kaspersky

Kaspersky Endpoint Security для Linux редакция под Эльбрус

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 10.1.2.329

Уважаемый пользователь!

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

Обозначение документа: 643.46856491.00108-01 90 01

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

kaspersky

Содержание

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Endpoint Security для Linux редакция под Эльбрус" (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.

Источники информации о программе

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

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

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

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

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

Страница Kaspersky Endpoint Security в Базе знаний

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

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

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

Электронная справка

В состав электронной справки программы входят файлы контекстной справки интерфейса программы.

В контекстной справке вы можете найти информацию об окнах плагина управления Kaspersky Endpoint Security: перечень и описание параметров.

Электронная справка создана для удобства пользователей и не является полноценным эквивалентом настоящего документа.

Сообщество пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе https://community.kaspersky.com.

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 127).

kaspersky

О программе

Программное изделие Kaspersky Endpoint Security 10 для Linux редакция под Эльбрус (далее также "Kaspersky Endpoint Security", "программа") 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 Endpoint Security, являются:

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

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению 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;
- контроль целостности компонентов программы.

В сертифицированной версии программы не поддерживаются следующие функции:

- графический пользовательский интерфейс программы;
- задача управления Сетевым экраном (Firewall ID:12);
- механизм автоматической загрузки обновлений программы.

Несмотря на то, что параметры некоторых из этих функций отображаются в плагине управления Kaspersky Endpoint Security в Kaspersky Security Center, невозможно использовать эти функции и настроить их параметры.

Инсталляционный комплект

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

- kesl-10.1.2-<номер сборки>.e2k.rpm, kesl-10.1.2-<номер сборки>.e2kv4.rpm

  Содержат основные файлы Kaspersky Endpoint Security. Пакеты могу быть установлены на операционные системы ALT Linux 8 в соответствии с типом пакетного менеджера.

- kesl_10.1.2-<номер сборки>_e2k-4c.deb, kesl_10.1.2-<номер сборки>_e2k-8c.deb

  Содержат основные файлы Kaspersky Endpoint Security. Пакеты могу быть установлены на операционные системы Эльбрус-Д и Astra Linux Special Edition (релиз "Ленинград") без режима замкнутой программной среды (ЗПС) в соответствии с типом пакетного менеджера.

- kesl-astra_10.1.2-<номер сборки>_e2k-8c.deb

  Содержат основные файлы Kaspersky Endpoint Security. Пакеты могу быть установлены на операционные системы Astra Linux Special Edition (релиз "Ленинград") с режимом замкнутой программной среды (ЗПС).

- kesl.zip

  Содержит файлы, используемые в процедуре удаленной установки Kaspersky Endpoint Security с помощью Kaspersky Security Center.

- klnagent64-<номер сборки>.e2k.rpm, klnagent64-<номер сборки>.e2kv4.rpm, klnagent64_<номер сборки>_e2k-4c.deb, klnagent64_<номер сборки>_e2k-8c.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 текстом Лицензионного соглашения и Политики конфиденциальности. В Лицензионном соглашении указано, на каких условиях вы можете пользоваться программой. Политика конфиденциальности описывает обработку и передачу данных

kaspersky

Требования

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

В этом разделе

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Минимальные аппаратные требования

- Процессоры - 8C, 8CB, 4C, 1C+.
- 2 ГБ оперативной памяти.
- Раздел подкачки не менее 1 ГБ.
- 1 ГБ на жестком диске для установки программного изделия и хранения временных файлов и файлов журналов.

Поддерживаемые операционные системы:

- Astra Linux Special Edition версии 8.1 (релиз "Ленинград") с режимом замкнутой программной среды на процессорах Эльбрус-1C+,Эльбрус-8C.
- Эльбрус-Д версии 1.4.3 на процессорах Эльбрус-1C+, Эльбрус-4C, Эльбрус-8C, Эльбрус-8CB.
- Альт 8 СП Сервер на процессорах Эльбрус-4C, Эльбрус-8C, Эльбрус-8CB.

Программные требования:

- Интерпретатор языка Perl версии не ниже 5.10.
- Установленная утилита which.
- Для работы плагина управления Kaspersky Endpoint Security должен быть установлен Microsoft® Visual C++ 2015 Redistributable Update 3 RC.

Kaspersky Endpoint Security совместим с Kaspersky Security Center 10 Service Pack 3 и Kaspersky Security Center 11.

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.

kaspersky

Установка 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" (см. раздел "Аппаратные и программные требования" на стр. 13).

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.

Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM.

Для работы с Kaspersky Endpoint Security вам требуется выполнить следующие действия:

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 требуется учетная запись root.

Установка пакета Kaspersky Endpoint Security

Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM.

► *Чтобы установить Kaspersky Endpoint Security из пакета формата RPM архитектуры e2k, выполните следующую команду:*

```
# rpm -i kesl-10.1.2-<номер сборки>.e2k.rpm
```

► *Чтобы установить Kaspersky Endpoint Security из пакета формата RPM архитектуры e2kv4, выполните следующую команду:*

```
# rpm -i kesl-10.1.2-<номер сборки>.e2kv4.rpm
```

► *Чтобы установить Kaspersky Endpoint Security из пакета формата DEB архитектуры e2k-4c, выполните следующую команду:*

```
# dpkg -i kesl-10.1.2-<номер сборки>_e2k-4c.deb
```

► *Чтобы установить Kaspersky Endpoint Security из пакета формата DEB архитектуры e2k-8c, выполните следующую команду:*

```
# dpkg -i kesl_10.1.2-<номер сборки>_e2k-8c.deb
```

kaspersky

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 от имени учетной записи root.

- *Чтобы установить Агент администрирования из пакета формата RPM архитектуры e2k, выполните следующую команду:*

```
# rpm -i klnagent64-<номер сборки>.e2k.rpm
```

- *Чтобы установить Агент администрирования из пакета формата RPM архитектуры e2kv4, выполните следующую команду:*

```
# rpm -i klnagent64-<номер сборки>.e2kv4.rpm
```

- *Чтобы установить Агент администрирования из пакета формата DEB архитектуры e2k-4c, выполните следующую команду:*

```
# dpkg -i klnagent64_<номер сборки>_e2k-4c.deb
```

- *Чтобы установить Агент администрирования из пакета формата DEB архитектуры e2k-8c, выполните следующую команду:*

```
# dpkg -i klnagent64_<номер сборки>_e2k-8c.deb
```

После установки пакета запустите скрипт послеустановочной настройки Kaspersky Endpoint Security, выполнив следующую команду:

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

kaspersky

Удаление программы

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

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 klnagent64
  ```

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

  ```
  # dpkg -r klnagent64
  ```

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.

kaspersky

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.

Первоначальная настройка 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 требуется запустить от имени учетной записи root после завершения установки пакета Kaspersky Endpoint Security.

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 учетной записи root.

Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге ознакомьтесь с текстом Лицензионного соглашения, которое заключается между вами и "Лабораторией Касперского", и Политики конфиденциальности, которая описывает обработку и передачу данных. Для этого нажмите на клавишу Enter. Для завершения просмотра используйте клавишу **Q**. Файл с текстом Лицензионного соглашения и Политики конфиденциальности расположен в директории `/opt/kaspersky/kesl/doc/license.<ID языка>`.

Шаг 3. Принятие Лицензионного соглашения

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

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы 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 4. Принятие Политики конфиденциальности

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

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы принимаете 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 5. 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;
- `no` (или `n`), если вы не согласны с условиями Положения о Kaspersky Security Network.

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

Отказ от участия в Kaspersky Security Network не прерывает процесс установки Kaspersky Endpoint Security. Вы можете включить или выключить использование Kaspersky Security Network в любой момент (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 108).

Настройка использования Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе **Прокси-сервер KSN**. См. подробнее в документации Kaspersky Security Center.

Шаг 6. Определение типа перехватчика файловых операций

На этом этапе определяется тип перехватчика файловых операций для используемой операционной системы.

Шаг 7. 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 8. 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 9. Загрузка антивирусных баз Kaspersky Endpoint Security" на стр. 21).

► *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 `no`.

По умолчанию программа предлагает значение `no`.

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

Шаг 9. Загрузка антивирусных баз Kaspersky Endpoint Security

На этом шаге вы можете загрузить на компьютер *антивирусные базы* программы 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, введите `yes`.

Если вы хотите отказаться от немедленной загрузки антивирусных баз, введите `no`.

По умолчанию программа предлагает значение `yes`.

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

Вы можете запустить задачу обновления антивирусных баз Kaspersky Endpoint Security без использования скрипта первоначальной настройки.

Шаг 10. Включение автоматического обновления антивирусных баз

На этом шаге вы можете включить автоматическое обновление антивирусных баз.

Введите `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 `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, управляя расписанием задачи обновления (см. раздел "Изменение параметров расписания задачи" на стр. 53).

Шаг 11. Активация программы

На этом шаге вам нужно активировать программу с помощью файла ключа. Для этого требуется указать полный путь к файлу ключа.

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 первоначальной настройки>
```

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

Параметр	Описание	Возможные значения
EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения	`yes` – согласие с условиями Лицензионного соглашения необходимо для продолжения процедуры установки программы `no` – не принимать Лицензионное соглашение. Установка программы будет прервана
PRIVACY_POLICY_AGREED	Обязательный параметр. Принятие Политики конфиденциальности	`yes` – принять Политику конфиденциальности, чтобы продолжить процедуру установки программы; `no` – не принимать Политику конфиденциальности. Установка программы будет прервана
USE_KSN	Согласие с Положением о Kaspersky Security Network	`yes` – принять Положение о Kaspersky Security Network `no` – не принимать Положение о Kaspersky Security Network
LOCALE	Дополнительный параметр. Языковой стандарт, используемый при работе Kaspersky Endpoint Security	Языковой стандарт в формате, определенном в RFC 3066. Если параметр `LOCALE` не указан, устанавливается языковой стандарт системы по умолчанию.
INSTALL_LICENSE	Файл ключа	—

Параметр	Описание	Возможные 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
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).

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:

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

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

По умолчанию используется порт 14000.

4. Если вы хотите использовать SSL-соединение, укажите номер SSL-порта Сервера администрирования.

   По умолчанию используется порт 13000.

5. Выполните одно из следующих действий:

   - Введите `yes`, если вы хотите использовать SSL-соединение.
   - Введите `no`, если вы не хотите использовать SSL-соединение.

   По умолчанию SSL-соединение включено.

6. При необходимости укажите режим шлюза для соединения:

   - `0` – не использовать шлюз для соединения;
   - `1` – использовать Агент администрирования в качестве шлюза для соединения;
   - `2` – подключаться к Серверу администрирования через шлюз для соединения.

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

Настройка разрешающих правил в системе SELinux

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

1. Переведите SELinux в разрешающий режим:

   - Если SELinux был активирован, выполните следующую команду:

     ```
     # setenforce Permissive
     ```

   - Если SELinux был выключен, в конфигурационном файле `/etc/selinux/config` задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.

2. Запустите следующие задачи:

   - задачу Защита от файловых угроз:

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

   - задачу проверки загрузочных секторов:

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

   - задачу проверки памяти процессов:

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

3. Создайте модуль правил на основе блокирующих записей:

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

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

4. Загрузите полученный модуль правил:

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

5. Переведите SELinux в принудительный режим:

   ```
   # setenforce Enforcing
   ```

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

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

Настройка разрешающих правил в системе AppArmor

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

1. Убедитесь, что модуль AppArmor загружен с помощью одной из следующих команд командной строки:
   - `systemctl status apparmor`
   - `/etc/init.d/apparmor status`
2. Создайте профиль Kaspersky Endpoint Security:
   a. В первой консоли выполните команды:

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

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

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

      - задачу проверки загрузочных секторов:

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

      - задачу проверки памяти процессов:

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

      - задачу обновления:

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

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

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

Созданные профиль можно определить вручную или с помощью команды:

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

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

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

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

   ```
   aa-logprof
   ```

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

5. Переведите профиль Kaspersky Endpoint Security в блокирующий режим:

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

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

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

Сертифицированное состояние программы

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

- Проведена первоначальная настройка параметров программы.
- Программа активирована.
- Антивирусные базы обновлены.
- Настроена и запущена задача Защита от файловых угроз.
- Параметры программы находятся в рамках допустимых значений, приведенных в приложении (см. раздел "Значения параметров программы в сертифицированном состоянии" на стр. 134).
- В журнале событий отсутствуют следующие ошибки в работе программы:
  - ApplicationStopped – Событие об аварийном завершении работы программы.
  - PolicyNotApplied – Событие о том, что основная политика не применилась.
  - IntegrityCheckFailed – Нарушена целостность файлов или модулей программы.
  - LicenseNotInstalled – Ошибка добавления ключа.
  - LicenseExpired – Истек срок действия лицензии.
  - LicenseRevoked - Ключ успешно удален (при условии, что это единственный ключ и нет действующего дополнительного ключа).

- AVBasesAreTotallyOutOfDate – Базы программы сильно устарели.
- AVBasesIntegrityCheckFailed – Нарушена целостность баз программы при условии, что базы программы сильно устарели.

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 задача Защита от файловых угроз остановлена.

Перед началом проверки убедитесь, что выполнены следующие условия:

- Программа готова к работе (см. раздел "Подготовка программы к работе" на стр. 18).
- Программа находится в сертифицированном состоянии (см. раздел "Сертифицированное состояние программы" на стр. 326).

Проверка работоспособности программы

1. Убедитесь, что программа активирована, антивирусные базы обновлены и запущена задача Защита от файловых угроз (*File_Monitoring*). Для этого выполните команду:

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

   Ожидаемый результат: программа выводит на экран следующую информацию:

   ```
   Key status : Valid
   Anti-virus databases loaded : Yes
   File monitoring : Available and running
   ```

2. Остановите задачу Защита от файловых угроз (*File_Monitoring*), выполнив следующую команду:

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

3. 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.

4. Запустите задачу Защита от файловых угроз (*File_Monitoring*), выполнив следующую команду:

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

5. 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.

6. Убедитесь, что зараженный файл был удален из директории компьютера.
7. Проверьте наличие событий об удалении зараженного файла, выполнив следующую команду:

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

kaspersky

Лицензирование программы

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

В этом разделе

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения. *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 документ license.<ID языка>. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время первоначальной настройки программы.

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

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 использования программы зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

- *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, нужно продлить срок действия коммерческой лицензии.

- *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.

Активация программы по пробной лицензии приводит к выходу программы из сертифицированного состояния.

Об активации программы

Активация программы – это процедура введения в действие *лицензии*, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии (см. раздел "*О лицензии*" на стр. 33).

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

Вы можете добавить ключ в программу одним из следующих способов: применить *файл ключа* или ввести *код активации. Код активации* – это уникальная последовательность из двадцати латинских букв и цифр.

Использование кода активации для добавления ключа приводит к выходу программы из сертифицированного состояния.

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского".

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

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

Для добавления ключа используется задача Лицензия (`License` – задача, реализующая сервер лицензий) или задача **Добавление ключа** в Kaspersky Security Center.

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

Ключ может быть активным и дополнительным.

Активный ключ – лицензионный ключ, используемый в текущий момент для работы программы. В программе не может быть больше одного активного ключа.

Дополнительный ключ – лицензионный 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 при наличии активного ключа.

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, версию и локализацию установленной программы, версии установленных обновлений программы, идентификатор компьютера и идентификатор установки программы на компьютере, код активации и уникальный идентификатор активации текущей лицензии, тип, версию и разрядность операционной системы, название виртуальной среды, если программа установлена в виртуальной среде, идентификаторы компонентов программы, активных на момент предоставления информации).

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 об отправке в "Лабораторию Касперского" статистической информации, полученной во время использования KSN, ее хранении и уничтожении вы можете прочитать в Лицензионном соглашении, Положении о Kaspersky Security Network и Политике конфиденциальности на веб-сайте "Лаборатории Касперского" (https://www.kaspersky.com/products-and-services-privacy-policy). Файлы с текстами Лицензионного соглашения и Положения о Kaspersky Security Network license.<ID языка> и ksn_license.<ID языка> входят в комплект поставки программы.

Разделение доступа к функциям программы по пользовательским ролям

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

Роль Администратора выдается пользователю с правами учетной записи root на текущую терминальную сессию на один час. Администратор имеет доступ ко всем функциям программы.

Чтобы получить роль администратора, пользователю с правами учетной записи root нужно запустить команду `kesl-control --admin-session`.

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

Роль пользователя позволяет:

- Управлять временными задачами выборочной проверки (Scan_File).
- Просматривать в списке запущенных задач только собственные задачи Scan_File_xxx и задачи обновления.
- Выполнять проверку только тех файлов, к которым разрешен доступ конкретному пользователю.

Роль пользователя не позволяет:

- Управлять параметрами и задачами программы.
- Управлять лицензированием программы.
- Управлять Хранилищем
- Просматривать события и отчеты.

kaspersky

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
  ```

kaspersky

Общие параметры Kaspersky Endpoint Security

Общие параметры конфигурационного файла имеют следующие значения:

SambaConfigPath

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

По умолчанию указана стандартная директория конфигурационного файла Samba на компьютере.

После изменения значения этого параметра требуется перезапуск программы.

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

NfsExportPath

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

По умолчанию указана стандартная директория конфигурационного файла NFS на компьютере.

После изменения значения этого параметра требуется перезапуск программы.

Значение по умолчанию: `/etc/exports`

TraceFolder

Директория, в которой хранятся файлы трассировки программы.

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

После изменения значения этого параметра требуется перезапуск программы.

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

TraceLevel

Уровень детализации журнала трассировки.

Доступные значения:

`Detailed` – наиболее детализированный журнал трассировки.

`NotDetailed` – журнал трассировки содержит оповещения об ошибках.

`None` – не создает журнал трассировки.

Значение по умолчанию: `None`.

TraceMaxFileCount

Максимальное количество файлов трассировки программы.

Файлы трассировки для текущего и для завершенных процессов трассировки считаются отдельно. Например, если для параметра `TraceMaxFileCount` указано значение 2, то максимально может храниться 4 файла трассировки: два файла для текущего процесса трассировки и два файла для завершенных процессов.

После изменения значения этого параметра требуется перезапуск программы.

Возможные значения: `1 – 99`.

Значение по умолчанию: `2`.

TraceMaxFileSize

Максимальный размер файла трассировки программы (в мегабайтах).

После изменения значения этого параметра требуется перезапуск программы.

Возможные значения: `1 – 1000`.

Значение по умолчанию: `250`.

BlockFilesGreaterMaxFileNamePath

Блокирование доступа к файлам, длина полного пути к которым превышает заданное значение параметра, в байтах.

Если длина полного пути к проверяемому файлу превышает значение этого параметра, задачи антивирусной проверки пропускают такой файл при проверке.

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

Возможные значения: `4096 – 33554432`.

Значение по умолчанию: `16384`.

DetectOtherObjects

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

UseKSN

Включает или выключает участие в Kaspersky Security Network.

Доступные значения:

`No` – выключить участие в Kaspersky Security Network.

`Basic` – включить участие в Kaspersky Security Network без отправки статистики.

`Extended` – включить участие в Kaspersky Security Network с отправкой статистики.

`SafeStatisticsToFile` – сохранять детектирующие статистики в файле формата JSON. Файлы со статистиками за каждую дату, отличную от текущей, упаковываются в отдельный tar-архив.

При этом программа не осуществляет отправку запросов и статистик в Kaspersky Security Network.

Значение по умолчанию: `No`.

KSNStatisticsFileSizeLimit

Максимальный размер файлов статистики (в мегабайтах). После изменения значения этого параметра требуется перезапуск программы.

Возможные значения: `1 – 9999`.

Значение по умолчанию: `1024`.

KSNStatisticsFileFolder

Директория, в которой сохраняются файлы статистики. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, с правами которой работает Kaspersky Endpoint Security. После изменения значения этого параметра требуется перезапуск программы.

Значение по умолчанию: `/var/log/kaspersky/kesl/common/offline-ksn-stats`

UseProxy

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

Доступные значения:

`Yes` – включить использование прокси-сервера.

`No` – выключить использование прокси-сервера.

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 правами учетной записи root. Если задано значение `0`, непривилегированный пользователь не может запускать задачи типа `Scan_File`.

Возможные значения: `0 – 4294967295`.

Значение по умолчанию: `0`.

UseSysLog

Включает или выключает запись информации о событиях в syslog.

Доступные значения:

`Yes` – включить запись информации о событиях в syslog.

`No` – выключить запись информации о событиях в syslog.

Значение по умолчанию: `No`.

UIReportsForRootOnly

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

Доступные значения:

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

`No` – разрешить просмотр отчетов из графического пользовательского интерфейса непривилегированным пользователям.

Значение по умолчанию: `No`.

В сертифицированной версии программы графический пользовательский интерфейс (GUI) недоступен.

EventsStoragePath

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

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

ExcludedMountPoint

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

Доступные значения:

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

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

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

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

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

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

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

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

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

Параметр `ExcludedMountPoint` не указан по умолчанию.

kaspersky

В этой главе

Команды управления параметрами Kaspersky Endpoint Security и задачами

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

Получение общих параметров Kaspersky Endpoint Security

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

Синтаксис команды

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

Аргументы и ключи

`--file <имя конфигурационного файла>`

Имя конфигурационного файла, в котором будут сохранены параметры Kaspersky Endpoint Security. Если вы укажете имя файла, не указав пути к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, конфигурационный файл не будет создан.

Пример:

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

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

Изменение общих параметров Kaspersky Endpoint Security

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

Для изменения параметров программы требуется наличие прав учетной записи root.

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

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

Синтаксис команды

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

Аргументы и ключи

`--file <имя конфигурационного файла>`

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

Примеры:

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

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

Установить низкий уровень детализации журнала трассировки:

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

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

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

Вывод справки о командах Kaspersky Endpoint Security

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

Синтаксис команды

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

где `<набор команд Kaspersky Endpoint Security>` может принимать следующие 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 управления Сетевым экраном.

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

[-S] – команды для управления статистикой.

-W – вывод событий.

Просмотр информации о программе

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

Синтаксис команды

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

Результат выполнения команды

Name

Название программы.

Version

Текущая версия программы.

Key status

Статус ключа.

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 задачи Защита от файловых угроз.

Integrity monitoring

Состояние задачи мониторинга файловых операций.

Firewall

Состояние задачи управления Сетевым экраном.

В сертифицированной версии программы задача управления Сетевым экраном недоступна.

Anti-Cryptor

Состояние задачи Защита от шифрования.

Application update state

Отображает наличие обновлений программы.

Команды Kaspersky Endpoint Security

Вы можете менять значения параметров Kaspersky Endpoint Security из командной строки.

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 и 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>`

Команды `--suspend-task` и `--resume-task` недоступны для задач Update (ID=6), Rollback (ID=7) и Retranslate (ID=8).

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 <полный путь к конфигурационному файлу>`

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 управления 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.

В сертифицированной версии программы задача управления Сетевым экраном недоступна.

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>`

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

`--limit`

Максимальное количество событий, о которых выводится информация

`--offset`

Количество записей, на которое следует отступить от начала выборки.

`--file`

Имя файла для вывода событий и путь к нему

`--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 или 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).

`RunMissedStartRules`

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

Пример:

Чтобы установить запуск задачи каждые десять часов, укажите следующие параметры:

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2019/May/30 23:05:00;10
RandomInterval=0
```

Экспорт и импорт параметров программы

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

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

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

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

При импорте параметров программы для параметра `UseKSN` устанавливается значение `No`. Чтобы начать или возобновить участие в Kaspersky Security Network, требуется ввести `UseKSN=Basic` или `UseKSN=Extended`.
При импорте параметров в сертифицированной версии программы также устанавливаются следующие значения для параметров:
`USE_GUI=No`,
параметр задачи Update `ApplicationUpdateMode=Disabled`,
параметр задачи Retranslate `AutoPatchDownload=No`,
все параметры задачи Firewall сбрасываются, т.к. задача недоступна.

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

- *Чтобы экспортировать параметры программы в конфигурационный файл, выполните следующую команду:*

```
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>
```

kaspersky

Управление задачами Kaspersky Endpoint Security с помощью командной строки

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

В этой главе

О задачах Kaspersky Endpoint Security

Вы можете управлять работой Kaspersky Endpoint Security с помощью задач как локально на компьютере (с помощью командной строки или конфигурационных файлов), так и централизованно через Kaspersky Security Center (см. раздел "Управление программой через Kaspersky Security Center" на стр. 115).

Различают 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.

Для работы с Kaspersky Endpoint Security предусмотрены следующие задачи:

- `File_Monitoring` – задача Защита от файловых угроз (ID=1, тип – OAS).
- `Scan_My_Computer` – задача антивирусной проверки (ID=2, тип – ODS).

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

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

Вы можете выполнять следующие действия над задачами:

- запускать и останавливать выполнение задач, а также приостанавливать и возобновлять выполнение некоторых задач;
- 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
```

Для каждой задачи отображается следующая информация:

- `Название`. Имя задачи.
- `ID`. Идентификатор задачи (см. раздел "О задачах Kaspersky Endpoint Security" на стр. 47).
- `Type`. Тип задачи (см. раздел "О задачах Kaspersky Endpoint Security" на стр. 47).
- `State`. Текущее состояние задачи.

Если в политике для Kaspersky Endpoint Security пользователю запрещено просматривать и изменять параметры задач, то отображается только информация о задачах Scan_File, File_Monitoring, Backup, License, Integrity_Monitor и Anti_Cryptor. Информация о других задачах недоступна. Если ваша лицензия не предоставляет 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" (на стр. 47).

kaspersky

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>
```

где:

- `<имя задачи>` – имя, которое вы указываете для новой задачи;
- `<тип задачи>` - предустановленный тип задачи (см. раздел "О задачах Kaspersky Endpoint Security" на стр. 47).

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>
```

где:

- `<имя задачи>` – имя, которое вы указываете для новой задачи;
- `<тип задачи>` – предустановленный тип задачи (см. раздел "О задачах Kaspersky Endpoint Security" на стр. 47).
- `<полный путь к конфигурационному файлу>` – полный путь к конфигурационному файлу (см. раздел "Конфигурационные файлы задачи по умолчанию" на стр. 130)

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

Изменение параметров задачи с помощью конфигурационного файла

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

1. Сохраните параметры задачи в конфигурационный файл:

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

2. Откройте созданный конфигурационный файл для редактирования.
3. Измените нужный параметр в конфигурационном файле.
4. Сохраните изменения в конфигурационном файле.

5. Импортируйте в задачу параметры из конфигурационного файла:

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

В результате задача будет сохранена с обновленными параметрами.

Изменение параметров задачи с помощью командной строки

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

1. Укажите нужное значение параметра:

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

   Kaspersky Endpoint Security изменит указанный параметр.

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

   ```
   kesl-control --get-settings <имя или идентификатор задачи>
   ```

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

Запуск и остановка задачи

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

► *Чтобы запустить задачу, выполните следующую команду:*

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

► *Чтобы остановить задачу, выполните следующую команду:*

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

Приостановка и возобновление задачи

Вы можете приостанавливать и возобновлять выполнение задач типов Scan_My_Computer, Scan_File, Boot_Scan и Memory_Scan.

► *Чтобы приостановить задачу, выполните следующую команду:*

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

После выполнения команды выполнение задачи приостанавливается.

► *Чтобы возобновить задачу, выполните следующую команду:*

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

После выполнения команды выполнение задачи возобновляется.

Управление областями проверки из командной строки

Вы можете добавлять или удалять область проверки с указанным параметром `Path` для задач проверки, Защита от файловых угроз и Защита от шифрования из командной строки.

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

```
kesl-control --set-settings <идентификатор 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 <идентификатор или имя задачи> --del-path
<путь>
```

Блок `[ScanScope.item_#]`, содержащий указанный путь, будет удален 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 проверки, Защита от файловых угроз и Защита от шифрования из командной строки.

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

```
kesl-control --set-settings <идентификатор 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 <идентификатор или имя задачи> --del-exclusion <путь>
```

Блок `[ExcludedFromScanScope.item_#]`, содержащий указанный путь, будет удален 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>
```

где:

- `<ID задачи>` – идентификатор задачи, который Kaspersky Endpoint Security присваивает задаче при создании.
- `<имя задачи>` – имя 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.

Получение параметров расписания задачи

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

Вы можете использовать эту команду для изменения расписания задачи.

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

1. Сохраните параметры расписания задачи в конфигурационном файле с помощью следующей команды:

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

2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры расписания в задачу с помощью следующей команды:

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

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
```

Изменение параметров расписания задачи

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

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

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

   Kaspersky Endpoint Security применит новые значения параметров расписания немедленно.

Синтаксис команды

```
kesl-control --set-schedule <ID задачи>|<имя задачи> --file <имя конфигурационного файла>
```

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

Аргументы и ключи

`<ID задачи>`

Идентификационный номер задачи в Kaspersky Endpoint Security.

`<имя задачи>`

Имя задачи.

`--file <имя конфигурационного файла>`

Имя конфигурационного файла, параметры расписания из которого будут импортированы в задачу; включает полный путь к файлу.

Пример:

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

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

Удаление задачи

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

► *Чтобы удалить задачу, выполните следующую команду:*

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

Задача Защита от файловых угроз (File_Monitoring ID:1)

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

В этой главе

О защите от файловых угроз

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

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

Для запуска и остановки задачи Защита от файловых угроз из командной строки требуется учетная запись root.

Нельзя создать пользовательскую задачу Защита от файловых угроз. Вы можете изменить параметры задачи Защиты от файловых угроз, заданные по умолчанию (см. раздел «Управление задачами Kaspersky Endpoint Security с помощью командной строки" на стр. 116).

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

Особенности проверки символических и жестких ссылок

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

Проверка символических ссылок

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

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

Проверка жестких ссылок

Когда программа 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), программа Kaspersky Endpoint Security автоматически подбирает и выполняет действие над объектом на основе данных об опасности обнаруженной в объекте угрозы и возможности его лечения.
- Если выбрано действие **Удалять** (Remove), Kaspersky Endpoint Security удаляет обрабатываемую жесткую ссылку. Остальные жесткие ссылки на этот файл обработаны не будут.
- Если выбрано действие **Лечить** (Cure), Kaspersky Endpoint Security лечит исходный файл. Если лечение невозможно, программа удаляет жесткую ссылку и создает вместо нее копию исходного файла с именем удаленной жесткой ссылки.

Когда вы восстанавливаете файл с жесткой ссылкой из хранилища, Kaspersky Endpoint Security создает копию исходного файла с именем жесткой ссылки, которая была помещена в хранилище. Связи с остальными жесткими ссылками на исходный файл восстановлены не будут.

Параметры задачи Защита от файловых угроз

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Защита от файловых угроз. Описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanArchived

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

Доступные значения:

`Yes` – проверять архивы.

`No` – не проверять архивы.

Значение по умолчанию: `No`

ScanSfxArchived

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

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы.

`No` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `No`.

ScanMailBases

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

Доступные значения:

`Yes` – проверять файлы почтовых баз.

`No` – не проверять файлы почтовых баз.

Значение по умолчанию: `No`.

ScanPlainMail

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

SizeLimit

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

Доступные значения:

`0` – `999999`.

`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 в значении параметра.

Доступные значения:

`0` – `9999`.

`0` – продолжительность проверки объектов не ограничена.

Значение по умолчанию: `60`.

FirstAction

Выбор первого действия Kaspersky Endpoint Security над зараженными объектами.

Перед тем как выполнить над объектом выбранное вами действие, Kaspersky Endpoint Security блокирует доступ к этому объекту для программ, которые к нему обращаются.

Доступные значения:

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

предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным. Если первым действием выбрано `Cure`, рекомендуется задать второе действие в параметре `SecondAction`.

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

`Recommended` (выполнять рекомендуемое действие) – Kaspersky Endpoint Security автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские программы, так как они не заражают другие файлы и поэтому не предполагают лечения.

`Block` (блокировать) – Kaspersky Endpoint Security блокирует доступ к зараженному объекту. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию: `Recommended`.

SecondAction

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

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

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

Значение по умолчанию: `Block`.

UseExcludeMasks

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ExcludeMasks

Исключает из проверки объекты по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски.

Значение по умолчанию не задано.

Пример:

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

UseExcludeThreats

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ExcludeThreats

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

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

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

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

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

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

ReportCleanObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ReportPackedObjects

Включает или отключает запись в журнал информации о проверенных объектах, которые являются частью составных объектов.

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

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

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

Значение по умолчанию: `No`.

UseAnalyzer

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

Доступные значения:

`Yes` – включить эвристический анализатор.

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`.

HeuristicLevel

Уровень эвристического анализа.

Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.

Доступные значения:

`Light` – наименее тщательная проверка, минимальная загрузка системы.

`Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы.

`Deep` – наиболее тщательная проверка, максимальная загрузка системы.

`Recommended` – рекомендуемое значение.

Значение по умолчанию: `Recommended`.

UseIChecker

Включает или отключает использование технологии iChecker.

Доступные значения:

`Yes` – включить использование технологии iChecker.

`No` – отключить использование технологии iChecker.

Значение по умолчанию: `Yes`.

ScanByAccessType

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

Доступные значения:

`SmartCheck` – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс во время своей работы многократно обращается к файлу в течение некоторого времени и изменяет его, повторно проверять файл только при последней попытке закрытия файла этим процессом.

`OpenAndModify` – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.

`Open` – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.

Значение по умолчанию: `SmartCheck`.

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

AreaDesc

Описание области проверки; содержит дополнительную информацию об области проверки. Максимальная длина строки – 4096 символов.

Значение по умолчанию: `All objects`.

Пример:

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

UseScanArea

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

Доступные значения:

`Yes` – проверять указанную область.

`No` – не проверять указанную область.

Значение по умолчанию: `Yes`.

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

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

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

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

Пример:

```
AreaMask=*doc
```

Path

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

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

Доступные значения:

`<путь к локальной директории>` – проверять объекты в указанной директории. Для указания пути можно использовать маски.

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

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

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

`Shared:NFS` – 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.

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область.

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

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

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

Доступные значения:

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

`Shared:NFS` – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS.

`Shared:SMB` – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется 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, доступ к которым предоставляется по протоколам SMB и NFS.

kaspersky

Задача антивирусной проверки (Scan_My_Computer ID:2)

В этом разделе содержится информация о задаче антивирусной проверки.

Об антивирусной проверке

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

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

Пользователи могут создавать пользовательские задачи антивирусной проверки.

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

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

О задаче выборочной проверке (Scan_File ID:3)

С помощью задачи выборочной проверки Scan_File вы можете проверить файл или директорию.

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

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

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

Параметры задачи антивирусной проверки

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

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

ScanArchived

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

Доступные значения:

`Yes` – проверять архивы.

`No` – не проверять архивы.

Значение по умолчанию: `Yes`.

ScanSfxArchived

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

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы.

`No` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `Yes`.

ScanMailBases

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

Доступные значения:

`Yes` – проверять файлы почтовых баз.

`No` – не проверять файлы почтовых баз.

Значение по умолчанию: `No`.

ScanPlainMail

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

UseSizeLimit

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

Доступные значения:

`Yes` – применять параметр `SizeLimit`.

`No` – не применять параметр `SizeLimit`.

Значение по умолчанию: `No`.

SizeLimit

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

Этот параметр применяется совместно с параметром `UseSizeLimit`.

Доступные значения:

`0` – `999999`.

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

Значение по умолчанию: `0`.

UseTimeLimit

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

Доступные значения:

`Yes` – применять параметр `TimeLimit`.

`No` – не применять параметр `TimeLimit`.

Значение по умолчанию: `No`.

TimeLimit

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

Этот параметр применяется совместно с параметром `UseTimeLimit`.

Доступные значения:

`0` – `9999`.

`0` – продолжительность проверки объектов не ограничена.

Значение по умолчанию: `0`.

FirstAction

Выбор первого действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

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

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

`Recommended` (выполнять рекомендуемое действие) – Kaspersky Endpoint Security автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские программы, так как они не заражают другие файлы и поэтому не предполагают лечения.

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

Значение по умолчанию: `Recommended`.

SecondAction

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

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

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

Значение по умолчанию: `Skip`.

UseExcludeMasks

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ExcludeMasks

Исключает из проверки объекты по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате командной оболочки.

Значение по умолчанию не задано.

Пример:

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

UseExcludeThreats

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ExcludeThreats

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

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

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

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

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

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

ReportCleanObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ReportPackedObjects

Включает или отключает запись в журнал информации о проверенных объектах, которые являются частью составных объектов.

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

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

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

Значение по умолчанию: `No`.

UseAnalyzer

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

Доступные значения:

- `Yes` – включить эвристический анализатор;
- `No` – отключить эвристический анализатор.

Значение по умолчанию: `yes`.

HeuristicLevel

Уровень эвристического анализа.

Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.

Доступные значения:

`Light` – наименее тщательная проверка, минимальная загрузка системы.

`Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы.

`Deep` – наиболее тщательная проверка, максимальная загрузка системы.

`Recommended` – рекомендуемое значение.

Значение по умолчанию: `Recommended`.

UseIChecker

Включает или отключает использование технологии iChecker.

Доступные значения:

`Yes` – включить использование технологии iChecker.

`No` – отключить использование технологии iChecker.

Значение по умолчанию: `Yes`.

ScanByAccessType

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

Доступные значения:

`SmartCheck` – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс во время своей работы многократно обращается к файлу в течение некоторого времени и изменяет его, повторно проверять файл только при последней попытке закрытия файла этим процессом.

`OpenAndModify` – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.

`Open` – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.

Значение по умолчанию: `SmartCheck`.

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

AreaDesc

Описание области проверки; содержит дополнительную информацию об области проверки. Максимальная длина строки – 4096 символов.

Значение по умолчанию: `All objects`.

Пример:

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

UseScanArea

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

Доступные значения:

`Yes` – проверять указанную область.

`No` – не проверять указанную область.

Значение по умолчанию: `Yes`.

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

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

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

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

Пример:

```
AreaMask=*doc
```

Path

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

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

Доступные значения:

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

`Shared:NFS` – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS.

`Shared:SMB` – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу SMB.

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

`AllShared` – проверять все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам SMB и NFS.

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

AreaDesc

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

Значение по умолчанию не задано.

Пример:

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

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область.

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

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

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

Доступные значения:

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

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

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

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

`Shared:NFS` – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS.

`Shared:SMB` – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется 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, доступ к которым предоставляется по протоколам SMB и NFS.

kaspersky

Задача проверки загрузочных секторов (Boot_Scan ID:4)

В этом разделе содержится информация о задаче проверки загрузочных секторов.

О задаче проверки загрузочных секторов

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

Параметры задачи проверки загрузочных секторов

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

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

UseExcludeMasks

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ExcludeMasks

Исключает из проверки объекты по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельное устройство по имени или несколько устройств, используя маски в формате командной оболочки.

Значение по умолчанию не задано.

UseExcludeThreats

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ExcludeThreats

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

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

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

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

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

ReportCleanObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ReportUnprocessedObjects

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

UseAnalyzer

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

Доступные значения:

- `Yes` – включить эвристический анализатор;
- `No` – отключить эвристический анализатор.

Значение по умолчанию: `yes`.

HeuristicLevel

Уровень эвристического анализа.

Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.

Доступные значения:

`Light` – наименее тщательная проверка, минимальная загрузка системы.

`Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы.

`Deep` – наиболее тщательная проверка, максимальная загрузка системы.

`Recommended` – рекомендуемое значение.

Значение по умолчанию: `Recommended`.

Action

Выбор действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

`Cure` (лечить) – Kaspersky Endpoint Security пытается вылечить объект. 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.

О задаче проверки памяти процессов

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

Параметры задачи проверки памяти процессов

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

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

UseExcludeThreats

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ExcludeThreats

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

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

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

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

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

ReportCleanObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

ReportUnprocessedObjects

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

Доступные значения:

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

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

Значение по умолчанию: `No`.

Action

Выбор действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

`Cure` (лечить) – Kaspersky Endpoint Security пытается остановить вредоносный процесс.

`Skip` (пропускать) – Kaspersky Endpoint Security не пытается остановить вредоносный процесс. Информация о вредоносном процессе сохраняется в журнале.

Значение по умолчанию: `Cure`.

kaspersky

Задача обновления (Update ID:6)

В этом разделе содержится информация о задаче обновления.

В этой главе

Об обновлении баз и модулей программы

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

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

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

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

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

В процессе обновления 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 и модули программы давно не обновлялись, то пакет обновлений может иметь значительный размер. Загрузка такого пакета обновлений может создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

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

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

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.

Об источниках обновлений

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

Если по каким-то причинам вы не можете использовать в качестве источника обновлений серверы обновлений "Лаборатории Касперского", вы можете получать обновления из *пользовательского источника обновлений* – из указанной вами локальной или сетевой директории (SMB / NFS), смонтированной пользователем, или с FTP- , HTTP- или HTTPS-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 HTTPS.

`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 HTTPS-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 HTTPS-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:

`Disabled` – не загружать и не устанавливать обновления программы.

Для сохранения сертифицированной конфигурации программы значение параметра `ApplicationUpdateMode` должно быть `Disabled`.

ConnectionTimeout

С помощью этого параметра вы можете указать время ожидания (в секундах) ответа от источника обновлений – HTTPS-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=https://example.com/bases/ – адрес HTTPS-сервера, на котором
находится 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 должна быть установлена программа Kaspersky Endpoint Security. Для обновления программы Kaspersky Endpoint Security не требуется останавливать ее работу. Если процесс обновления

завершается с ошибкой, Kaspersky Endpoint Security автоматически откатывает обновления до предыдущей версии.

Пользователи сертифицированных версий могут устанавливать только обновления программы, прошедшие процедуру сертификации. Дистрибутивы обновленных версий доступны на сайте https://certifiedbuilds.kaspersky.ru/.

Установка обновлений, не прошедших процедуру сертификации, приводит к выходу программы из сертифицированного состояния.

Задача отката обновлений (Rollback ID:7)

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

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

Задача отката обновлений не имеет 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.

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 HTTPS.

`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 HTTPS-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 HTTPS-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 – HTTPS-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=https://example.com/bases/` – адрес HTTPS-сервера, на котором находится директория с обновлениями.

`URL=/home/bases/` – директория на защищаемом компьютере, в которой содержатся базы программы.

Enabled

Включает или выключает использование источника обновлений, указанного в параметре `URL`. Для выполнения задачи необходимо, чтобы использование хотя бы одного источника обновлений было включено.

Доступные значения:

`Yes` – Kaspersky Endpoint Security использует источник обновления.

`No` – Kaspersky Endpoint Security не использует источник обновления.

Значение по умолчанию не задано.

AutoPatchDownload

Включает или выключает загрузку обновлений программы.

Доступные значения:

`No` – не загружать обновления программы.

kaspersky

Задача Лицензия (License ID:9)

В этом разделе содержится информация о задаче Лицензия.

В этой главе

О задаче Лицензия

Задача Лицензия позволяет управлять ключами Kaspersky Endpoint Security.

Добавление активного ключа

Команда `kesl-control --install-active-key` добавляет активный ключ.

Синтаксис команды

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

Аргументы и ключи

`<путь к файлу ключа>`

Путь к файлу ключа; если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

Добавить ключ из файла /home/test/00000001.key в качестве активного:

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

Добавление дополнительного ключа

Команда `kesl-control --install-additional-key` добавляет дополнительный ключ.

Если активный ключ не добавлен, то дополнительный ключ будет добавлен 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:

Добавить дополнительный ключ из файла /home/test/00000002.key:

```
kesl-control --install-additional-key /home/test/00000002.key
```

Удаление активного ключа

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

Синтаксис команды

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

Удаление дополнительного ключа

Команда `kesl-control --revoke-additional-key` удаляет дополнительный ключ.

Синтаксис команды

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

kaspersky

Задача управления Хранилищем (Backup ID:10)

В этом разделе содержится информация о задаче управления Хранилищем.

В этой главе

О Хранилище

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

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, пользователь может попытаться восстановить файл из его вылеченной копии в директорию исходного размещения файла.

Параметры задачи управления 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 управления Хранилищем и перезапустите Kaspersky Endpoint Security.

Если указанной директории не существует или она недоступна, Kaspersky Endpoint Security использует директорию Хранилища по умолчанию.

Значение по умолчанию: `/var/opt/kaspersky/kesl/common/objects-backup/`

Просмотр идентификаторов объектов в Хранилище

При помещении объекта в Хранилище Kaspersky Endpoint Security присваивает ему числовой идентификатор. Этот идентификатор используется для выполнения действий над объектом, таких как восстановление (см. раздел "Восстановление объектов из Хранилища" на стр. 91) или удаление (см. раздел "Удаление объектов из Хранилища" на стр. 91) объекта из Хранилища.

► *Чтобы просмотреть идентификаторы объектов в Хранилище,*

выполните команду: `kesl-control -B --query`

Идентификатор объекта отображается в строке `ObjectId`.

О восстановлении объектов из Хранилища

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

Вы можете восстанавливать объекты из Хранилища. Восстановление объектов может потребоваться в следующих случаях:

- При лечении зараженного файла Kaspersky Endpoint Security не удалось сохранить его целостность, и в результате информация в файле стала недоступной.
- Если вы считаете, что объект безопасен для сервера, и хотите использовать его, вы можете исключить объект из области проверки, и программа не будет обнаруживать его во время последующих проверок. Для этого вам нужно исключить объект по имени или по названию угрозы, обнаруженной при выполнении задачи Защита от файловых угроз, а также по имени объекта и по названию угрозы, обнаруженной в задаче антивирусной проверки.

Восстановление зараженных объектов может привести к заражению компьютера.

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

Восстановление объектов из Хранилища

► *Чтобы восстановить объект из Хранилища, выполните одно из следующих действий:*

- Если вы хотите восстановить объект с исходным именем и в исходное местоположение, выполните команду:

  ```
  kesl-control --restore <идентификатор объекта>
  ```

  где `<идентификатор объекта>` – идентификатор объекта в Хранилище.

- Если вы хотите восстановить объект с новым именем в указанную директорию, выполните команду:

  ```
  kesl-control --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 == '<object ID>'"
```

► *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
```

kaspersky

Задача мониторинга файловых операций (Integrity_Monitoring ID:11)

В этом разделе содержится информация о задаче Мониторинг файловых операций.

В этой главе

О мониторинге файловых операций

Задача Мониторинг файловых операций предназначена для отслеживания действий, выполняемых с файлами и директориями в области мониторинга, указанной в параметрах задачи. Вы можете использовать задачу, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом сервере.

Для использования функции мониторинга файловых операций требуется приобрести лицензию, которая включает эту функцию. 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. раздел "Мониторинг файловых операций при доступе (OAFIM)" на стр. 92). Кроме этого можно создавать и запускать задачи *Мониторинг файловых операций по требованию* (ODFIM) (см. на стр. 93).

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. Вы можете изменять области проверки и мониторинга в режиме реального времени. Если область мониторинга не указана, параметры задачи нельзя сохранить в конфигурационном файле. При добавлении области мониторинга или области исключения программа не проверяет, существует ли такая директория.

Вы можете указать несколько областей мониторинга.

Исключения из области мониторинга

Вы можете создавать исключения из области мониторинга. Исключения указываются для каждой отдельной области и работают только для указанной области мониторинга. Вы можете указать несколько областей исключения.

Исключения имеют более высокий приоритет, чем область мониторинга, и не проверяются задачей, даже если указанная папка или файл находятся в области мониторинга. Если параметры одного из правил указывают область мониторинга на более низком уровне, чем директория, указанная в исключении, область мониторинга не рассматривается при выполнении задачи.

Чтобы указать исключения, можно использовать те же маски в формате командной оболочки, которые используются для указания областей мониторинга.

Контролируемые параметры

Во время работы задачи Мониторинг файловых операций контролируется изменение следующих параметров:

- содержимое (write (), truncate (), etc.);
- метаданные (правообладание (chmod / chown));
- отметки времени (utimensat);
- расширенные атрибуты (setxattr) и другие.

Технологические ограничения операционной системы Linux не позволяют компоненту Мониторинг файловых операций определять, какой администратор или процесс внес изменение в файл.

Мониторинг файловых операций по требованию (ODFIM)

В ходе выполнения задачи ODFIM изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве *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 при доступе" на стр. 94). 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 или выключает исключение из области мониторинга объектов, указанных параметром `ExcludeMasks`.

Параметр `UseExcludeMasks` работает только с указанным параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

`No` – не исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

Значение по умолчанию: `No`.

ExcludeMasks

Указывает список масок, которые определяют объекты, исключаемые из области мониторинга.

Прежде чем указать этот параметр, убедитесь, что для параметра `UseExcludeMasks` выбрано значение `Yes`.

Маски указываются в формате командной оболочки.

Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (`ExcludeMasks.item_0000`, `ExcludeMasks.item_0001`).

Значение по умолчанию не задано.

Блок [ScanScope.item_#]

В блоках `[ScanScope.item_#]` указываются области мониторинга для задачи Мониторинг файловых операций. Для задачи должна быть указана минимум одна область мониторинга.

Вы можете указать в конфигурационном файле несколько блоков `[ScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

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

AreaDesc

Указывает имя области мониторинга.

UseScanArea

Включает или выключает мониторинг указанной области.

Доступные значения:

`Yes` – контролировать указанную область.

`No` – не контролировать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает полный путь к объекту или директориям для мониторинга.

Значение по умолчанию: `/opt/kaspersky/kesl/`

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

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

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

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты 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).

[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_#]`.

Можно указать в конфигурационном файле несколько блоков `[ExcludedFromScanScope.item_#]` в любом порядке. Программа Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

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

AreaDesc

Указывает имя области, которую нужно исключить из мониторинга.

UseScanArea

Указывает, будут ли указанные области исключены из мониторинга.

Доступные значения:

`Yes` – исключать указанные области из мониторинга.

`No` – не исключать указанные области из мониторинга.

Значение по умолчанию: `Yes`.

Path

Указывает путь к объектам или директориям, исключенным из мониторинга. Для указания пути можно использовать маски.

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты, исключенные из мониторинга.

Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: `*` (будут контролироваться все объекты).

Параметры задачи Мониторинг файловых операций по требованию

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

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

RebuildBaseline

Включает или выключает повторное создание 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 или выключает проверку хеша (SHA-256).

Доступные значения:

`Yes` – включить проверку хеша.

`No` – выключить проверку хеша.

Значение по умолчанию: `No`.

TrackDirectoryChanges

Включает или выключает мониторинг директорий.

Доступные значения:

`Yes` – контролировать директории.

`No` – не контролировать директории.

Значение по умолчанию: `No`.

TrackLastAccessTime

Включает или выключает проверку времени последнего доступа к файлу. В операционной системе Linux это параметр `noatime`.

Доступные значения:

`Yes` – проверять время последнего доступа к файлу.

`No` – не проверять время последнего доступа к файлу.

Значение по умолчанию: `No`.

UseExcludeMasks

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

Этот параметр работает только с указанным параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

`No` – не исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

Значение по умолчанию: `No`

ExcludeMasks

Указывает список масок, которые определяют объекты, исключаемые из области мониторинга.

Прежде чем указать этот параметр, убедитесь, что для параметра `UseExcludeMasks` выбрано значение `Yes`.

Маски указываются в формате командной оболочки.

Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (`ExcludeMasks.item_0000`, `ExcludeMasks.item_0001`).

Значение по умолчанию не задано.

[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. Программа Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

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

AreaDesc

Указывает имя области мониторинга.

UseScanArea

Включает или выключает мониторинг указанной области.

Доступные значения:

`Yes` – контролировать указанную область;

`No` – не контролировать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает полный путь к объекту или директориям для мониторинга.

Значение по умолчанию: `/opt/kaspersky/kesl/`

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

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

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

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты 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).

[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_#]`.

Можно указать в конфигурационном файле несколько блоков `[ExcludedFromScanScope.item_#]` в любом порядке. Программа Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

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

AreaDesc

Указывает имя области, которую нужно исключить из мониторинга.

UseScanArea

Указывает, будут ли указанные области исключены из мониторинга.

Доступные значения:

`Yes` – исключать указанные области из мониторинга;

`No` – не исключать указанные области из мониторинга.

Значение по умолчанию: `Yes`.

Path

Указывает путь к объектам или директориям, исключенным из мониторинга. Для указания пути можно использовать маски.

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).

kaspersky

Задача Защита от шифрования (AntiCryptor ID:13)

В этом разделе содержится информация о задаче Защита от шифрования.

В этой главе

О задаче Защита от шифрования

Задача Защита от шифрования позволяет защитить ваши файлы в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования.

В ходе выполнения задачи Защита от шифрования программа Kaspersky Endpoint Security проверяет обращения удаленных компьютеров сети к файлам, расположенным в общих сетевых директориях защищаемого сервера. Если программа расценивает действия удаленного компьютера, получающего доступ к общим сетевым ресурсам, как шифрование, она добавляет этот компьютер в список недоверенных компьютеров и запрещает ему доступ к общим сетевым директориям.

Kaspersky Endpoint Security не расценивает действия как шифрование, если обнаруженная активность шифрования имеет место в директориях, исключенных из области задачи Защита от шифрования (см. раздел "Параметры задачи Защита от шифрования" на стр. 101).

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

Чтобы задача Защита от шифрования работала корректно необходимо, чтобы в операционной системе была установлена хотя бы одна из служб: Samba или NFS. Для службы NFS необходимо, чтобы был установлен пакет rpcbind.

Задача Защита от шифрования корректно работает с протоколами SMB1, SMB2, SMB3, NFS3, TCP / UDP и IP / IPv6. Работа с протоколами NFS2 и NFS4 не поддерживается. Мы рекомендуем настроить параметры сервера таким образом, чтобы протоколы NFS2 и NFS4 нельзя было использовать для подключения ресурсов.

Задача Защита от шифрования не блокирует доступ к сетевым файловым ресурсам, пока действия компьютера не расцениваются как вредоносные. Таким образом, минимум один файл будет зашифрован, прежде чем программа обнаружит вредоносную активность.

kaspersky

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. Программа Kaspersky Endpoint Security блокирует доступ к общим сетевым директориям для всех удаленных компьютеров в списке недоверенных компьютеров. Информация обо всех заблокированных компьютерах защищаемого сервера отправляется в Kaspersky Security Center.

Правила управления Сетевым экраном, созданные задачей Защита от шифрования, невозможно удалить с помощью утилиты iptables: Kaspersky Endpoint Security восстанавливает набор правил раз в минуту. Используйте команду `--allow-hosts`, чтобы разблокировать компьютер (см. раздел "Разблокирование заблокированных компьютеров" на стр. 104).

По умолчанию Kaspersky Endpoint Security удаляет недоверенные компьютеры из списка через 30 минут после добавления в список. Доступ компьютеров к сетевым файловым ресурсам восстанавливается автоматически после удаления недоверенного компьютера из списка. Вы можете изменять список заблокированных компьютеров и указывать период, после которого заблокированные компьютеры автоматически разблокируются.

Параметры задачи Защита от шифрования

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Защита от шифрования.

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

UseHostBlocker

Включает или выключает блокирование недоверенных компьютеров.

Если блокирование недоверенных компьютеров выключено, Kaspersky Endpoint Security все равно проверяет действия удаленных компьютеров с сетевыми файловыми ресурсами на наличие вредоносного шифрования, когда работает задача Защита от шифрования. При обнаружении вредоносного шифрования создается событие `EncryptionDetected`, но атакующий компьютер не блокируется.

Доступные значения:

`Yes` – включить блокирование недоверенных компьютеров.

`No` – выключить блокирование недоверенных компьютеров.

Значение по умолчанию: `Yes`.

BlockTime

Указывает длительность блокирования доступа к сетевым файловым ресурсам в минутах.

Изменение параметра `BlockTime` не влияет на длительность блокировки ранее заблокированных скомпрометированных компьютеров. Длительность блокирования не является динамическим значением и рассчитывается на момент блокирования.

Доступные значения:

Целые числа от `1` до `4294967295`

Значение по умолчанию: `30`.

UseExcludeMasks

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

Этот параметр работает только с указанным параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные в параметре `ExcludeMasks`, из области защиты.

`No` – не исключать объекты, указанные в параметре `ExcludeMasks`, из области защиты.

Значение по умолчанию: `No`.

ExcludeMasks

Указывает список масок, которые определяют объекты, исключаемые из области защиты.

Прежде чем указать этот параметр, убедитесь, что для параметра `UseExcludeMasks` выбрано значение `Yes`.

Маски указываются в формате командной оболочки.

Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (`ExcludeMasks.item_0000`, `ExcludeMasks.item_0001`).

Значение по умолчанию не задано.

Блок [ScanScope.item_#]

В блоках `[ScanScope.item_#]` указываются области, защищаемые Kaspersky Endpoint Security. Для задачи Защита от шифрования должна быть указана минимум одна область защиты.

Для задачи Защита от шифрования можно указывать только общие директории.

Вы можете указать в конфигурационном файле несколько блоков `[ScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

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

AreaDesc

Указывает имя области защиты.

Значение по умолчанию: `All Shared Folders`.

UseScanArea

Включает или выключает защиту указанной области.

Доступные значения:

`Yes` – защищать указанную область.

`No` – не защищать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает путь к защищаемым объектам.

Доступные значения:

Абсолютный путь, доступный через SMB / NFS (например, `Path=/tmp`)

`AllShared` – защищать все ресурсы, доступные через SMB / NFS.

`Shared:SMB <путь>` – защищать ресурсы, доступные через SMB.

`Shared:NFS <путь>` – защищать ресурсы, доступные через NFS.

Значение по умолчанию: `AllShared`.

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

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

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

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты 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_#]`.

Можно указать в конфигурационном файле несколько блоков `[ExcludedFromScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

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

AreaDesc

Указывает имя области, которую нужно исключить из проверки.

Значение по умолчанию: `All objects`.

UseScanArea

Указывает, будут ли указанные области исключены из защиты.

Доступные значения:

`Yes` – исключать указанные области из защиты.

`No` – не исключать указанные области из защиты.

Значение по умолчанию: `Yes`.

Path

Указывает путь к объектам, исключенным из защиты.

Вы можете указать только абсолютный путь к локальной директории (например, `/root /tmp/123`), которую не будет защищать задача Защита от шифрования.

Для указания пути можно использовать маски.

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.

kaspersky

Примеры:

Адреса IPv4:

```
dec - 192.168.0.1
dec - 192.168.0.0/24
```

Адреса IPv6:

```
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
hex - 2001:db8::ae21:ad12
hex - ::ffff:255.255.255.254
hex - ::
```

kaspersky

Проверка целостности компонентов программы

Программа Kaspersky Endpoint Security содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленник может подменить один или несколько файлов или исполняемых модулей программы файлами, содержащими вредоносный код. Чтобы избежать подмены модулей и файлов, в Kaspersky Endpoint Security предусмотрена проверка целостности компонентов программы.

Программа проверяет модули и файлы на наличие неавторизованных изменений или повреждений. Если модуль или файл программы имеет некорректную контрольную сумму, то он считается поврежденным.

Программа проверяет целостность *файла манифеста*, содержащего перечень файлов программы, целостность которых важна для корректной работы компонента программы.

Проверка целостности компонентов программы выполняется с помощью утилиты проверки целостности integrity_check_tool, расположенной в директории /opt/kaspersky/kesl/bin. В той же директории расположен файл манифеста integrity_check.xml, защищенный криптографической подписью "Лаборатории Касперского".

Для запуска утилиты проверки целостности требуется учетная запись root.

Для проверки целостности может быть использована как утилита, устанавливаемая вместе с программой, так и утилита на сертифицированном компакт-диске.

Рекомендуется запускать утилиту проверки целостности с сертифицированного компакт-диска, чтобы гарантировать целостность утилиты. При запуске с компакт-диска требуется указать полный путь к файлу манифеста в папке программы.

► *Чтобы проверить целостность компонентов программы, выполните следующую команду:*

```
integrity_check_tool -v[|--verify] -m [|--manifest] <путь к файлу>
```

где `<путь к файлу>` – путь к файлу манифеста. По умолчанию утилита использует файл integrity_check.xml, расположенный в папке /opt/kaspersky/kesl/bin.

Вы можете запустить утилиту проверки целостности со следующими необязательными параметрами:

`-h, --help` – вывод справки о параметрах утилиты.

`-V, --verbose` – расширенный вывод выполняемых действий и результатов. Если вы не укажете этот параметр, будут выводиться только ошибки, объекты, не прошедшие проверку, и суммарная статистика проверки.

`-L, --log-file <файл>`, где `<файл>` – имя файла для вывода событий, произошедших во время проверки. По умолчанию события выводится в стандартный поток stdout.

`-l, --log-level <0-1000>`, где `<0-1000>` – уровень детализации вывода событий. По умолчанию используется уровень детализации `0`.

Результат проверки каждого файла манифеста выводится рядом с названием файла манифеста в следующем виде:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата `0`).

`FAILED` – целостность файлов не подтверждена (код возврата не `0`).

kaspersky

Участие в Kaspersky Security Network

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

В этом разделе

Об участии в 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 угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний компонентов программы.

В зависимости от расположения инфраструктуры различают:

- Глобальный KSN – инфраструктура расположена на серверах "Лаборатории Касперского".
- Локальный KSN (Kaspersky Private Security Network) – инфраструктура расположена на сторонних серверах поставщика услуг, например, внутри сети интернет-провайдера.

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

Настройка использования Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе **Прокси-сервер KSN**. См. подробнее в документации Kaspersky Security Center.

При использовании Локального KSN статистическая информация и файлы с компьютеров, на которых установлен Kaspersky Security, не отправляются на серверы "Лаборатории Касперского".

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.

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 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 и расположен в директории `/opt/kaspersky/kesl/doc/ksn_license.<ID языка>`.

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 Kaspersky Security Center.

Настройка службы KSN Proxy выполняется в свойствах Сервера администрирования Kaspersky Security Center.

Участие в Kaspersky Security Network является добровольным. Программа предлагает участвовать в KSN во время первоначальной настройки программы. Вы можете начать или прекратить использование KSN в любой момент.

Включение и выключение использования Kaspersky Security Network

Настройка использования Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе **Прокси-сервер KSN**. См. подробнее в документации Kaspersky Security Center.

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

► *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 программа Kaspersky Endpoint Security, установленная на компьютере, работает под политикой, назначенной в Kaspersky Security Center, изменить значение параметра `UseKSN` можно только с помощью Kaspersky Security Center.

Если программа Kaspersky Endpoint Security, установленная на компьютере, выходит из-под политики, устанавливается значение параметра `UseKSN=No`.

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 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 угроз не отправляются.
- Если отображается статус `No`, Kaspersky Endpoint Security не подключен к Kaspersky Security Network.

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

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.

kaspersky

События

Во время работы Kaspersky Endpoint Security возникают события, отражающие изменение состояния антивирусной защиты сервера и состояния Kaspersky Endpoint Security в целом.

Для просмотра событий Kaspersky Endpoint Security из командной строки используйте команды управления журналом событий или команду `kesl-control -W`.

В Kaspersky Security Center вы можете своевременно получать информацию о событиях с помощью уведомлений. *Уведомление* – это сообщение с информацией о событии, которое произошло во время работы программы. Вы можете настроить уведомление администратора о событиях по электронной почте.

Подробную информацию о событиях и уведомлениях см. в документации Kaspersky Security Center.

Просмотр журнала событий в командной строке

Вы можете просмотреть события программы с помощью команд управления журналом событий.

Синтаксис команды

```
kesl-control [-E] --query "<поле><оператор сравнения> '<значение>' [и <поле> <оператор сравнения>'<значение>' ]* ] --limit --offset --file <имя файла и путь> --db <файл БД>
```

Аргументы и ключи

`--query`

Вывод информации о событиях, удовлетворяющих фильтру.

`--limit`

Максимальное количество событий, о которых выводится информация

`--offset`

Количество записей, на которое следует отступить от начала выборки.

`--file <имя файла и путь>`

Имя файла для вывода событий и путь к нему

`--db <файл БД>`

Имя файла базы данных.

Включение вывода событий из командной строки

Команда `kesl-control -W` включает режим вывода событий Kaspersky Endpoint Security. Вы можете использовать эту команду либо отдельно, либо вместе с командой `kesl-control --start-task`, чтобы отображать 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 событий через Kaspersky Security Center

► *Чтобы посмотреть список всех событий в работе Сервера администрирования Kaspersky Security Center, управляемых устройств и программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В рабочей области узла **Сервер администрирования** перейдите на закладку **События**.

   В списке отображаются события из выборки, которая в настоящий момент указана в раскрывающемся списке **Выборки событий**. События в списке не обновляются автоматически. Чтобы просмотреть последние события, обновите список по ссылке **Обновить**.

В Kaspersky Security Center вы можете выполнять следующие действия при просмотре событий:

- Выбирать выборку, события из которой должны отображаться в списке. Раскрывающийся список **Выборки событий** содержит предопределенные выборки (созданные по умолчанию), а также пользовательские выборки. Если пользователь не создавал собственные выборки, пользовательских выборок нет в списке.
- Добавлять или удалять графы из списка событий.
- Искать события в списке по ключевым словам.
- Просматривать подробную информацию о событии, выбранном в списке. Поле с подробной информацией о событии находится справа от списка событий.
- Создавать и настраивать выборки событий.
- Экспортировать и импортировать события выборки.
- Настраивать уведомления о событиях и экспорт событий в SIEM-систему.

Подробную информацию о работе с событиями см. в документации Kaspersky Security Center.

Настройка параметров событий Kaspersky Security

► *Чтобы настроить параметры событий, происходящих во время работы программы, 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. По правой клавише мыши откройте контекстное меню компьютера и выберите пункт **Свойства**.
4. В окне **Свойства: <Имя компьютера>** выберите раздел **Программы**.
5. В разделе **Программы** выберите **Kaspersky Endpoint Security 10.1.1 для Linux редакция под Эльбрус** в списке установленных программ и в контекстном меню программы выберите пункт **Свойства**.

Откроется окно **Параметры Kaspersky Endpoint Security 10.1.1 для Linux редакция под Эльбрус**.

6. В окне **Параметры Kaspersky Endpoint Security 10.1.1 для Linux редакция под Эльбрус** в списке слева выберите раздел **Настройка событий**.
7. В правой части окна выберите закладку с названием уровня важности событий, параметры которых вы хотите настроить:
   - **Критическое событие**.
   - **Отказ функционирования**.
   - **Предупреждение**.
   - **Информационное сообщение**.
8. Выберите типы событий, параметры которых вы хотите настроить:
   - Используйте клавиши **SHIFT** и **CTRL**, если вы хотите выбрать несколько типов событий.
   - Нажмите на кнопку **Выбрать все**, если вы хотите выбрать все типы событий.
9. Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства <N событий>**, где N – количество выбранных типов событий.
10. В блоке **Регистрация событий** установите флажок **На Сервере администрирования в течение (сут)**. Программа будет отправлять на Сервер администрирования Kaspersky Security Center события выбранных вами типов.
11. В поле ввода укажите количество дней, в течение которых события должны храниться на Сервере администрирования. Kaspersky Security Center удаляет события по истечении заданного времени.
12. В блоке **Уведомления о событиях** выберите способ уведомления:
    - **Уведомлять по электронной почте**.
    - **Уведомлять по SMS**.
    - **Уведомлять запуском исполняемого файла или скрипта**.
    - **Уведомлять по SNMP**.
13. Нажмите на кнопку **ОК** в окне **Свойства <N событий>**.
14. Нажмите на кнопку **ОК** в окне **Параметры Kaspersky Endpoint Security 10.1.1 для Linux редакция под Эльбрус**.

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 11.

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать программу Kaspersky Endpoint Security, настраивать параметры работы программы, 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 требуется 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:
  - добавления ключей;
  - копирования обновлений;
  - обновления;
  - отката обновлений;
  - проверки загрузочных секторов;
  - проверки памяти процессов;
  - антивирусной проверки;
  - проверки целостности файлов.

kaspersky

В этом разделе

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. По правой клавише мыши откройте контекстное меню компьютера и 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 10.1.1 для Linux редакция под Эльбрус**.
8. Выполните следующие действия:
   - Если вы хотите запустить программу, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  или выполните следующие действия:
     a. По правой клавише мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 для Linux редакция под Эльбрус и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ "Лаборатории Касперского".

        Откроется окно **Параметры Kaspersky Endpoint Security 10.1.1 для Linux редакция под Эльбрус** на закладке **Общие**.
     b. Нажмите на кнопку **Запустить**.

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

  a. По правой клавише мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 для Linux редакция под Эльбрус и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ.

  Откроется окно **Параметры Kaspersky Endpoint Security 10.1.1 для Linux редакция под Эльбрус** на закладке **Общие**.

  b. Нажмите на кнопку **Остановить**.

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. По правой клавише мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.
4. В окне **Свойства** выберите закладку **Защита**.

На закладке **Защита** отображается следующая информация о защищаемом компьютере:

- **Статус устройства** – информация об антивирусной безопасности защищаемого компьютера, например: *Базы устарели*, *Срок действия лицензии истек*.
- **Статус постоянной защиты** – состояние задачи Защита от файловых угроз, например: *Выполняется*, *Остановлена*.
- **Последняя проверка по требованию** – дата и время последнего выполнения задачи антивирусной проверки.
- **Всего обнаружено угроз** – 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**.
- **Активные угрозы** – количество зараженных объектов, которые 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. По правой клавише мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.
4. В окне **Свойства: <Имя компьютера>** выберите раздел **Программы**.

5. В разделе **Программы** выберите **Kaspersky Endpoint Security 10.1.1 для Linux редакция под Эльбрус** в списке установленных программ и в контекстном меню программы выберите пункт **Свойства**.

   Откроется окно **Параметры Kaspersky Endpoint Security 10.1.1 для Linux редакция под Эльбрус**.

В окне **Параметры Kaspersky Endpoint Security 10.1.1 для Linux редакция под Эльбрус** отображается следующая информация о Kaspersky Endpoint Security:

Раздел **Общие**

Номер версии – номер версии Kaspersky Endpoint Security.

Установлено – дата и время установки Kaspersky Endpoint Security на защищаемом компьютере.

Текущее состояние – состояние задачи Защита от файловых угроз, например: *Выполняется* или *Приостановлена*.

Последнее обновление ПО – дата и время последнего обновления программных модулей Kaspersky Endpoint Security.

Установленные обновления – список программных модулей, для которых установлены обновления.

Базы программы – дата и время последнего обновления антивирусных баз, а также количество записей в базах.

Раздел **Ключи**

Тип лицензии – тип лицензии, *коммерческая* или *пробная*.

Дата активации (поле доступно только для активного ключа) – дата добавления активного ключа;

Дата окончания срока действия лицензии (поле доступно только для активного ключа) – дата окончания срока годности активного ключа.

Срок действия – количество дней, в течение которых действует ключ.

Ограничение – количество компьютеров, на которых вы можете использовать ключ.

Раздел **Настройка событий**

В этом разделе вы можете просмотреть события, которые Kaspersky Endpoint Security сохраняет в хранилище событий.

Раздел **Дополнительно**

В этом разделе вы можете просмотреть информацию о плагине управления программой.

Управление политиками

Этот раздел содержит информацию о создании и настройке политик для Kaspersky Endpoint Security. Более подробную информацию о концепции управления программой Kaspersky Endpoint Security с помощью политик Kaspersky Security Center вы можете прочитать в документации Kaspersky Security Center.

О политиках

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

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

Возможность изменять параметр программы на клиентском компьютере определяется статусом "замка" у параметра в политике:

- Если параметр закрыт "замком" (), это означает, что вы не можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используется значение параметра, заданное политикой.
- Если параметр не закрыт "замком" (), это означает, что вы можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используются значения параметра, установленные локально. Значение параметра, установленное в политике, не применяется.

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

Вы можете использовать политики для настройки параметров таких задач Kaspersky Endpoint Security, как Защита от файловых угроз, Защита от шифрования, Мониторинг файловых операций при доступе и задача управления Хранилищем.

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, от имени 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 Kaspersky Security Center.

Создание политики

► *Чтобы создать политику, выполните следующие действия:*

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

3. В рабочей области выберите закладку **Политики**.
4. Нажмите на кнопку **Новая политика**, чтобы запустить мастер создания политики.
5. В окне Выбор программы для создания групповой политики выберите **Kaspersky Endpoint Security 10.1.1 для Linux редакция под Эльбрус**.
6. Следуйте указаниям мастера создания политики.

Изменение параметров политики

► *Чтобы изменить параметры политики, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием нужной группы администрирования, для которой вы хотите изменить параметры политики.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - По ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.
   - Двойным щелчком мыши.
   - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.
5. Измените параметры политики.
6. В окне **Свойства: <Название политики>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Управление задачами

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

Подробнее об управлении задачами через Kaspersky Security Center вы можете прочитать в документации Kaspersky Security Center.

О задачах для Kaspersky Endpoint Security

Kaspersky Security Center управляет работой программы Kaspersky Endpoint Security, установленной 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 компьютеров, указанных в параметрах задачи. Если в набор компьютеров, для которого сформирована задача, добавлены новые компьютеры, то для них эта задача не выполняется. В этом случае вам нужно создать новую задачу или изменить параметры уже существующей задачи.

Вы можете создавать следующие задачи:

- **Добавление ключа**. В процессе выполнения задачи Kaspersky Endpoint Security добавляет ключ, в том числе дополнительный, для активации программы.
- **Копирование обновлений**. В процессе выполнения задачи Kaspersky Endpoint Security скачивает антивирусные базы в указанную директорию, не устанавливая их.
- **Обновление**. В процессе выполнения задачи Kaspersky Endpoint Security обновляет антивирусные базы в соответствии с установленными параметрами обновления.
- **Откат обновлений**. В процессе выполнения задачи Kaspersky Endpoint Security откатывает последнее обновление антивирусных баз.
- **Поиск вирусов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет области компьютера, указанные в параметрах задачи, на вирусы и другие программы, представляющие угрозу.
- **Проверка загрузочных секторов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет загрузочные секторы компьютера.
- **Проверка системной памяти**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет системную память компьютера.
- **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 и останавливать выполнение задач;
- приостанавливать и возобновлять выполнение некоторых 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.

Общую информацию о задачах в Kaspersky Security Center вы можете прочитать в документации Kaspersky Security Center.

Создание локальной задачи

► *Чтобы создать локальную задачу, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева Консоли администрирования 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. По правой клавише мыши откройте контекстное меню компьютера и 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.

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.
3. В рабочей области выберите закладку **Задачи**.
4. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
5. Следуйте указаниям мастера создания задачи.

Создание задачи для набора компьютеров

► *Чтобы создать задачу для набора компьютеров, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Задачи**.
3. В рабочей области нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.
5. В окне мастера **Выбор устройств, которым будет назначена задача** нажмите кнопку **Назначить задачу выборке устройств**.
6. В окне мастера **Выборка устройств** нажмите кнопку **Обзор**.

   Откроется окно **Выборка устройств**.
7. Выберите нужное устройство и нажмите кнопку **ОК**.
8. Следуйте указаниям мастера создания задачи.

kaspersky

Запуск, остановка, приостановка и возобновление выполнения задачи вручную

Приостановка и возобновление выполнения задачи доступны только для задач **Поиск вирусов**, **Проверка загрузочных секторов**, **Проверка системной памяти** и **Проверка целостности файлов по требованию**.

Если на компьютере запущена программа Kaspersky Endpoint Security, вы можете запустить, остановить, приостановить или возобновить выполнение задачи на этом компьютере через Kaspersky Security Center. Если программа Kaspersky Endpoint Security остановлена, выполнение запущенных задач прекращается, а управление запуском, остановкой, приостановкой и возобновлением задач через Kaspersky Security Center становится невозможным.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, на котором вы хотите запустить, остановить, приостановить или 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 или возобновить.
8. По правой клавише мыши откройте контекстное меню локальной задачи и выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, для которой вы хотите запустить, остановить, приостановить или 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 или возобновить.
5. По правой клавише мыши откройте контекстное меню групповой задачи и выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Задачи**.
3. В рабочей области в списке задач выберите нужную задачу для наборов компьютеров, выполнение которой вы хотите запустить, остановить, приостановить или возобновить.
4. По правой клавише мыши откройте контекстное меню задачи и выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

Изменение параметров задачи

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите настроить параметры 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. В списке локальных задач выберите нужную локальную задачу.
8. По правой клавише мыши откройте контекстное меню задачи и выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название локальной задачи>**.
9. В окне **Свойства: <Название локальной задачи>** измените параметры локальной задачи.
10. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием нужной группы администрирования.
3. В рабочей области выберите закладку **Задачи**.
4. В списке задач выберите нужную групповую задачу.
5. По правой клавише мыши откройте контекстное меню задачи и выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название групповой задачи>**.
6. В окне **Свойства: <Название групповой задачи>** измените параметры задачи.
7. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Задачи**.
3. В рабочей области в списке задач выберите нужную задачу.
4. По правой клавише мыши откройте контекстное меню задачи и выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название задачи для наборов устройств>**.
5. В окне **Свойства: <Название задачи для наборов устройств >** измените параметры задачи.
6. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Все разделы окна свойств задач, кроме раздела **Параметры**, стандартны для программы Kaspersky Security Center. Их подробное описание вы можете прочитать в документации Kaspersky Security Center. Раздел **Параметры** содержит специфические параметры программы Kaspersky Endpoint Security, его содержимое варьируется в зависимости от выбранного типа и вида задачи.

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/klnagent64/bin.

В зависимости от используемых ключей Агент администрирования 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>` – записать значения параметров подключения Агента администрирования к Серверу и результаты выполнения утилиты в файл журнала. Если этот ключ не указан, параметры, результаты и сообщения об ошибках выводятся на экран.
- `-sp` – вывести пароль для аутентификации пользователя на прокси-сервере. Этот ключ 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.

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/klnagent64/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>` – записать результаты выполнения утилиты в указанный файл. Если этот ключ не используется, результаты и сообщения об ошибках выводятся на stdout.
- `-address <адрес сервера>` – адрес Сервера администрирования для подключения. В качестве адреса может быть указан 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 незащищенное подключение к Серверу администрирования. Если этот ключ не указан, подключение Агента к Серверу администрирования осуществляется по защищенному SSL-протоколу.
- `-cert <путь к файлу сертификата>` – использовать указанный файл сертификата для аутентификации доступа к новому Серверу администрирования. Если этот ключ не используется, Агент администрирования получит сертификат при первом подключении к Серверу администрирования.
- `-silent` – запустить утилиту на выполнение в неинтерактивном режиме. Использование ключа может быть полезно, например, при запуске утилиты из сценария запуска при регистрации пользователя.
- `-dupfix` – этот ключ используется в случае, если установка Агента администрирования была выполнена не традиционным способом, с использованием дистрибутива, а, например, путем восстановления из образа диска.

Устранение уязвимостей и установка критических обновлений в программе

Для сохранения бинарной целостности сертифицированной программы запрещается устанавливать обновления программных модулей, не прошедшие процедуру сертификации. Прошедшие процедуру сертификации обновления программных модулей требуется получать путем обращения в техническую поддержку АО "Лаборатория Касперского" по телефонам: +7 (495) 663-81-47, 8-800-700-88-11 или из регулярно обновляемых статей об актуальных версиях сертифицированных программ на сайте разработчика-изготовителя (http://support.kaspersky.ru/general/certificates). Информацию об обновлениях следует проверять не реже, чем один раз в месяц.

Программы должны периодически (один раз в полгода) подвергаться анализу уязвимостей: компания, осуществляющая эксплуатацию программы, должна проводить такой анализ при помощи открытых источников, содержащих базу уязвимостей, в том числе с сайта разработчика-изготовителя (http://www.bdu.fstec.ru; https://support.kaspersky.ru/vulnerability).

Перед использованием программы на компьютере требуется установить все доступные обновления операционной системы.

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки.

Обращение в Службу технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (http://support.kaspersky.ru/b2b);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

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" (http://support.kaspersky.ru/b2b).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 1. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

kaspersky

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

В этом разделе

Конфигурационные файлы задач по умолчанию

Этот раздел содержит информацию о конфигурационных файлах по умолчанию для задач Kaspersky Endpoint Security.

Конфигурационные файлы можно изменить в любой момент. Вы также можете изменить значения параметров из командной строки.

Правила редактирования конфигурационных файлов Kaspersky Endpoint Security

При редактировании конфигурационного файла соблюдайте следующие правила:

- В конфигурационном файле необходимо указать все обязательные параметры. Отдельные параметры задачи можно указать без файла, с помощью командной строки.
- Если параметр принадлежит к какой-либо секции, помещайте его только в этой секции. В пределах одной секции вы можете помещать параметры в любом порядке.
- Заключайте имена секций в квадратные скобки [ ].
- Вводите значения параметров в формате имя параметра=значение (пробелы между именем параметра и его значением не обрабатываются).

Пример:

```
[ScanScope.item_0000]
AreaDesc=Home
AreaMask.item_0000=*doc
Path=/home
```

  Символы "пробел" и "табуляция" игнорируются перед первой кавычкой и после последней кавычки строкового значения, а также в начале и в конце строкового значения, не заключенного в кавычки.

- Если вам нужно указать несколько значений параметра, повторите параметр столько раз, сколько значений вы хотите указать.

Пример:

```
AreaMask.item_0000=*xml
AreaMask.item_0001=*doc
```

- Соблюдайте регистр при вводе значений параметров следующих типов:
  - имена (маски) проверяемых объектов и объектов исключения;
  - названия (маски) угроз;

  При вводе остальных значений параметров соблюдать регистр не требуется.
- Указывайте значения параметров булевского типа следующим образом: `Yes – No`.
- Заключайте в кавычки строковые значения, содержащие символ "пробел" (например, имена файлов и директорий, пути к ним; выражения, содержащие дату и время в формате "ГГГГ-ММ-ДД ЧЧ:ММ:СС").

  Остальные значения вы можете вводить как в кавычках, так и без них.

Пример:

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

Одиночная кавычка в начале или в конце строки считается ошибкой.

Конфигурационный файл задачи Защита от файловых угроз

```
ScanArchived=No
ScanSfxArchived=No
ScanMailBases=No
ScanPlainMail=No
TimeLimit=60
SizeLimit=0
FirstAction=Recommended
SecondAction=Block
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
ScanByAccessType=SmartCheck
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи антивирусной проверки

```
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи выборочной проверки

```
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи проверка загрузочных секторов

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

Конфигурационный файл задачи проверка памяти процессов

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

Конфигурационный файл задачи обновления

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

Конфигурационный файл задачи копирования обновлений

```
SourceType=KLServers
UseKLServersWhenUnavailable=Yes
ConnectionTimeout=10
AutoPatchDownload=No
```

Конфигурационный файл задачи управления Хранилищем

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

Конфигурационный файл задачи Мониторинг файловых операций

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

```
AreaMask.item_0000=*
```

Конфигурационный файл задачи Защита от шифрования

```
UseHostBlocker=yes
BlockTime=30
UseExcludeMasks=no
[ScanScope.item_0000]
AreaDesc=AllSharedFolders
UseScanArea=yes
Path=AllShared
AreaMask.item_0000=*
```

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 параметрах программы;

64 – Kaspersky Endpoint Security не запущен;

66 – антивирусные базы не загружены (используется только командой `--app-info`);

67 – активация 2.0 завершилась с ошибкой из-за сетевых проблем;

68 – выполнение команды невозможно, так как программа работает под политикой;

70 – попытка запуска уже запущенной задачи, удаления запущенной задачи, изменения параметров запущенной задачи, остановки уже остановленной задачи, приостановки уже приостановленной задачи, возобновления выполнения уже выполняющейся задачи.

71 – не приняты условия Положения о Kaspersky Security Network.

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 Защита от файловых угроз, задача антивирусной проверки	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. • Recommended – программа автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе.
SecondAction	Задача Защита от файловых угроз, задача антивирусной проверки	Если значение FirstAction=Cure: • Remove – программа удаляет зараженный объект, предварительно создав его резервную копию.
Action	Задача проверки памяти процессов, задача проверки загрузочных секторов	Cure – программа пытается вылечить объект, сохранив копию объекта в Хранилище.
UseAnalyzer	Задача Защита от файловых угроз, задача антивирусной проверки, задача проверки загрузочных секторов	Yes – эвристический анализатор включен.
HeuristicLevel	Задача Защита от файловых угроз, задача антивирусной проверки, 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 Защита от файловых угроз, задача антивирусной проверки	Yes – проверять архивы.

Название параметра	Сущность, к которой относится параметр	Значение параметра в сертифицированном состоянии программы
ScanSfxArchived	Задача Защита от файловых угроз, задача антивирусной проверки	Yes – проверять самораспаковывающиеся архивы.
ScanMailBases	Задача Защита от файловых угроз, задача антивирусной проверки	Yes – проверять файлы почтовых баз.
ScanByAccessType	Задача Защита от файловых угроз	Open – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.
SourceType	Задача обновления	Одно из следующих значений: • KLServers – программа получает обновления с одного из серверов обновлений "Лаборатории Касперского". • SCServer – программа загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. • Custom – программа загружает обновления из пользовательского источника (локальной или сетевой директории (SMB / NFS), смонтированной пользователем, или FTP- , HTTP- или HTTPS-сервера).
UseKSN	Общие параметры программы	No – не принимать Положение о Kaspersky Security Network. SaveStatisticsToFile – режим сбора детектирующих статистик в файлы.

kaspersky

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности 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. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную 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, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения 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 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 Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, 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, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.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.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Outlook, Visual C++ – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CentOS – товарный знак Red Hat Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.