KASPERSKY lab

Kaspersky Endpoint Security 10

Service Pack 1 для Linux

Версия 10.1.0.5960, 10.1.0.6024 (для Astra Linux)

Подготовительные процедуры и руководство по эксплуатации

Уважаемый пользователь!

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

Дата редакции документа: 25.04.2018

Обозначение документа 643.46856491.00049-06 90 01

http://www.kaspersky.ru
https://help.kaspersky.com/ru
http://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 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.

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.

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 Лицензия (License ID:9)

Этот раздел содержит информацию о задаче Лицензия.

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 управления 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.

Использование графического пользовательского интерфейса Kaspersky Endpoint Security

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

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.

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

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 текста	Описание условного обозначения
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком "Пример".
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.

О программе

Программное изделие Kaspersky Endpoint Security представляет собой САВЗ типов «Б», «В», «Г» второго класса защиты.

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

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

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

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) БД ПКВ программы;
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация программы.

Требования

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

В этом разделе

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Минимальные общие требования:

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

Программные требования:

- Поддерживаемые 32-битные операционные системы:
  - Ubuntu 14.04.5 LTS;
  - Ubuntu 16.04.4 LTS;
  - Ubuntu 17.10.1;
  - Red Hat® Enterprise Linux® 6.9;
  - CentOS-6.9;
  - Debian GNU / Linux 8.10;
  - Debian GNU / Linux 9.4;
  - ОС Альт 8 СП;
  - Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6).

- Поддерживаемые 64-битные операционные системы:
  - Ubuntu 14.04.5 LTS;
  - Ubuntu 16.04.4 LTS;
  - Ubuntu 17.10.1;
  - Red Hat Enterprise Linux 6.9;
  - Red Hat Enterprise Linux 7.4;
  - CentOS-6.9;
  - CentOS-7.4;
  - Debian GNU / Linux 8.10;
  - Debian GNU / Linux 9.4;
  - Oracle Linux 7.4;
  - SUSE® Linux Enterprise Server 12 SP3;
  - openSUSE® 42.3;
  - ОС Альт 8 СП;
  - Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6);
  - ROSA "Cobalt" (настольный выпуск) 7.3;
  - ROSA "Cobalt" (серверный выпуск) 7.3;
  - EMIAS 1.0;
  - Astra Linux 1.4;
  - Astra Linux 1.5.
- Интерпретатор языка Perl версии 5.10.
- Установленная утилита which.
- Установленные пакеты для компиляции программ (gcc, binutils, glibc, glibc-devel, make, ld).
- Исходный код ядра операционной системы – для компиляции модулей Kaspersky Endpoint Security на операционных системах, не поддерживающих технологию fanotify.
- Kaspersky Endpoint Security 10 для Linux совместим с Kaspersky Security Center 10 SP1 и Kaspersky Security Center 10 SP2.
- Для работы плагина управления Kaspersky Endpoint Security должен быть установлен Microsoft® Visual C++ 2015 Redistributable Update 3 RC.
- До установки Агента администрирования должны быть установлены следующие модули:

- Модуль libc6-i386 должен быть установлен на 64-битные версии Debian и Ubuntu.
- Модуль glibc.i686 должен быть установлен на Red Hat Enterprise Linux 7, CentOS 7, Oracle Linux 7.
- Модуль glibc-32bit должен быть установлен на openSUSE 42, CentOS 6.

Инсталляционный комплект

Инсталляционный комплект Kaspersky Endpoint Security содержит следующие файлы:

- `kesl-10.1.0-<номер сборки>.i386.rpm`

  `kesl_10.1.0-<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-10.1.0-<номер сборки>.x86_64.rpm`

  `kesl_10.1.0-<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 по установке Kaspersky Endpoint Security из пакета установки (далее "пакет") и по установке Агента администрирования.

В этом разделе

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.

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-10.1.0-<номер сборки>.i386.rpm
```

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

```
# rpm -i kesl-10.1.0-<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-10.1.0-<номер сборки>_i386.deb
```

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

```
# dpkg -i kesl_10.1.0-<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:*

- Поддерживаемые 32-битные операционные системы:

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

- Поддерживаемые 64-битные операционные системы:

  ```
  /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 этом разделе

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

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

Вы можете обновить предыдущую версию программы следующими способами:

- локально из командной строки (см. раздел "Обновление программы с помощью командной строки");
- удаленно с помощью пакета ПО Kaspersky Security Center (см. документацию для Kaspersky Security Center).

Для обновления предыдущей версии программы до Kaspersky Endpoint Security 10 Service Pack 1 для Linux не нужно удалять предыдущую версию программы. Перед началом обновления предыдущей версии программы рекомендуется закрыть все работающие программы.

В этом разделе

Обновление программы с помощью командной строки

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

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

► *Чтобы обновить программу, выполните следующие действия:*

1. Запустите нужный пакет установки Kaspersky Endpoint Security 10 Service Pack 1 для Linux (см. раздел "Установка пакета Kaspersky Endpoint Security").

Kaspersky Endpoint Security 10 для Linux останавливается, и экспортируются параметры программы и журнал событий.

2. Запустите скрипт послеустановочной настройки (см. раздел "О первоначальной настройке Kaspersky Endpoint Security").

   Скрипт послеустановочной настройки пошагово запрашивает значения параметров Kaspersky Endpoint Security.

   > Согласие с условиями Лицензионного соглашения и Политики конфиденциальности является обязательным.

   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 для Linux можно удаленно обновить до Kaspersky Endpoint Security 10 Service Pack 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 Агент администрирования (см. раздел "Установка Агента администрирования").

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

   Программа работает корректно во время обновления Агента администрирования.

2. Установите Kaspersky Endpoint Security 10 Service Pack 1 для Linux удаленно.

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 этом разделе

Подготовка программы к работе

Этот раздел содержит инструкции о первоначальной настройке Kaspersky Endpoint Security.

1.1.1 *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.

Kaspersky Endpoint Security 10 для Linux можно обновить до Kaspersky Endpoint Security 10 Service Pack 1 для Linux. (см. раздел "Обновление старой версии программы").

Антивирус Касперского 8.0 для Linux File Server нельзя обновить до Kaspersky Endpoint Security 10 Service Pack 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. раздел "Включение и выключение использования Kaspersky Security Network").

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. раздел "Шаг 8. Загрузка антивирусных баз Kaspersky Endpoint Security").

► *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. раздел "Изменение параметров расписания задачи").

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 отключить использование графического пользовательского интерфейса в любой момент. (см. раздел "Локальное включение и отключение графического пользовательского интерфейса").

1.1.2 *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>
```

Параметры конфигурационного файла первоначальной настройки Kaspersky Endpoint Security

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

Таблица 1. Параметры конфигурационного файла первоначальной настройки программы

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. Для сохранения сертифицированной конфигурации программы допустимо использование исключительно Локального KSN (KPSN). В противном случае использование KSN должно быть отключено. no – не принимать Положение о Kaspersky Security Network.

Параметр	Описание	Возможные значения
SERVICE_LOCALE	Дополнительный параметр Языковой стандарт, используемый при работе Kaspersky Endpoint Security	Языковой стандарт в формате, определенном в RFC 3066. Если параметр SERVICE_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 – отключить использование графического пользовательского интерфейса.
IMPORT_SETTINGS	Использование параметров программы из конфигурационного файла	• yes – использовать параметры программы из конфигурационного файла. • no – не использовать параметры программы из конфигурационного файла.

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).

1.1.3 *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:
   - Поддерживаемые 32-битные операционные системы:

     ```
     # /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
     ```
   - Поддерживаемые 64-битные операционные системы:

     ```
     # /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.

1.1.4 *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 постоянной защиты:

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

   - задачу проверки памяти процессов:

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

   - задачу проверки загрузочных секторов:

     ```
     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.

1.1.5 *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 одним из следующих способов:
   - `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. Во второй консоли запустите следующие задачи:

   - задачу постоянной защиты:

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

   - задачу проверки памяти процессов:

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

   - задачу проверки загрузочных секторов:

```
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**.

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

   ```
   aa-complain opt.kaspersky.kesl.libexec.kesl
   ```

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 opt.kaspersky.kesl.libexec.kesl
   ```

> 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.

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'
```

Сертифицированное состояние программы

Программа находится в сертифицированном (безопасном) состоянии, 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").

Лицензирование программы

В этом разделе описаны основные аспекты лицензирования программы.

В этом разделе

О лицензионном соглашении

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

- Связаться со Службой технической поддержки.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" 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 буферный период для продления подписки, в течение которого функциональность программы сохраняется. Наличие и длительность буферного 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 буферный 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 используемом продукте, 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, текущее состояние лицензии, 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 продуктов 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.

В этом разделе

После изменения общих параметров Kaspersky Endpoint Security перезапустите программу.

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.

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.

Значение по умолчанию: `/etc/exports`

TraceFolder

Директория, в которой Kaspersky Endpoint Security сохраняет файлы журнала трассировки.

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

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`.

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 проверки по требованию пропускают такой файл при проверке.

Возможные значения: `4096 – 33554432`.

Значение по умолчанию: `16384`.

DetectOtherObjects

Включает / отключает 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`. Отключить обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Значение по умолчанию: `No`.

UseKSN

Включает / отключает 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 / отключает использование прокси для Kaspersky Security Network, активации программы и обновлений.

Доступные значения:

`Yes`. Включить использование прокси.

`No`. Отключить 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.

Возможные 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 / отключает запись информации о событиях в syslog. В некоторых случаях программа не может создать и сохранить событие. В этом случае информация сохраняется в syslog.

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

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

Значение по умолчанию: `No`.

UIReportsForRootOnly

Включает / отключает просмотр отчетов для пользователей из графического пользовательского интерфейса.

`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`.

Команды управления параметрами Kaspersky Endpoint Security и задачами

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

1.1.6 *Получение общих параметров Kaspersky Endpoint Security*

Опция `--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 опции `--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 опции `--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
```

1.1.7 *Изменение общих параметров Kaspersky Endpoint Security*

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

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

1. Сохраните общие параметры Kaspersky Endpoint Security в конфигурационном файле с помощью опции `--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 опции `--set-app-settings`. Kaspersky Endpoint Security применит новые значения параметров после того, как вы остановите и снова запустите Kaspersky Endpoint Security с помощью опций `--stop-app` и `--start-app` или с помощью опции `--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.

Пример:

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
```

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

Опция `-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 опцией `--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

Опция `--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 file>
```

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 / отключает запуск пропущенной задачи после запуска Kaspersky Endpoint Security.

Экспорт и импорт параметров программы

Kaspersky Endpoint Security разрешает 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 указать `UseKSN=Basic` или `UseKSN=Extended` (см. раздел "Участие в Kaspersky Security Network").

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, как управлять задачами.

В этом разделе

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. раздел "Управление программой через Kaspersky Security Center").

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 постоянной защиты (ID=1, тип – OAS);
- Scan_My_Computer – задача проверки по требованию (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 и останавливать задачи;
- создавать и удалять задачи (только для пользовательских задач);
- изменять параметры задач.

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:

- Name. Имя задачи.
- ID. Идентификатор задачи (см. раздел "О задачах Kaspersky Endpoint Security").

- Type. Тип задачи (см. раздел "О задачах Kaspersky Endpoint Security" на 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».

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;
- <task type> – предустановленный тип задачи (см. раздел "О задачах Kaspersky Endpoint Security").

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;

- <task type> – предустановленный тип задачи (см. раздел "О задачах Kaspersky Endpoint Security");
- <полный путь к конфигурационному файлу> – полный путь к конфигурационному файлу (см. раздел "Конфигурационные файлы задачи по умолчанию").

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>|<ID задачи> --
   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>|<ID задачи> --
   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 ID задачи>
   setting=value [setting=value]
   ```

   Kaspersky Endpoint Security изменит указанный параметр.

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

```
kesl-control --get-settings <имя или ID 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>
```

Управление областями проверки из командной строки

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

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

```
kesl-control --set-settings <ID или 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 или 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 Anti-Cryptor из командной строки.

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

```
kesl-control --set-settings <ID или 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 или 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.

Приостановка и возобновление задачи

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

► *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.

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

Опция `--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

   опции `-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 опции `--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

Опция `--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 `--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 `-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 постоянной защиты (File_Monitoring ID:1)

Этот раздел содержит информацию о задаче постоянной защиты.

В этом разделе

О постоянной защите

Постоянная защита позволяет избежать заражения файловой системы компьютера. Задача постоянной защиты создается с параметрами по умолчанию при установке Kaspersky Endpoint Security на компьютер. По умолчанию задача постоянной защиты запускается автоматически при старте Kaspersky Endpoint Security. Задача постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы. Вы можете останавливать и запускать ее.

Вы не можете создавать пользовательские задачи постоянной защиты. Вы можете изменять параметры предустановленной задачи постоянной защиты.

Параметры постоянной защиты содержатся в конфигурационном файле, который использует задача постоянной защиты.

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 разрешает 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 постоянной защиты или в область проверки задачи проверки по требованию.

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 постоянной защиты

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

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

ScanArchived

Включает / отключает проверку 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

Включает / отключает проверку 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

Включает / отключает проверку 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

Включает / отключает проверку 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 задачах постоянной защиты, перед тем как выполнить выбранное вами действие, Kaspersky Endpoint Security блокирует доступ к объекту для программы, которая к нему обратилась.

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 / 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 / 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. 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 / 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 / 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 / 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 / отключает эвристический анализатор.

Эвристический анализ позволяет 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 / 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 задачах постоянной защиты.

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: `Все объекты`.

Пример:

```
AreaDesc="Проверка почтовых баз"
```

UseScanArea

Включает / 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

Указывает 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 / отключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает 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;

`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 постоянной защиты. Файлы в глобальной области исключения исключаются из области постоянной защиты.

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

1. Сохраните параметры задачи постоянной защиты в файле с помощью следующей команды:

   ```
   kesl-control --get-settings <имя или ID 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 постоянной защиты с помощью следующей команды:

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

Задача проверки по требованию (Scan_My_Computer ID:2)

В этом разделе содержится информация о задаче проверки по требованию.

В этом разделе

О проверке по требованию

Проверка по требованию – это однократная полная или выборочная проверка файлов на компьютере, которую выполняет Kaspersky Endpoint Security. Kaspersky Endpoint Security может выполнять одновременно несколько задач проверки по требованию.

В Kaspersky Endpoint Security по умолчанию создана одна предустановленная задача проверки по требованию – 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 проверки по требованию.

Также в Kaspersky Endpoint Security по умолчанию создана предустановленная задача выборочной проверки.

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

Параметры задачи проверки по требованию

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

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

ScanArchived

Включает / отключает проверку 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

Включает / отключает проверку 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

Включает / отключает проверку 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

Включает / отключает проверку 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

Включает / отключает применение 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

Включает / отключает применение 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 / 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 / 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. 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 / 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 / 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 / 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 / отключает эвристический анализатор.

Эвристический анализ позволяет 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 / 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 задачах постоянной защиты.

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: `Все объекты`.

Пример:

```
AreaDesc="Проверка почтовых баз"
```

UseScanArea

Включает / 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

Указывает 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 / отключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает 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;

`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 этом разделе

О задаче выборочной проверки

Задача выборочной проверки использует параметры, которые применяются командой

`--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 проверки по требованию (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.

Параметры 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

Включает / отключает проверку 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

Включает / отключает проверку 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

Включает / отключает проверку 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

Включает / отключает проверку 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

Включает / отключает применение 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

Включает / отключает применение 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 / 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 / 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. 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 / 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 / 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 / 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 / отключает эвристический анализатор. Эвристический анализ позволяет 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 / 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 задачах постоянной защиты.

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: `Все объекты`.

Пример:

```
AreaDesc="Проверка почтовых баз"
```

UseScanArea

Включает / 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

Указывает 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 / отключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает 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;

`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 этом разделе

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 / 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 / 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. Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

ReportCleanObjects

Включает / 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 / 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 / отключает эвристический анализатор. Эвристический анализ позволяет 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`.

Действие

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 этом разделе

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 / 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. Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

ReportCleanObjects

Включает / 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 / 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`.

Действие

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 этом разделе

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.

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.

  Для сохранения сертифицированной конфигурации программы автоматическое обновление программы должно быть отключено.

  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 задач 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.

Доступные значения:

`Disable` – 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`.

> Для сохранения сертифицированной конфигурации программы загрузка и установка обновлений программы должны быть отключены:
>
> `ApplicationUpdateModen=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.

► *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 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 или Положение о Kaspersky Security Network.

► *Чтобы принять Лицензионное соглашение,*

1. Прочитайте текст Лицензионного соглашения.

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 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` для пакета в формате rpm.
   - `# KESL_ USE_KSN=Yes dpkg -i <имя пакета в формате deb>.deb` для пакета в формате deb.

Для сохранения сертифицированной конфигурации программы допустимо использование исключительно Локального KSN (KPSN). В противном случае использование KSN должно быть отключено.

Задача отката обновления (Rollback ID:7)

В этом разделе содержится информация о задаче отката обновления.

Задача отката обновления выполняется для отката последнего успешного обновления баз.

У этой задачи нет параметров.

Подробнее об управлении задачей отката обновления см. в разделе "Управление задачами Kaspersky Endpoint Security с помощью командной строки".

Задача копирования обновлений (Retranslate ID:8)

В этом разделе содержится информация о задаче копирования обновлений.

В этом разделе

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

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.

AutoPatchDownload

Включает / отключает автоматическую загрузку обновлений программы.

Доступные значения:

`Yes` – загружать обновления программы автоматически;

`No` – не загружать обновления программы автоматически.

Значение по умолчанию: `Yes`.

Задача Лицензия (License ID:9)

В этом разделе содержится информация о задаче Лицензия.

В этом разделе

О задаче Лицензия

Задача Лицензия позволяет управлять ключами и кодами активации Kaspersky Endpoint Security.

Добавление активного ключа

Опция `--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

Опция `--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

Опция `--revoke-active-key` удаляет активный ключ.

Синтаксис команды

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

Удаление дополнительного ключа

Опция `--revoke-additional-key` удаляет дополнительный ключ.

Синтаксис команды

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

Ввод дополнительного кода активации

Опция `--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 этом разделе

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 Хранилищем

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. Идентификатор используется для действий с объектом, например, при восстановлении (см. раздел "Восстановление объектов из Хранилища") или удалении объекта из Хранилища (см. раздел "Удаление объектов 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 обнаруженной угрозы в задаче постоянной защиты, а также по имени или по названию обнаруженной угрозы в задачах проверки по требованию.

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 идентификатор 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 этом разделе

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 расширенную 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. 134). Кроме этого можно создавать и запускать задачи *Мониторинг файловых операций по требованию* (ODFIM).

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 () и др.);
- 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 *эталона*.

Вы можете создать несколько задач ODFIM.

Эталон

Эталон задается во время первого запуска задачи ODFIM на компьютере. Для каждой задачи ODFIM создается отдельный эталон. Задача выполняется, только если эталон соответствует области мониторинга. Если эталон не соответствует области мониторинга, Kaspersky Endpoint Security создает событие о нарушении целостности файла.

Вы можете заново создать эталон для задачи с помощью соответствующего параметра (см. раздел "Параметры задачи Мониторинг файловых операций по требованию" на стр. 135). Эталон создается заново после завершения задачи ODFIM.

Эталон также создается заново при изменении параметров задачи, например, когда добавляется новая область мониторинга. Эталон будет создан заново при следующем выполнение задачи.

Задача ODFIM создает хранилище для эталонов на компьютере с установленным компонентом Мониторинг файловых операций.

Удалить эталон 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 / отключает 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 / отключает 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.

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 / отключает повторное создание эталона после завершения задачи ODFIM.

Доступные значения:

`Yes` – создавать эталон повторно после завершения задачи ODFIM;

`No` – не создавать эталон повторно после завершения задачи ODFIM.

Значение по умолчанию: `No`.

CheckFileHash

Включает / отключает проверку хеша (SHA-256).

Доступные значения:

`Yes` – включить проверку хеша;

`No` – отключить проверку хеша.

Значение по умолчанию: `No`.

TrackDirectoryChanges

Включает / отключает мониторинг директорий.

Доступные значения:

`Yes` – контролировать директории;

`No` – не контролировать директории.

Значение по умолчанию: `No`.

TrackLastAccessTime

Включает / отключает 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 / 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 / отключает 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.

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 управления сетевым экраном (Firewall ID:12)

В этом разделе содержится информация о задаче Управление сетевым экраном.

В этом разделе

О задаче Управление сетевым экраном

Для сохранения сертифицированной конфигурации программы задача Управления 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 личные 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. раздел "О сетевых пакетных правилах"). 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. раздел "О динамических правилах").

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 подсетей. С помощью заданной сетевой зоны вы можете использовать одно и то же правило для нескольких IP-адресов или подсетей, не создавая отдельное правило для каждого IP-адреса или подсети. Сетевую зону можно использовать в качестве значения для опции

`--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 добавлять IP-адреса и подсети в сетевую зону (см. раздел "Добавление сетевого адреса в блок зоны") и удалять их из нее (см. раздел "Удаление сетевого адреса из блока 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` – подсеть адресов IPv4, где p – число от 0 до 32;

`x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff;

`x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64.

Значение по умолчанию: `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` – подсеть адресов IPv4, где p – число от 0 до 32;

`x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff;

`x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64.

Значение по умолчанию: `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 подсетей IP-адресов.

Address.item_xxxx

Доступные значения:

`d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255.

`d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32.

`x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff.

`x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64.

Значение по умолчанию: “” (в этой зоне нет сетевых адресов)

Блок [NetworkZonesLocal]

В блоке `[NetworkZonesLocal]` указываются сетевые адреса, связанные с локальными сетями.

Вы можете указать несколько IP-адресов или подсетей IP-адресов.

Address.item_xxxx

Доступные значения:

`d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255.

`d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32.

`x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff.

`x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64.

Значение по умолчанию: “” (в этой зоне нет сетевых адресов)

Блок [NetworkZonesTrusted]

В блоке `[NetworkZonesTrusted]` указываются сетевые адреса, связанные с доверенными сетями.

Вы можете указать несколько IP-адресов или подсетей IP-адресов.

Address.item_xxxx

Доступные значения:

`d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255.

`d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32.

`x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff.

`x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64.

Значение по умолчанию: “” (в этой зоне нет сетевых адресов)

Добавление сетевого пакетного правила

Вы можете добавить сетевое пакетное правило вручную.

Сетевые пакетные правила можно добавлять только по одному.

► *Чтобы добавить сетевое пакетное правило, выполните следующую команду:*

```
kesl-control -F --add-rule --name <имя правила> --action
<действие> --protocol <протокол> --direction <направление> --
remote <удаленный адрес> --local <локальный адрес> --at <индекс
в списке сетевых пакетных правил>
```

В конфигурационный файл задачи Управление сетевым экраном будет добавлен блок, содержащий параметры нового сетевого пакетного правила. Если вы не указали в команде конкретный параметр, устанавливается значение по умолчанию (см. раздел "Конфигурационный файл задачи Управление сетевым экраном").

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 *Public*, 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 <index>`

  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 задачи.

Если зона содержит несколько элементов с одинаковым сетевым адресом, команда `–del-zone` не будет выполнена.

Если указанный сетевой адрес или индекс не существует, выводится ошибка.

Задача Защита от шифрования (AntiCryptor ID:13)

В этом разделе содержится информация о задаче Защита от шифрования.

В этом разделе

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.

По умолчанию Kaspersky Endpoint Security блокирует доступ недоверенных компьютеров к сетевым файловым ресурсам на 30 минут.

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 опцию `--allow-hosts`, чтобы разблокировать компьютер (см. раздел "Разблокирование заблокированных компьютеров").

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 / отключает блокирование недоверенных компьютеров.

Если блокирование недоверенных компьютеров отключено, 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` – отключить 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 / 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 / отключает 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: `Все объекты`.

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.

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, как включить и выключить использование Kaspersky Security Network.

В этом разделе

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 (KPSN).

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" (https://www.kaspersky.ru/products-and-services-privacy-policy). 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 к интернету.
- 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 Kaspersky Security Center Service Pack 2.

В этом разделе

Об управлении Kaspersky Endpoint Security с помощью Kaspersky Security Center

Kaspersky Security Center позволяет дистанционно 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.
  - устанавливать обновления;
  - откатывать обновления баз;
  - проверять загрузочные сектора;
  - проверять память процессов;
  - выполнять проверку по требованию;
  - контролировать целостность файлов.

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, справа от списка программ "Лаборатории Касперского", выполните следующие действия:

    a. Правой клавишей мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 SP1 для Linux и выберите пункт **Свойства**. Вы также модете нажать на кнопку **Свойства**, расположенную под списком программ "Лаборатории Касперского".

    Откроется окно Параметры программы Kaspersky Endpoint Security 10 SP1 для Linux на закладке **Общие**.

    b. Нажмите на кнопку **Запустить**.

- Если вы хотите остановить работу программы, справа от списка программ "Лаборатории Касперского", выполните следующие действия:

    a. Правой клавишей мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 SP1 для Linux и выберите пункт **Свойства**. Вы также можете нажать кнопку **Свойства**, расположенную под списком программ.

    Откроется окно **Параметры** программы Kaspersky Endpoint Security 10 SP1 для Linux на закладке **Общие**.

    b. Нажмите на 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 документации 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 на 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 постоянной защиты, например: *Выполняется*, *Остановлена*, *Приостановлена*;
- **Последняя проверка по требованию** – дата и время последнего выполнения задачи проверки по требованию;
- **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 на 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.
6. 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 постоянной защиты, например: Выполняется, 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 задачами

Этот раздел содержит информацию об управлении задачами для Kaspersky Endpoint Security.

Подробнее о методике управления задачами через Kaspersky Security Center вы можете прочитать в документации для Kaspersky Security Center.

1.1.8 *О задачах для Kaspersky Endpoint Security*

Kaspersky Security Center управляет работой продукта 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 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.
- **Проверка по требованию**. 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 эталона.

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.

Общая информация о задачах в Kaspersky Security Center приводится в документации для Kaspersky Security Center.

1.1.9 *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 на кнопку **Добавить**.

   Запустится мастер создания задачи.
8. Следуйте указаниям мастера создания задачи.

1.1.10 *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 на кнопку **Создать задачу**.
   - Выберите пункт **Создать задачу** в контекстном меню Kaspersky Security Center.

Запустится мастер создания задачи.

5. Следуйте указаниям мастера создания задачи.

1.1.11 *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 на кнопку **Назначить задачу набору устройств**.
6. В следующем окне мастера нажмите на кнопку **Выбрать**.

   Откроется окно **Выбор устройства**.
7. Выберите нужное устройство.
8. Нажмите на кнопку **ОК** в окне **Выбор устройства**.
9. Следуйте указаниям мастера создания задачи.

1.1.12 *Запуск, остановка, приостановка и возобновление выполнения задачи вручную*

Если на клиентском компьютере запущена программа Kaspersky Endpoint Security, вы можете запустить / остановить / приостановить / возобновить выполнение задачи на этом клиентском компьютере через Kaspersky Security Center (см. раздел "Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере"). 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 на кнопку справа от списка локальных задач, чтобы запустить или остановить локальную задачу.
   - Нажмите на кнопку **Свойства** под списком локальных задач. Откроется окно **Свойства задачи <Название задачи>**. Далее на закладке **Общие** окна **Свойства задачи <Название задачи>** нажмите на кнопку **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли 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 на 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 на кнопку **Запустить** / **Остановить** справа от списка задач для наборов компьютеров, чтобы запустить или остановить задачу для наборов компьютеров.

1.1.13 *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 на кнопку **Свойства**.

Откроется окно Свойства: <Название локальной задачи>.

9. В окне **Свойства: <Название локальной задачи>** выберите раздел Параметры.
10. Измените параметры локальной задачи.
11. В окне **Свойства: <Название локальной задачи>** нажмите на кнопку **ОК**, 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 на 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 на кнопку **ОК**, 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 на 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 документации для Kaspersky Security Center. Блок **Параметры** содержит специфические параметры Kaspersky Endpoint Security 10 SP 1 для Linux. Содержание этого блока зависит от выбранной задачи и ее типа.

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 при помощи политик Kaspersky Security Center вы можете прочитать в документации для Kaspersky Security Center.

1.1.14 *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 Постоянная защита, 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 документации для *Kaspersky Security Center*.

1.1.15 *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 на кнопку **Создать политику**.
   - Правой клавишей мыши откройте контекстное меню. Выберите пункт **Создать политику**.

   Запустится мастер создания политики.
5. Следуйте указаниям мастера создания политики.

1.1.16 *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 на 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 постоянной защиты**, **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 на кнопку **OK**, чтобы сохранить внесенные изменения.

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.

Использование графического пользовательского интерфейса Kaspersky Endpoint Security

В этом разделе описана работа в Kaspersky Endpoint Security с использованием графического пользовательского интерфейса.

В этом разделе

Локальное включение и отключение графического пользовательского интерфейса

Вы можете включить или отключить графический пользовательский интерфейс Kaspersky Endpoint Security локально с помощью командной строки.

Для включения и отключения графического пользовательского интерфейса требуются root-права.

► *Чтобы включить или отключить графический пользовательский интерфейс, выполните следующие действия:*

1. Запустите конфигурационный скрипт программы:

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

2. В командной строке 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 проверки по требованию.

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.

1.1.17 *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 для Linux** открывает главное окно программы. В главном окне программы отображается статус защиты вашего компьютера, а также состояние задачи проверки по требованию и обновления. Вы также можете перейти в окно **Отчеты**, **Хранилище**, **Настройки** 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.

1.1.18 *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 проверки по требованию и количество обнаруженных угроз. Закладка позволяет перейти в окно **Проверка**. В этом окне можно запустить и остановить задачи проверки по требованию, 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 **Настройки**. При нажатии этой кнопки открывается окно Настройка, где можно включить или выключить участие в Kaspersky Security Network, а также задачи Постоянная защита, 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 SP 1 для Linux**.

Управление задачами и компонентами

По умолчанию графический пользовательский интерфейс Kaspersky Endpoint Security разрешает вам запускать и останавливать следующие задачи:

- Задача полной проверки (Scan_My_Computer)
- Задачи проверки по требованию (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:

- Постоянная защита
- Управление сетевым экраном

- Защита от шифрования
- Мониторинг файловых операций

Кроме того, вы можете управлять своим участием в Kaspersky Security Network (см. раздел "Управление участием в Kaspersky Security Network").

1.1.19 *Запуск и остановка задач проверки*

Вы можете запускать и останавливать задачи полной проверки, проверки по требованию, проверки загрузочных секторов и проверки памяти процессов с помощью графического пользовательского интерфейса Kaspersky Endpoint Security.

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

1. Откройте главное окно программы.
2. Кнопкой **Проверка**, расположенной в главном окне программы, откройте окно **Проверка**.
3. Выполните одно из следующих действий:
   - Если вы хотите запустить задачу, нажмите на кнопку **Запустить** под той задачей, которую вы хотите запустить.

     Отображается ход выполнения задачи.
   - Если вы хотите остановить задачу, нажмите на 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 на 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.

1.1.20 *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.
2. Кнопкой **Обновить**, расположенной в главном окне программы, откройте окно **Обновление**.

3. Выполните одно из следующих действий:

   - Если вы хотите запустить задачу, нажмите на 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 на кнопку **Остановить** под той задачей, которую вы хотите остановить.

     Задача будет остановлена.

4. При необходимости вы можете нажать на 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.
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.

1.1.21 *Включение и выключение компонентов программы*

С помощью графического пользовательского интерфейса Kaspersky Endpoint Security вы можете в любой момент включить или выключить такие компоненты программы, как Постоянная защита, Управление сетевым экраном, Защита от шифрования и Мониторинг файловых операций.

Если компонент включен, доступна кнопка **Выключить**. По умолчанию включена только постоянная защита.

Если компонент выключен, доступна кнопка **Включить**.

► *Чтобы включить или выключить компонент, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части главного окна программы нажмите на кнопку **Настройки**.

   Откроется окно **Настройка**.

3. В окне **Настройка** выполните следующие действия для нужного компонента:

- Если вы хотите включить компонент, нажмите на кнопку **Включить**.
- Если вы хотите выключить компонент, нажмите на кнопку **Отключить**.

1.1.22 *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.
2. В нижней части главного окна программы нажмите кнопку **Настройки**.

   Откроется окно **Настройка**.
3. В окне **Настройки** 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 на 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 на кнопку **ОК**.

   Кнопка **ОК** недоступна, если выбран вариант **Не выбрано**.

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

1. Откройте главное окно программы.
2. В нижней части главного окна программы нажмите кнопку **Настройки**.

   Откроется окно **Настройки**.
3. В окне **Настройки** нажмите на 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.

1.1.23 *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 постоянной защиты и задачах проверки по требованию. Вы можете обновить отображаемый отчет, нажав кнопку **Обновить**.

  При остановке задачи происходит сброс статистики задачи постоянной защиты. Сброса статистики задач проверки по требованию не происходит. Вместо этого статистика накапливается, 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;

1.1.24 *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.
2. В нижней части главного окна программы нажмите на 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.
2. Нажмите на 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.
2. Нажмите на 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. По умолчанию для уровня трассировки установлено значение **Диагностика (300)**.

5. Чтобы начать процесс трассировки, нажмите на кнопку **Включить**.
6. Чтобы остановить процесс трассировки, нажмите на кнопку **Выключить**.

Созданные файлы трассировки хранятся в директории `/var/log/kaspersky/kesl/`.

Обращение в службу технической поддержки

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

В этом разделе

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.

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. 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".

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – 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.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

В этом разделе

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.

1.1.25 *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 пробела и табуляции 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.

1.1.26 *Конфигурационный файл задачи Постоянная защита*

```
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=*
```

1.1.27 *Конфигурационный файл задачи Проверка по требованию*

```
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=*
```

1.1.28 *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=*
```

1.1.29 *Конфигурационный файл задачи Проверка загрузочных секторов*

```
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
Action=Cure
```

1.1.30 *Конфигурационный файл задачи Проверка памяти процессов*

```
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportUnprocessedObjects=No
Action=Cure
```

1.1.31 *Конфигурационный файл задачи Обновление*

```
SourceType="KLServers"
UseKLServersWhenUnavailable=Yes
IgnoreProxySettingsForKLServers=No
IgnoreProxySettingsForCustomSources=No
ApplicationUpdateMode=DownloadOnly
ConnectionTimeout=10
```

1.1.32 *Конфигурационный файл задачи Копирование обновлений*

```
SourceType=KLServers
UseKLServersWhenUnavailable=Yes
ConnectionTimeout=10
ApplicationUpdateMode=DownloadOnly
```

1.1.33 *Конфигурационный файл задачи Управление Хранилищем*

```
DaysToLive=90
BackupSizeLimit=0
BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

1.1.34 *Конфигурационный файл задачи Управление сетевым экраном*

```
DefaultIncomingAction=Allow
DefaultIncomingPacketAction=Allow
```

```
[NetworkZonesTrusted]
[NetworkZonesLocal]
[NetworkZonesPublic]
```

1.1.35 *Конфигурационный файл задачи Мониторинг файловых операций*

```
UseExcludeMasks=No
[ScanScope.item_0000]
AreaDesc=Kaspersky internal objects
UseScanArea=Yes
Path=/opt/kaspersky/kesl/
AreaMask.item_0000=*
```

1.1.36 *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 с Антивирусом Касперского для Linux Mail Server, выполните следующие действия:*

1. Сохраните параметры задачи постоянной защиты 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 постоянной защиты 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 опцией `--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 2. 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 Хранилище. Если лечение невозможно, программа оставляет объект неизменным. • `Remove` – программа удаляет зараженный объект, предварительно создав его резервную копию.

Название параметра	Сущность, к которой относится параметр	Значение параметра в сертифицированном состоянии программы
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.
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.

Название параметра	Сущность, к которой относится параметр	Значение параметра в сертифицированном состоянии программы
ScanMailBases	Задача постоянной проверки, задача проверки по требованию	Yes – проверять файлы почтовых баз.
ApplicationUpdateMode	Задача обновления	Disable – не загружать и не устанавливать обновления программы.
UseKSN	Общий параметр программы	No – выключить участие в Kaspersky Security Network.

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

> Перечисленные источники информации носят исключительно справочный характер и не являются заменой данного руководства.

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

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

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

Страница Kaspersky Endpoint Security в Базе знаний

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

На странице Kaspersky Endpoint Security в Базе знаний (http://support.kaspersky.ru/kes10linux) вы найдете статьи с полезной информацией, рекомендациями и ответами на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи в Базе знаний могут дать ответы на вопросы, связанные как с Kaspersky Endpoint Security, так и с другими программами "Лаборатории Касперского". Статьи Базы знаний также могут включать новости технической поддержки.

Обсуждение программ "Лаборатории Касперского" на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и другими пользователями на нашем форуме.

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

Для доступа к ресурсам веб-сайта необходимо подключение к интернету.

Если вы не нашли решение своей проблемы, обратитесь в Службу технической поддержки.

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.com (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.

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.

Oracle – зарегистрированный товарный знак Oracle Corporation и (или) ее аффилированных компаний.

Red Hat, Red Hat Enterprise Linux, CentOS – 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.