметры задач и параметры программы. Раздел **Основная защита** включает блоки **Параметры защиты от файловых угроз**, **Области исключений** и **Параметры управления сетевым экраном**. Раздел **Дополнительные параметры защиты** включает блоки **Параметры KSN**, **Параметры защиты от шифрования** и **Параметры мониторинга файловых операций**. Раздел **Общие параметры** включает блоки **Параметры прокси-сервера**, **Параметры программы** и **Хранилища**.
6. Измените параметры политики.
7. В окне **Свойства: <Название политики>** нажмите кнопку **ОК**, чтобы сохранить внесенные изменения.

Управление задачами

Этот раздел содержит информацию об управлении задачами для Kaspersky Endpoint Security через Kaspersky Security Center.

Подробнее об управлении задачами через Kaspersky Security Center вы можете прочитать в документации Kaspersky Security Center.

О задачах для Kaspersky Endpoint Security

Kaspersky Security Center управляет работой программы Kaspersky Endpoint Security, установленного на компьютерах, с помощью задач (https://help.kaspersky.com/KSC/11/ru-RU/92435.htm).

При работе с Kaspersky Endpoint Security через Kaspersky Security Center вы можете создавать следующие типы задач:

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

> Задачи для наборов компьютеров, не входящих в группы администрирования, выполняются только для указанных в параметрах задачи компьютеров. Если в набор компьютеров, для которого сформирована задача, добавлены новые компьютеры, то для них эта задача не выполняется. В этом случае вам необходимо создать новую задачу или изменить параметры уже существующей задачи.

Вы можете создавать задачи следующих типов:

- **Обновление**. В процессе выполнения задачи Kaspersky Endpoint Security обновляет антивирусные базы в соответствии с установленными параметрами обновления.
- **Откат обновления**. В процессе выполнения задачи Kaspersky Endpoint Security откатывает последнее обновление антивирусных баз.
- **Копирование обновления**. В процессе выполнения задачи Kaspersky Endpoint Security скачивает антивирусные базы в указанную директорию, не устанавливая их.
- **Антивирусная проверка**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи.
- **Проверка загрузочных секторов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет загрузочные сектора компьютера.
- **Проверка памяти процессов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет системную память компьютера.
- **Добавление ключа**. В процессе выполнения задачи Kaspersky Endpoint Security добавляет ключ, в том числе дополнительный, для активации программы.
- **Проверка целостности файлов по требованию**. В ходе выполнения этой задачи изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.

Вы можете выполнять следующие действия над задачами:

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

Права на доступ к параметрам задач Kaspersky Endpoint Security (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через параметры доступа к функциональным областям Kaspersky Endpoint Security. Для настройки прав доступа к параметрам функциональных областей Kaspersky Endpoint Security перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center (https://help.kaspersky.com/KSC/11/ru-RU/174017.htm).

Общая информация о задачах в Kaspersky Security Center приводится в документации для Kaspersky Security Center.

Создание локальной задачи

► *Чтобы создать локальную задачу, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите создать локальную задачу.
5. Правой клавишей мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.

   Откроется окно свойств компьютера.
6. Выберите раздел **Задачи**.
7. Нажмите кнопку **Добавить**.

   Запустится мастер создания задачи.
8. Следуйте указаниям мастера создания задачи.

Создание групповой задачи

► *Чтобы создать групповую задачу, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Откройте папку **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center.
3. В рабочей области выберите закладку **Задачи**.
4. Выполните одно из следующих действий:
   - Нажмите кнопку **Создать задачу**.
   - Выберите пункт **Создать →задачу** в контекстном меню Kaspersky Security Center.

   Запустится мастер создания задачи.
5. Следуйте указаниям мастера создания задачи.

Создание задачи для выбора устройства

► *Чтобы создать задачу для выбора устройства, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** в дереве Консоли администрирования.
3. Нажмите на кнопку **Создать задачу**.

   Запустится мастер создания задачи.

4. Следуйте указаниям мастера создания задачи.
5. В окне мастера **Выбор устройств, которым будет назначена задача** нажмите кнопку **Назначить задачу набору устройств**.
6. В следующем окне мастера нажмите кнопку **Выбрать**.

   Откроется окно **Выбор устройства**.
7. Выберите нужное устройство.
8. Нажмите кнопку **ОК** в окне **Выбор устройства**.
9. Следуйте указаниям мастера создания задачи.

Запуск, остановка, приостановка и возобновление выполнения задачи вручную

Если Kaspersky Endpoint Security запущен на компьютере (см. стр. 149), вы можете запускать, останавливать, приостанавливать и возобновлять задачи на этом компьютере с помощью Kaspersky Security Center. Если программа Kaspersky Endpoint Security остановлена, выполнение запущенных задач прекращается, а управлять запуском, остановкой, приостановкой и возобновлением задач через Kaspersky Security Center становится невозможно.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, на котором вы хотите запустить / остановить / приостановить / возобновить выполнение локальной задачи.
5. Выберите пункт **Свойства** в контекстном меню компьютера.

   Откроется окно свойств компьютера.
6. Выберите раздел **Задачи**.

   В правой части окна отобразится список локальных задач.
7. Выберите локальную задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
8. Выполните одно из следующих действий:
   - Правой клавишей мыши откройте контекстное меню локальной задачи. Выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.
   - Нажмите кнопку  справа от списка локальных задач, чтобы запустить или остановить локальную задачу.

- Нажмите кнопку **Свойства** под списком локальных задач. Откроется окно **Свойства задачи <Название задачи>**. Далее на закладке **Общие** окна **Свойства задачи <Название задачи>** нажмите кнопку **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли 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. В списке групповых задач выберите групповую задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
5. Выполните одно из следующих действий:
   - Правой клавишей мыши откройте контекстное меню групповой задачи. Выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.
   - Нажмите кнопку  / справа от списка групповых задач, чтобы запустить или остановить групповую задачу.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Задачи для наборов устройств** дерева консоли выберите задачу для набора компьютеров, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
3. Выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню задачи для набора компьютеров. Выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.
   - Нажмите кнопку  справа от списка задач для наборов компьютеров, чтобы запустить или остановить задачу для набора компьютеров.

Изменение параметров задачи

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите настроить параметры программы.

5. Выполните одно из следующих действий:
   - Правой клавишей мыши откройте контекстное меню компьютера и выберите пункт **Свойства**.
   - В меню Действия выберите пункт Свойства компьютера.

   Откроется окно свойств компьютера.
6. Выберите раздел **Задачи**.

   В правой части окна отобразится список локальных задач.
7. Выберите в списке локальных задач нужную локальную задачу.
8. Выполните одно из следующих действий:
   - Правой клавишей мыши откройте контекстное меню задачи и выберите пункт **Свойства**.
   - Нажмите кнопку **Свойства**.

   Откроется окно Свойства: <Название локальной задачи>.
9. В окне **Свойства: <Название локальной задачи>** выберите раздел Параметры.
10. Измените параметры локальной задачи.
11. В окне **Свойства: <Название локальной задачи>** нажмите кнопку **OK**, чтобы сохранить внесенные изменения.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием нужной группы администрирования.
3. В рабочей области выберите закладку **Задачи**.
4. В нижней части панели задач отобразится список групповых задач.
5. Выберите в списке групповых задач нужную групповую задачу.
6. Выполните одно из следующих действий:
   - Правой клавишей мыши откройте контекстное меню задачи и выберите пункт **Свойства**.
   - Нажмите кнопку **Изменить параметры задачи**, которая находится справа от списка групповых задач.

   Откроется окно **Свойства: <Название групповой задачи>**.
7. В окне **Свойства: <Название групповой задачи>** выберите раздел **Параметры**.
8. Измените параметры групповой задачи.
9. В окне **Свойства: <Название групповой задачи>** нажмите кнопку **OK**, чтобы сохранить внесенные изменения.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Задачи** дерева Консоли администрирования выберите задачу для набора компьютеров, параметры которой вы хотите изменить.
3. Откройте окно **Свойства: <имя политики>** одним из следующих способов:

- В контекстном меню политики выберите пункт **Свойства**.
- Перейдите по ссылке **Настроить политику**, расположенной в правой части рабочей области Консоли администрирования.

4. В окне **Свойства: <Название задачи для набора компьютеров>** выберите раздел **Параметры**.
5. Измените параметры задачи для набора компьютеров.
6. В окне **Свойства: <Название задачи для набора компьютеров>** нажмите кнопку OK, чтобы сохранить внесенные изменения.

Все блоки окна свойств задач, кроме блока **Параметры**, стандартны для программы Kaspersky Security Center. С более подробным описанием вы можете ознакомиться в Справке Kaspersky Security Center. Блок **Параметры** содержит специфические параметры Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux. Содержание этого блока зависит от выбранной задачи и ее типа.

Проверка соединения с Сервером администрирования вручную. Утилита klnagchk

В комплект поставки Агента администрирования входит утилита *klnagchk*, предназначенная для проверки соединения с Сервером администрирования.

После установки Агента администрирования утилита располагается в директории /opt/kaspersky/klnagent/bin. В зависимости от используемых ключей Агент выполняет следующие действия при запуске:

- выводит на экран или заносит в файл журнала событий значения параметров подключения установленного на клиентском компьютере Агента администрирования к Серверу администрирования;
- записывает в файл журнала событий статистику Агента администрирования (с момента последнего запуска данного компонента) и результаты выполнения утилиты либо выводит информацию на экран;
- предпринимает попытку установить соединение Агента администрирования с Сервером администрирования;
- если соединение установить не удалось, посылает ICMP-пакет для проверки статуса компьютера, на котором установлен Сервер администрирования.

Синтаксис утилиты

```
klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>]
[-restart]
```

Описание ключей

- `-logfile <имя файла>` – записывать значения параметров для подключения Агента администрирования к Серверу администрирования и результаты работы утилиты в файл журнала. По умолчанию информация сохраняется в файле stdout.tx. Если этот ключ не используется, параметры, результаты и сообщения об ошибках отображаются на экране.
- `-sp` – показывать пароль для проверки подлинности пользователя на прокси-сервере. Этот параметр используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.

- `-savecert <имя файла>` – сохранить сертификат для аутентификации доступа к Серверу администрирования в указанном файле.
- `-restart` – перезапустить Агент администрирования после завершения утилиты.

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 располагается в директории /opt/kaspersky/klnagent/bin. В зависимости от используемых ключей Агент выполняет следующие действия при запуске:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает результаты выполнения операции в файл журнала событий или выводит их на экран.

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>` – записывать результаты завершения утилиты в указанный файл. Если этот ключ не используется, результаты и сообщения об ошибках отправляются в stdout.
- `-address <адрес сервера>` – адрес Сервера администрирования, используемый для соединения. Это может быть IP-адрес, NetBIOS или DNS-имя компьютера.
- `-pn <номер порта>` – номер порта, по которому будет осуществляться незащищенное подключение к Серверу администрирования. По умолчанию используется порт 14000.
- `-ps <номер SSL-порта>` – номер SSL-порта, по которому будет осуществляться защищенное подключение к Серверу администрирования с использованием протокола 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` – запускать утилиту в неинтерактивном режиме. Использование ключа может быть полезно, например, при запуске утилиты из сценария запуска при регистрации пользователя.
- `-dupfix` – данный ключ используется в случае, если установка Агента администрирования была выполнена не традиционным способом, с использованием дистрибутива, а, например, путем восстановления из образа диска.

Управление программой через Kaspersky Security Center Web Console

Этот раздел содержит информацию об управлении программой Kaspersky Endpoint Security через Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console представляет собой программу (веб-приложение), предназначенную для контроля состояния системы безопасности сетей организации, находящихся под защитой программ "Лаборатории Касперского". *Веб-плагин Kaspersky Endpoint Security*(далее также "веб-плагин") используется для удаленного управления Kaspersky Endpoint Security с помощью Kaspersky Security Center (см. стр. 163).

Kaspersky Security Center Web Console позволяет выполнять следующие действия:

- Контролировать состояние системы безопасности организации.
- Устанавливать и управлять программами "Лаборатории Касперского" на компьютерах в сети.
- Управлять политиками (см. стр. 166) и задачами (см. стр. 169), созданными для компьютеров в вашей сети.
- Просматривать отчеты о состоянии системы безопасности.

Kaspersky Security Center Web Console предоставляет веб-интерфейс, который обеспечивает взаимодействие меду вашим компьютером и Сервером администрирования через браузер. Сервер администрирования – это программа, которая служит для управления программами "Лаборатории Касперского", установленными на компьютеры вашей сети. Сервер администрирования подключается к компьютерам вашей сети через защищенные каналы связи (по протоколу SSL).

Kaspersky Security Center Web Console работает следующим образом:

1. Вы подключаетесь к Kaspersky Security Center Web Console с помощью браузера, в окне которого отображаются страницы веб-портала программы.
2. С помощью элементов управления веб-портала вы выбираете команду, которую требуется выполнить. Kaspersky Security Center Web Console выполняет следующие действия:
   - Если вы выбрали команду, связанную с получением информации (например, просмотр списка устройств), Kaspersky Security Center Web Console формирует запрос на получение информации к Серверу администрирования, затем получает от него необходимые данные и передает их браузеру в удобном для отображения виде.
   - Если вы выбрали команду управления (например, удаленная установка программы), Kaspersky Security Center Web Console получает команду от браузера и передает ее Серверу администрирования. Затем программа получает результат выполнения команды от Сервера администрирования и отображает его в браузере.

Дополнительную информацию о Kaspersky Security Center Web Console см. в документации Kaspersky Security Center.

В этой главе

О веб-плагине Kaspersky Endpoint Security

Веб-плагин представляет собой интерфейс взаимодействия между Kaspersky Security Center Web Console и Kaspersky Endpoint Security. С помощью веб-плагина можно настраивать задачи и политики программы в Kaspersky Security Center Web Console.

Веб-плагин по умолчанию устанавливается в Kaspersky Security Center Web Console. В отличие от плагина управления Kaspersky Endpoint Security для Kaspersky Security Center, который устанавливается на компьютер администратора, веб-плагин устанавливается на компьютер, на котором установлен сервер Web Console. Таким образом, функции веб-плагина Kaspersky Endpoint Security доступны всем администраторам, имеющим доступ к Kaspersky Security Center Web Console в браузере.

Можно просмотреть список установленных веб-плагинов и при необходимости обновить их с помощью интерфейса Kaspersky Security Center Web Console (**Операции** → **Плагины**). Дополнительную информацию о веб-плагине см. в документации Kaspersky Security Center (https://help.kaspersky.com/KSC/11/ru-RU/172510.htm).

Вход и выход из Kaspersky Security Center Web Console

Чтобы войти в Kaspersky Security Center Web Console, необходимо знать веб-адрес Сервера администрирования и номер порта, указанного во время установки (по умолчанию номер порта – 8080) (https://help.kaspersky.com/KSC/11/ru-RU/166765.htm). Необходимо включить JavaScript в браузере.

► *Чтобы войти в Kaspersky Security Center Web Console, выполните следующие действия:*

1. В браузере укажите <веб-адрес Сервера администрирования>:<номер порта>.

   Появится страница входа.

2. Войдите, указав имя пользователя и пароль локального администратора.

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

3. При входе в систему появится информационная панель, где отображается выбранный при последнем входе язык и тема.

   При первом входе в Kaspersky Security Center Web Console в нижней части экрана отображается учебник. Можно выполнить инструкции из учебника или закрыть его, нажав на кнопку закрытия (X).

Можно приступить к работе с Kaspersky Security Center Web Console. Дополнительную информацию об интерфейсе Kaspersky Security Center Web Console см. в документации Kaspersky Security Center (https://help.kaspersky.com/KSC/11/ru-RU/172510.htm).

► *Чтобы выйти из Kaspersky Security Center Web Console, выполните следующие действия:*

1. Щелкните мышью по вашему имени пользователя в верхнем правом углу экрана.
2. В раскрывшемся меню выберите пункт **Выход**.

Kaspersky Security Center Web Console закроется, и появится страница входа.

Просмотр состояния защиты устройства

► *Чтобы просмотреть состояние защиты устройства, выполните следующие действия:*

1. В Kaspersky Security Center Web Console перейдите к списку управляемых устройств (**Устройства** → **Управляемые устройства**).
2. В списке выберите требуемое устройство, чтобы просмотреть о нем подробную информацию.

   Откроется окно с общей информацией о выбранном устройстве.
3. Откройте закладку **Защита** (**Общие** → **Защита**).

На закладке **Защита** отображается следующая информация о выбранном устройстве:

- **Видимость** – видимость выбранного устройства в сети.
- **Статус** – текущий статус выбранного устройства, например, *OK*, *Критический* или *Предупреждение*.
- **Описание статуса** – причины изменения статуса выбранного устройства на *Критический* или *Предупреждение*.

  Статус устройства меняется на *Критический*, если не запущена задача Мониторинг файловых операций.

  Статус устройства меняется на *Предупреждение*, если требуется перезапуск программы или перезагрузка операционной системы. После перезагрузки статус устройства меняется на *OK*.

  Дополнительную информацию об изменении статуса см. в документации Kaspersky Security Center (https://help.kaspersky.com/KSC/SP3/ru-RU/82113.htm).
- **Статус защиты** – состояние задачи Защита от файловых угроз, например: *Выполняется*, *Остановлена*, *Приостановлена*.
- **Последняя полная проверка** – дата и время последнего выполнения задачи полной проверки на выбранном устройстве.
- **Обнаружено вирусов** – общее количество вредоносных объектов, обнаруженных на выбранном устройстве (счетчик обнаруженных угроз) с момента установки Kaspersky Endpoint Security.
- **Объекты, которые не удалось вылечить** – количество зараженных объектов, которые программе Kaspersky Endpoint Security не удалось вылечить.

Активация Kaspersky Endpoint Security

Программу можно активировать удаленно с помощью интерфейса Kaspersky Security Center Web Console следующим способом:

- С помощью задачи *Добавление ключа*.

  Этот способ позволит добавить ключ для определенного компьютера или группы компьютеров.

- С помощью распространения на компьютеры ключей из хранилища ключей Сервера администрирования Kaspersky Security Center.

  Этот способ позволяет автоматически добавлять ключи на компьютеры, уже подключенные к Kaspersky Security Center, и на новые компьютеры. Для использования этого способа добавьте ключ в хранилище ключей Сервера администрирования Kaspersky Security Center. Дополнительную информацию о добавлении ключей в хранилище ключей Сервера администрирования Kaspersky Security Center см. в документации Kaspersky Security Center.

► *Чтобы активировать программу с помощью задачи Добавление ключа, выполните следующие действия:*

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

   Откроется таблица задач.

2. Нажмите кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настроить параметры задачи:
   - В раскрывающемся списке **Программа** выберите Kaspersky Endpoint Security.
   - В списке **Тип задачи** выберите **Добавление ключа**.
   - В поле **Название задачи** укажите название задачи.
   - В разделе **Устройства, которым будет назначена задача** выберите область действия задачи.
4. Выберите устройства в соответствии с выбранной областью действия задачи.
5. Нажмите на кнопку **Далее**.
6. Завершите работу мастера, нажав на кнопку **Создать**.

   Новая задача появится в таблице задач.

7. Выберите задачу **Добавление ключа** программы Kaspersky Endpoint Security.

   Откроется окно свойств задачи.

8. Перейдите на закладку **Параметры программы**.
9. В разделе **Тип ключа** выберите способ активации: с помощью кода активации или файла ключа.
10. Нажмите на кнопку **Выбрать ключ**.

    Появится список ключей, хранящихся в хранилище ключей Сервера администрирования Kaspersky Security Center.

11. Выберите файл ключа или код активации и нажмите на кнопку **OK**.
12. С помощью флажка **Добавить ключ в качестве дополнительного** можно добавить на компьютер дополнительный ключ. Дополнительный ключ становится активным, когда истекает срок действия активного ключа, или если активный ключ удален. Наличие дополнительного ключа позволяет

избежать ограничений функциональных возможностей программы после истечения срока действия активного ключа.

13. Нажмите на кнопку **Сохранить**.

Новая задача появится в списке задач. Чтобы запустить задачу, установите флажок рядом с названием задачи и нажмите на кнопку **Запустить**.

► *Чтобы активировать программу с помощью распространения на компьютеры ключа из хранилища ключей Сервера администрирования, выполните следующие действия:*

1. В главном окне Web Console выберите **Операции** → **Лицензирование** → **Лицензии "Лаборатория Касперского"**.
2. Откройте свойства ключа, щелкнув мышью по названию программного решения, к которому относится ключ.
3. Включите переключатель **Распространять ключ автоматически**.

В результате ключ будет автоматически распространен на соответствующие компьютеры. Во время автоматического распространения ключа в качестве активного или дополнительного учитывается лицензионное ограничение на количество компьютеров (заданное в свойствах ключа). При достижении лицензионного ограничения распространение ключа на компьютеры прекращается автоматически. Количество компьютеров, на которые был добавлен ключ, а также другие данные можно посмотреть в свойствах ключа на закладке **Устройства**.

Управление политиками

Политика – это набор параметров программы, указанных для группы администрирования (см. стр. 192). Политика определяет не все параметры программы.

Для одной программы можно настроить несколько политик с различными значениями параметров. Однако в каждый момент времени для программы в группе администрирования может быть только одна активная политика.

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

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

Возможность изменять параметр программы на клиентском компьютере определяется статусом "замка" у параметра в политике:

- Если параметр закрыт "замком» (), это означает, что вы не можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используется значение параметра, заданное политикой.
- Если параметр не закрыт "замком" (), это означает, что вы можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используются значения параметра, установленные локально. Значение параметра, установленное в политике, не применяется.

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

Вы можете использовать политики для настройки параметров таких задач Kaspersky Endpoint Security, как Защита от файловых угроз, Управление сетевым экраном, Защита от шифрования, Мониторинг файловых операций при доступе и Хранилища.

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

Вы можете выполнять следующие действия над политикой:

- Создавать политику.
- Изменять параметры политики.

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

- Удалять политику.
- Изменять состояние политики.

Дополнительную информацию о политиках см. в документации Kaspersky Security Center.

Создание политики

► *Чтобы создать политику, выполните следующие действия:*

1. В главном окне Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Политики и профили**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Выбор программы**.
3. Выберите **Kaspersky Endpoint Security 10 SP1 MR1 для Linux** и нажмите на кнопку **Далее**.
4. Прочитайте положение о Kaspersky Security Network и выполните одно из следующих действий:
   - Выберите **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия настоящего KSN**, чтобы включить Kaspersky Security Network на компьютерах, контролируемых создаваемой политикой.
   - Выберите **Я не принимаю условия настоящего Положения о Kaspersky Security Network**, чтобы отключить Kaspersky Security Network на компьютерах, контролируемых создаваемой политикой.

   Отказ от участия в Kaspersky Security Network не прерывает процесс создания политики. В параметрах политики можно в любое время включить, отключить или изменить режим Kaspersky Security Network для управляемых компьютеров.
5. Нажмите на кнопку **Далее**.

   Откроется окно параметров создаваемой политики на закладке **Общие**.

6. На закладке **Общие** можно настроить следующие параметры политики:
   - Заданное по умолчанию имя политики.
   - Статус политики:
     - **Активная политика**. При следующей синхронизации компьютера с Сервером администрирования политика будет использоваться в качестве активной на компьютере.
     - **Неактивная политика**. Дополнительная политика, не используемая в данный момент. При необходимости неактивную политику можно активировать.
     - **Политика для автономных пользователей**. Политика, которая становится активной, когда компьютер покидает корпоративную сеть.

     По умолчанию выбран вариант **Активная политика**.
   - Параметры наследования политики:
     - **Наследовать параметры родительской политики**. Если выбран этот вариант, значения параметров политики наследуются из групповой политики верхнего уровня, и, следовательно, недоступны для изменения. По умолчанию параметр включен.
     - **Принудительное наследование параметров в дочерних политиках**. Если выбран этот параметр, параметры дочерних политик недоступны для изменения. По умолчанию этот параметр отключен.

   Дополнительную информацию о параметрах политики см. в документации Kaspersky Security Center.
7. На закладке **Параметры программы** можно изменить параметры Kaspersky Endpoint Security.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить политику.

Созданная политика появится в списке политик. Параметры политики можно изменить позже. Дополнительную информацию об управлении политиками см. в документации Kaspersky Security Center (https://help.kaspersky.com/KSC/11/ru-RU/172510.htm).

Изменение параметров политики

► *Чтобы изменить параметры политики, выполните следующие действия:*

1. В главном окне Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Политики и профили**.
2. В списке политик щелкните мышью по названию политики, параметры которой требуется изменить.

   Параметры политики для Kaspersky Endpoint Security включают параметры задач и общие параметры программы. Раздел **Основная защита от угроз** содержит параметры задач Защита от файловых угроз и Управление сетевым экраном, а также исключения из области проверки. Раздел **Дополнительная защита от угроз** содержит параметры Kaspersky Security Network, а также параметры задач Защита от шифрования и Мониторинг файловых операций. В разделе **Общие параметры** содержатся параметры прокси-сервера, программы и Хранилища.

   Дополнительную информацию об общих параметрах политики см. в документации Kaspersky Security Center (https://help.kaspersky.com/KSC/11/ru-RU/177410.htm).
3. Измените параметры политики.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Политика будет сохранена с обновленными значениями параметров.

Управление задачами

Kaspersky Security Center Web Console управляет работой программы Kaspersky Endpoint Security, установленного на компьютерах, с помощью задач. Задачи реализуют основные функции управления, например: добавление ключа, проверку объектов, обновление баз и модулей программы.

При работе с Kaspersky Endpoint Security через Kaspersky Security Center Web Console вы можете создавать следующие типы задач:

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

> Задачи для наборов компьютеров, не входящих в группы администрирования, выполняются только для указанных в параметрах задачи компьютеров. Если в набор компьютеров, для которого сформирована задача, добавлены новые компьютеры, то для них эта задача не выполняется. В этом случае вам необходимо создать новую задачу или изменить параметры уже существующей задачи.

Вы можете создавать задачи следующих типов:

- **Обновление**. В процессе выполнения задачи Kaspersky Endpoint Security обновляет антивирусные базы в соответствии с установленными параметрами обновления.
- **Откат обновления**. В процессе выполнения задачи Kaspersky Endpoint Security откатывает последнее обновление антивирусных баз.
- **Копирование обновления**. В процессе выполнения задачи Kaspersky Endpoint Security скачивает антивирусные базы в указанную директорию, не устанавливая их.
- **Антивирусная проверка**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи.
- **Проверка загрузочных секторов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет загрузочные сектора компьютера.
- **Проверка памяти процессов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет системную память компьютера.
- **Добавление ключа**. В процессе выполнения задачи Kaspersky Endpoint Security добавляет ключ, в том числе дополнительный, для активации программы.
- **Проверка целостности файлов по требованию**. В ходе выполнения этой задачи изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.

Вы можете выполнять следующие действия над задачами:

- создавать новые задачи (см. стр. 170).
- изменять параметры задач (см. стр. 170).
- управлять задачами (см. стр. 170).

Права на доступ к параметрам задач Kaspersky Endpoint Security (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через

параметры доступа к функциональным областям Kaspersky Endpoint Security. Для настройки прав доступа к параметрам функциональных областей Kaspersky Endpoint Security перейдите в раздел Безопасность окна свойств Сервера администрирования Kaspersky Security Center.

Общая информация о задачах в Kaspersky Security Center Web Console приводится в документации для Kaspersky Security Center.

Создание задачи

► *Чтобы создать задачу, выполните следующие действия:*

1. В главном окне Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится **Мастер создания задачи**.
3. В раскрывающемся списке **Программа** выберите Kaspersky Endpoint Security SP1 MR1 и следуйте инструкциям мастера.
4. Если на странице **Завершение создания задачи** вы выбрали **Перейти к параметрам задачи после ее создания**, можно изменить параметры задачи, заданные по умолчанию. Если этот параметр не был выбран, задача будет создана с параметрами по умолчанию. Заданные по умолчанию параметры можно будет изменить позже, в любое время.
5. Нажмите на кнопку **Создать**.

Задача создана и появилась в списке задач.

Изменение параметров задачи

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

1. В главном окне Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Задачи**.
2. В списке задач щелкните мышью по названию задачи, параметры которой требуется изменить.
3. Измените параметры задачи.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Задача будет сохранена с обновленными значениями параметров.

Управление задачами

► *Чтобы запустить, приостановить, возобновить, остановить, удалить, скопировать или переместить задачу, выполните следующие действия:*

1. В главном окне Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Задачи**.
2. В списке задач выберите задачи, которые требуется запустить, приостановить, возобновить, остановить, удалить, скопировать или переместить, и нажмите на соответствующую кнопку.

Использование графического пользовательского интерфейса Kaspersky Endpoint Security

В этом разделе описана работа в Kaspersky Endpoint Security с использованием графического пользовательского интерфейса.

В этой главе

Локальное включение и выключение графического пользовательского интерфейса

Вы можете включить или выключить графический пользовательский интерфейс Kaspersky Endpoint Security локально с помощью командной строки.

Пользователи без root-прав не могут запустить графический пользовательский интерфейс, если в конфигурационном файле первоначальной настройки Kaspersky Endpoint Security указано значение параметра `USE_GUI=no` (см. стр. 36).
Для включения и выключения графического пользовательского интерфейса требуются root-права.

► *Чтобы включить или выключить графический пользовательский интерфейс, выполните следующие действия:*

1. Запустите конфигурационный скрипт программы:

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

   Отобразится сообщение с вопросом.

2. Выполните одно из следующих действий:

   - Если вы хотите включить графический пользовательский интерфейс, введите `Y`.

Если вы включите графический пользовательский интерфейс, пользователи без root-прав смогут запускать задачи антивирусной проверки.

Если пользователь вошел в систему, для него будет запущен графический пользовательский интерфейс, если доступны все необходимые библиотеки. Значок программы появляется в области уведомлений панели задач, и создается ярлык.

- Если вы хотите отключить графический пользовательский интерфейс, введите `N`.

  Программа запрещает пользователям запускать графический пользовательский интерфейс. Значок программы и ярлык удаляются.

Интерфейс программы

Этот раздел содержит информацию об основных элементах графического пользовательского интерфейса программы.

Значок программы в области уведомлений

После включения графического пользовательского интерфейса Kaspersky Endpoint Security значок программы появляется в области уведомлений справа на панели задач.

Значок обеспечивает доступ к контекстному меню и главному окну программы.

Контекстное меню значка программы содержит следующие пункты:

- **Kaspersky Endpoint Security 10 SP1 MR1 для Linux** Открывает главное окно программы. В главном окне программы отображается состояние защиты вашего компьютера, а также состояние задач антивирусной проверки и обновлений. Вы также можете перейти в окно **Отчеты**, **Хранилище**, **Параметры** или **Поддержка**.
- **Выход**. Выход из графического пользовательского интерфейса Kaspersky Endpoint Security.

Вы можете открыть контекстное меню значка программы, щелкнув правой кнопкой мыши по значку программы в области уведомлений.

Главное окно программы

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

Главное окно программы разделено на несколько частей.

- В центральной части окна отображается статус защиты вашего компьютера. Если щелкнуть эту часть главного окна, откроется окно **Центр защиты**.
- На закладке **Проверка** отображается состояние задачи антивирусной проверки и количество обнаруженных угроз. Закладка позволяет перейти в окно **Проверка**. В этом окне можно запустить и остановить задачи антивирусной проверки, проверки загрузочных секторов и проверки памяти процессов. Вы также можете просмотреть отчеты для этих задач.

- На вкладке **Обновление** отображается состояние задачи обновления и антивирусных баз. Закладка позволяет перейти в окно **Обновление**. В этом окне можно запустить или остановить задачи обновления или копирования обновлений. Вы также можете просмотреть отчеты для этих задач.
- В нижней части главного окна программы представлены следующие элементы:
  - Кнопка **Отчеты**. При нажатии этой кнопки открывается окно **Отчеты**, где вы можете просмотреть статистику задач и различные отчеты.
  - Кнопка **Хранилище**. При нажатии этой кнопки открывается окно **Хранилище**, которое содержит информацию об объектах в Хранилище.
  - Кнопка **Параметры**. При нажатии этой кнопки открывается окно Параметры, где можно включить или выключить участие в Kaspersky Security Network, а также задачи Защита от файловых угроз, Управление сетевым экраном, Защита от шифрования и Мониторинг файловых операций.
  - Кнопка **Поддержка**. При нажатии этой кнопки открывается окно **Поддержка**, в котором содержится информация о текущей версии Kaspersky Endpoint Security, лицензиях, статусе ключа, статусе баз, операционной системе, а также ссылки на информационные ресурсы "Лаборатории Касперского".

► *Открыть главное окно Kaspersky Endpoint Security можно одним из следующих способов:*

- Дважды щелкните или щелкните правой кнопкой мыши значок программы в области уведомлений панели задач.
- Щелкните правой кнопкой мыши программу и выберите **Kaspersky Endpoint Security 10 SP1 MR1 для Linux**.

Управление задачами и компонентами

По умолчанию графический пользовательский интерфейс Kaspersky Endpoint Security позволяет вам запускать и останавливать следующие задачи:

- Задача полной проверки (Scan_My_Computer).
- Задачи антивирусной проверки (Scan_File, Boot_Scan, Memory_Scan).
- Задачи обновления (обновление, откат обновления баз, копирование обновлений).

Графический пользовательский интерфейс Kaspersky Endpoint Security также позволяет вам включать и выключать следующие компоненты:

- Защита от файловых угроз
- Управление сетевым экраном
- Защита от шифрования
- Мониторинг файловых операций

Кроме того, вы можете управлять своим участием в Kaspersky Security Network (см. стр. 175).

Запуск и остановка задач проверки

С помощью графического пользовательского интерфейса Kaspersky Endpoint Security вы можете запускать и останавливать задачи полной проверки, антивирусной проверки, проверки загрузочных секторов и проверки памяти процессов.

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

1. Откройте главное окно программы. (см. стр. 172).
2. Кнопкой **Проверка**, расположенной в главном окне программы, откройте окно **Проверка**.
3. Выполните одно из следующих действий:
   - Если вы хотите запустить задачу, нажмите кнопку **Запустить** под той задачей, которую вы хотите запустить.

     Отображается ход выполнения задачи.
   - Если вы хотите остановить задачу, нажмите кнопку **Остановить** под той задачей проверки, которую вы хотите остановить.

     Задача проверки останавливается, и отображается информация о проверенных объектах и обнаруженных угрозах.
4. При необходимости вы можете нажать кнопку **Показать отчет**, чтобы просмотреть отчет по задаче.

   Окно **Отчеты** доступно для пользователей без root-прав, только если для общего параметра программы `UIReportsForRootOnly` выбрано значение `No`. В других случаях окно **Отчеты** доступно только пользователям с root-правами.

Запуск и остановка задач обновления

С помощью графического пользовательского интерфейса вы можете запускать и останавливать такие задачи, как Обновление, Откат обновления и Копирование обновлений.

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

1. Откройте главное окно программы. (см. стр. 172).
2. Кнопкой **Обновить**, расположенной в главном окне программы, откройте окно **Обновление**.
3. Выполните одно из следующих действий:
   - Если вы хотите запустить задачу, нажмите кнопку **Запустить** под той задачей, которую вы хотите запустить.

     Отображается ход выполнения задачи.

     При успешном завершении задачи обновления становится доступна ссылка **Откат обновления**, с помощью которой вы можете откатить последнее обновление.
   - Если вы хотите остановить задачу, нажмите кнопку **Остановить** под той задачей, которую вы хотите остановить.

     Задача будет остановлена.

4. При необходимости вы можете нажать кнопку **Показать отчет**, чтобы просмотреть отчет по задаче.

   Окно **Отчеты** доступно для пользователей без root-прав, только если для общего параметра программы `UIReportsForRootOnly` выбрано значение `No`. В других случаях окно **Отчеты** доступно только пользователям с root-правами.

► *Чтобы запустить задачу отката обновления, выполните следующие действия:*

1. Откройте главное окно программы. (см. стр. 172).
2. Кнопкой **Обновить**, расположенной в главном окне программы, откройте окно **Обновление**.
3. В блоке **Обновление** перейдите по ссылке **Откат обновления**, чтобы откатить последнее успешное обновление баз.

Включение и выключение компонентов программы

С помощью графического пользовательского интерфейса Kaspersky Endpoint Security вы можете в любой момент включить или выключить следующие компоненты программы: Защита от файловых угроз, Управление сетевым экраном, Защита от шифрования и Мониторинг файловых операций. .

Если компонент включен, доступна кнопка **Выключить**. По умолчанию включен только компонент Защита от файловых угроз.

Если компонент выключен, доступна кнопка **Включить**.

► *Чтобы включить или выключить компонент, выполните следующие действия:*

1. Откройте главное окно программы. (см. стр. 172).
2. В нижней части главного окна программы нажмите кнопку **Параметры**.

   Откроется окно **Параметры**.
3. В окне **Параметры** выполните следующие действия для нужного компонента:
   - Если вы хотите включить компонент, нажмите кнопку **Включить**.
   - Если вы хотите выключить компонент, нажмите кнопку **Выключить**.

Управление участием в Kaspersky Security Network

Вы можете управлять своим участием в Kaspersky Security Network в любой момент.

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

1. Откройте главное окно программы. (см. стр. 172).
2. В нижней части главного окна программы нажмите кнопку **Параметры**.

   Откроется окно **Параметры**.
3. В окне **Параметры** выберите один из следующих вариантов:

- **Kaspersky Security Network со статистикой** – чтобы включить Kaspersky Security Network, получать информацию из базы знаний и отправлять анонимную статистику и данные о типах и источниках новых угроз.
- **Kaspersky Security Network баз статистики** – чтобы получать информацию из базы знаний, но не отправлять анонимную статистику и данные о типах и источниках новых угроз.

4. Нажмите кнопку **Включить**.
5. В окне **Участие в Kaspersky Security Network** внимательно прочитайте Положение о Kaspersky Security Network и выберите один из следующих вариантов:
   - **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия настоящего Положения о Kaspersky Security Network** – чтобы включить Kaspersky Security Network.
   - **Я не принимаю условия настоящего Положения о Kaspersky Security Network** – чтобы выключить использование Kaspersky Security Network.
6. Нажмите кнопку **ОК**.

   Кнопка **ОК** недоступна, если выбран вариант **Не выбрано**.

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

1. Откройте главное окно программы. (см. стр. 172).
2. В нижней части главного окна программы нажмите кнопку **Параметры**.

   Откроется окно **Параметры**.
3. В окне **Параметры** нажмите кнопку **Выключить**.
4. В открывшемся окне выполните одно из следующих действий:
   - Нажмите **Да**, чтобы подтвердить выключение Kaspersky Security Network.
   - Нажмите **Отмена**, чтобы продолжать участвовать в Kaspersky Security Network.

Отчеты

В этом разделе содержится информация о том, как просматривать отчеты в графическом пользовательском интерфейсе Kaspersky Endpoint Security.

Принципы работы с отчетами

Окно **Отчеты** доступно для пользователей без root-прав, только если для общего параметра программы `UIReportsForRootOnly` выбрано значение `No`. В других случаях окно **Отчеты** доступно только пользователям с root-правами.

Информация о производительности задач Kaspersky Endpoint Security регистрируется в отчетах.

Данные в отчете представлены в виде таблицы, которая содержит список событий. Каждая строка в таблице содержит информацию об отдельном событии. Атрибуты события расположены в графах таблицы. События, зарегистрированные в работе разных задач, имеют разный набор атрибутов.

Доступны следующие отчеты, перечисленные в меню слева:

- **Статистика**. Содержит статистические данные о задаче Защита от файловых угроз и задачах антивирусной проверки. Вы можете обновить отображаемый отчет, нажав кнопку **Обновить**.

  При остановке задачи Защита от файловых угроз происходит сброс статистики. Сброса статистики для задач антивирусной проверки не происходит. Вместо этого статистика накапливается за время, пока программа установлена на компьютере.

- **Системный аудит**. Этот отчет содержит информацию о событиях, которые произошли во время взаимодействия пользователя с программой. Он также содержит информацию о событиях, которые произошли во время обычной работы программы.

- **Защита от угроз**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы следующих компонентов Kaspersky Endpoint Security:

  - Защита от шифрования
  - Мониторинг файловых операций
  - Управление сетевым экраном
  - Файловый Антивирус

- **Задачи проверки по требованию**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы следующих задач Kaspersky Endpoint Security:

  - Задачи проверки
  - Обновление
  - Проверка целостности

В отчетах применяются следующие уровни важности событий:

- **Информационные события**. События справочного характера, как правило, не содержащие важной информации.
- **Важные события**. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе Kaspersky Endpoint Security.
- **Критические события**. События критической важности, указывающие на проблемы в работе Kaspersky Endpoint Security или на уязвимости в защите компьютера пользователя.

Для удобства работы с отчетами вы можете изменять представление данных на экране следующими способами:

- отфильтровать список событий по времени;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке;

Просмотр отчетов

Окно **Отчеты** доступно для пользователей без root-прав, только если для общего параметра программы `UIReportsForRootOnly` выбрано значение `No`. В других случаях окно **Отчеты** доступно только пользователям с root-правами.

► *Чтобы просмотреть отчеты, выполните следующие действия:*

1. Откройте главное окно программы. (см. стр. 172).
2. В нижней части главного окна программы нажмите кнопку **Отчеты**.

   Откроется окно **Отчеты**.
3. Чтобы просмотреть конкретный отчет, в левой части окна **Отчеты** выберите нужную задачу из списка задач.

   В правой части окна отобразится отчет, содержащий список событий о работе выбранной задачи Kaspersky Endpoint Security.

   По умолчанию события в отчете отсортированы по возрастанию значений графы **Дата**. Вы можете выбрать другой порядок, щелкнув заголовок нужной графы.
4. Чтобы просмотреть в отчете подробную сводную информацию о каждом событии, выберите соответствующее событие в отчете.

   Блок со сводной информацией о событии отображается в нижней части окна.

Просмотр объектов в Хранилище

► *Чтобы просмотреть объекты, которые Kaspersky Endpoint Security переместил в Хранилище, выполните следующие действия:*

1. Откройте главное окно программы. (см. стр. 172).
2. Нажмите кнопку **Хранилище**.

   В открывшемся окне отображается информация об объектах в Хранилище.

Вы можете просмотреть следующую информацию об объектах в Хранилище:

- название угрозы;
- полный путь к объекту;
- дата перемещения объекта в Хранилище;
- дата удаления объекта из Хранилища. Это поле отображается, если указан параметр `DaysToLive`;
- размер объекта.

Вы можете восстановить объекты из Хранилища в их оригинальные директории. Вы также можете удалить объекты из Хранилища. Удаленные объекты восстановить невозможно. Информация об этих действиях записывается в журнал событий.

Создание файла трассировки

► *Чтобы создать файл трассировки, выполните следующие действия:*

1. Откройте главное окно программы (см. стр. 172).
2. Нажмите кнопку **Поддержка**.
3. В окне **Поддержка** перейдите по ссылке **Трассировка**.

4. В раскрывающемся списке **Уровень** выберите уровень трассировки.

   Рекомендуется уточнить необходимый уровень трассировки у специалиста из Службы технической поддержки «Лаборатории Касперского». По умолчанию для уровня трассировки установлено значение **Диагностика (300)**.

5. Чтобы начать процесс трассировки, нажмите кнопку **Включить**.
6. Чтобы остановить процесс трассировки, нажмите кнопку **Выключить**.

Созданные файлы трассировки хранятся в директории /var/log/kaspersky/kesl/.

Устранение уязвимостей и установка критических обновлений в программе

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

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

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

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- На форуме "Лаборатории Касперского" (http://forum.kaspersky.com).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки".

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этой главе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского". Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить по телефону. Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной или интернациональной Службы технической поддержки.
- Отправить запрос с портала My Kaspersky. Этот метод позволяет вам связаться с нашими специалистами с помощью формы запроса.

Техническая поддержка доступна только пользователям, которые приобрели лицензию на использование программы. Техническая поддержка не предоставляется пользователям, использующим пробные версии.

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки Лаборатории Касперского. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2c#region3).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. Вы можете использовать Kaspersky CompanyAccount для отслеживания статуса ваших онлайн-запросов и хранения их истории.

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).

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

В этой главе

Конфигурационные файлы задачи по умолчанию

Этот раздел содержит информацию о конфигурационных файлах по умолчанию для задач Kaspersky Endpoint Security.

Конфигурационные файлы можно изменить в любой момент. Вы также можете изменить значения параметров из командной строки.

Правила редактирования конфигурационных файлов Kaspersky Endpoint Security

При редактировании конфигурационного файла соблюдайте следующие правила:

- В конфигурационном файле необходимо указать все обязательные параметры. Отдельные параметры задачи можно указать без файла, с помощью командной строки.
- Если параметр принадлежит к какой-либо секции, помещайте его только в этой секции. В пределах одной секции вы можете помещать параметры в любом порядке.
- Заключайте имена секций в квадратные скобки [ ].
- Вводите значения параметров в формате имя параметра=значение (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
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 Антивирусная проверка

```
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
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Выборочная проверка

```
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
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Проверка загрузочных секторов

```
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
Action=Cure
```

Конфигурационный файл задачи Проверка памяти процессов

```
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportUnprocessedObjects=No
Action=Cure
```

Конфигурационный файл задачи Обновление

```
SourceType="KLServers"
UseKLServersWhenUnavailable=Yes
IgnoreProxySettingsForKLServers=No
IgnoreProxySettingsForCustomSources=No
ApplicationUpdateMode=Disabled
ConnectionTimeout=10
```

Конфигурационный файл задачи Копирование обновлений

```
SourceType=KLServers
UseKLServersWhenUnavailable=Yes
ConnectionTimeout=10
ApplicationUpdateMode=Disabled
```

Конфигурационный файл задачи Управление Хранилищем

```
DaysToLive=90
BackupSizeLimit=0
BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

Конфигурационный файл задачи Управление сетевым экраном

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

[NetworkZonesTrusted]
```

```
[NetworkZonesLocal]

[NetworkZonesPublic]
```

Конфигурационный файл задачи Мониторинг файловых операций

```
UseExcludeMasks=No
[ScanScope.item_0000]
AreaDesc=Kaspersky internal objects
UseScanArea=Yes
Path=/opt/kaspersky/kesl/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Защита от шифрования

```
UseHostBlocker=yes
BlockTime=30
UseExcludeMasks=no
[ScanScope.item_0000]
AreaDesc=AllSharedFolders
UseScanArea=yes
Path=AllShared
AreaMask.item_0000=*
```

Настройка совместной работы: Антивирус Касперского для Linux Mail Server

► *Чтобы настроить совместную работу Kaspersky Endpoint Security 10 с Антивирусом Касперского для Linux Mail Server, выполните следующие действия:*

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

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

2. Откройте созданный конфигурационный файл для редактирования.
3. Добавьте в созданный файл следующий блок:

   ```
   [ExcludedFromScanScope.item_#]

   Path=</var/opt/kaspersky/klms>
   ```

4. Повторите указанный выше блок для всех почтовых агентов, интегрированных с Антивирусом Касперского для Linux Mail Server.
5. Для исключения из проверки временной директории фильтров и служб Антивируса Касперского для Linux Mail Server добавьте в созданный файл следующую секцию:

   ```
   [ExcludedFromScanScope.item_#]

   Path=/tmp/klmstmp
   ```

6. Сохраните изменения в конфигурационном файле.
7. Импортируйте параметры из конфигурационного файла в задачу Защита от файловых угроз с помощью следующей команды:

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

Коды возврата командной строки

В этом разделе приведено описание кодов возврата командной строки.

0 – команда / задача выполнена успешно;

1 – общая ошибка в аргументах команды;

2 – ошибка в переданных настройках программы;

64 – Kaspersky Endpoint Security не запущен;

66 – антивирусные базы 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 программа работает под политикой;

128 – неизвестная ошибка;

65 – все остальные ошибки.

Значения параметров программы в сертифицированном состоянии

Этот раздел содержит перечень параметров программы, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии.

Если вы меняете какие-либо из перечисленных параметров с их значений в сертифицированном состоянии на другие значения, вы выводите программу из сертифицированного состояния.

Таблица 3. Параметры и их значения для программы в сертифицированном состоянии

Название параметра	Сущность, к которой относится параметр	Значение параметра в сертифицированном состоянии программы
`FirstAction`	Задача постоянной проверки, задача проверки по требованию	Одно из следующих значений: • `Cure` – программа пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно, программа оставляет объект неизменным. • `Remove` – программа удаляет зараженный объект, предварительно создав его резервную копию.
`SecondAction`	Задача постоянной проверки, задача проверки по требованию	Если значение `FirstAction=Cure`: • `Remove` – программа удаляет зараженный объект, предварительно создав его резервную копию.
`UseAnalyzer`	Задача постоянной проверки, задача проверки по требованию, задача проверки загрузочных секторов	`Yes` – эвристический анализатор включен.

Название параметра	Сущность, к которой относится параметр	Значение параметра в сертифицированном состоянии программы
HeuristicLevel	Задача постоянной проверки, задача проверки по требованию, задача проверки загрузочных секторов	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 постоянной проверки, задача проверки по требованию	Yes – проверять архивы.
ScanSfxArchived	Задача постоянной проверки, задача проверки по требованию	Yes – проверять самораспаковывающиеся архивы.
ScanMailBases	Задача постоянной проверки, задача проверки по требованию	Yes – проверять файлы почтовых баз.
ScanPacked	Задача постоянной проверки, задача проверки по требованию	Yes – проверять упакованные файлы.
ApplicationUpdateMode	Задача обновления, задача отката обновлений	Disabled – не загружать и не устанавливать обновления программы.
UIReportsForRootOnly	Общие параметры Kaspersky Endpoint Security	Yes – разрешить просмотр отчетов из графического пользовательского интерфейса только пользователю с root-правами.

Глоссарий

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать вредоносный код в проверяемых объектах. Антивирусные базы создаются специалистами "Лаборатории Касперского" и обновляются каждый час.

Группа администрирования

Набор компьютеров, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Компьютеры группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Групповые политики и групповые задачи можно создать для каждой установленной программы в группе.

Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех клиентских компьютерах, входящих в состав этой группы администрирования.

Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

Задача

Операции в программе "Лаборатории Касперского" реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз программы.

Задача для конкретных устройств

Задача, назначенная набору клиентских компьютеров из произвольной группы администрирования и выполняемая на этих компьютерах.

Зараженный объект

Объект, часть кода которого полностью совпадает с частью кода известной вредоносной программы. "Лаборатория Касперского" не рекомендует открывать такие объекты.

Исключение

Объект, исключенный из проверки программой "Лаборатории Касперского". Вы можете исключить из проверки файлы определенных форматов, маски файлов, определенную область (например, папку или программу), процесс программы или объект по типу угрозы, согласно классификации Вирусной энциклопедии. Для каждой задачи можно назначить набор исключений.

Код активации

Код, который вы получаете при приобретении лицензии Kaspersky Endpoint Security. Этот код необходим для активации программы.

Код активации представляет собой последовательность из 20 букв и цифр в формате xxxxx-xxxxx-xxxxx-xxxxx.

Лечение

Способ обработки зараженных объектов, в результате которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, предоставляемый "Лабораторией Касперского" вместе с файлом ключа или кодом активации. Этот документ содержит информацию о предоставляемой лицензии.

Лицензия

Ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Маска файла

Представление имени файла с подстановочными знаками. Стандартными подстановочными символами в масках файлов являются * и ?, где * – любое количество символов, а ? – любой отдельный символ.

Обновление

Функция программы "Лаборатории Касперского", позволяющая ей поддерживать защиту компьютера в актуальном состоянии. Во время обновления программа загружает обновления для своих баз и модулей с серверов обновлений "Лаборатории Касперского", а затем автоматически устанавливает и применяет их.

Параметры задачи

Параметры программы, специфические для каждого типа задачи.

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры Хранилища.

Плагин управления программой

Специализированный компонент, который обеспечивает интерфейс для управления программой через Консоль администрирования. У каждой программы есть собственный плагин. Он включен во все программы "Лаборатории Касперского", которыми можно управлять через Kaspersky Endpoint Security.

Подписка

Позволяет эксплуатировать программу согласно выбранным характеристикам (таким как дата окончания срока действия или количество устройств). Подписку можно приостановить или возобновить, автоматически продлить или отменить.

Политика

Политика определяет параметры программы и управляет доступом к настройке программы, установленной на компьютерах в рамках группы администрирования. Для каждой программы необходимо создавать отдельную политику. Вы можете создать неограниченное количество различных политик для программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

Постоянная защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект (на чтение, запись и исполнение) и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, а объекты с угрозами или предположительно зараженные объекты обрабатываются в соответствии с параметрами задачи (лечатся, удаляются или помещаются на карантин).

Потенциально заражаемый объект

Объект, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например с расширением .com, .exe или .dll. Риск проникновения вредоносного кода в такие файлы весьма высок.

Прокси-сервер

Служба в компьютерных сетях, через которую пользователи могут выполнять косвенные запросы к другим сетевым службам. Сначала пользователь подключается к прокси-серверу и запрашивает ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос пользователя или ответ сервера может быть изменен прокси-сервером в определенных целях.

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского". Его также можно использовать для управления этими программами.

Серверы обновлений "Лаборатории Касперского"

HTTP- и FTP-серверы "Лаборатории Касперского", с которых программа загружает обновления баз на мобильные устройства.

Хранилище

Специальное хранилище для резервных копий файлов, которые создаются перед попыткой лечения или удаления.

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем защиты компьютеров от цифровых угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности для конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей (IDC Endpoint Tracker 2014).

"Лаборатория Касперского" основана в России в 1997 году. Она выросла в международную группу компаний с 38 офисами в 33 странах. В компании работают более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, отвечающие за безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файлов и веб-серверов, почтовых шлюзов и сетевых экранов. Ассортимент компании также включает продукты, специально созданные для защиты от DDoS-атак, защиты промышленных систем управления и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту от компьютерных угроз организации любого размера. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства для их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Kaspersky Endpoint Security используют в своих продуктах многие другие разработчики программ: среди них Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu и ZyXEL. Многие инновационные технологии компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. По результатам тестов и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives в 2014 году, "Лаборатория Касперского" по количеству сертификатов Advanced+ стала одним из двух ведущих поставщиков и наконец получила сертификат Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей, а число корпоративных клиентов превышает 270 000.

Веб-сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru
Вирусная лаборатория:	https://virusdesk.kaspersky.ru (для проверки подозрительных файлов и сайтов)
Веб-форум "Лаборатории Касперского":	https://forum.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в директории установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Amazon – товарный знак Amazon.com, Inc.

Core – зарегистрированный товарный знак Intel Corporation в США и других странах.

Linux – зарегистрированный товарный знак Линуса Торвальдса (Linus Torvalds) в США и других странах.

Microsoft, Outlook, Outlook Express и Windows – зарегистрированные товарные знаки Microsoft Corporation в США и других странах.

Novell – зарегистрированный товарный знак Novell Inc. в США и других странах.

JavaScript и Oracle – зарегистрированные товарные знаки Oracle Corporation и (или) ее аффилированных компаний.

CentOS – товарный знак Red Hat, Inc.

Red Hat и Red Hat Enterprise Linux – зарегистрированные товарные знаки Red Hat Inc. в США и других странах.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

SUSE – зарегистрированный товарный знак SUSE LLC в США и других странах.