kaspersky

Kaspersky Endpoint Security 11.3 для Linux

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 11.3.0.7441

kaspersky

Уважаемый пользователь!

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

Дата редакции документа: 15.11.2022

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

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

kaspersky

Содержание

kaspersky

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Endpoint Security 11.3 для Linux" (далее также "Kaspersky Endpoint Security", "программа").

Подготовительные процедуры изложены в разделах "Подготовка к установке программы", "Установка программы" 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, эксплуатация и администрирование Kaspersky Endpoint Security, а также поддержка организаций, использующих Kaspersky Endpoint Security. Документ адресован техническим специалистам, которые имеют опыт работы с системой удаленного централизованного управления программами "Лаборатории Касперского" Kaspersky Security Center.

kaspersky

Источники информации о программе

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

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

На странице программы (https://www.kaspersky.ru/small-to-medium-business-security/endpoint-linux) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

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

Страница Kaspersky Endpoint Security в Базе знаний

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

На странице программы в Базе знаний (https://support.kaspersky.ru/kes11linux) 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 программе Kaspersky Endpoint Security, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" на Форуме

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

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

kaspersky

О программе

Программное изделие "Kaspersky Endpoint Security для Linux" (далее также “Kaspersky Endpoint Security”, “программа”) представляет собой средство антивирусной защиты типов “Б”, “В”, “Г” и предназначено для применения на серверах и автоматизированных рабочих местах информационных систем, а также на автономных автоматизированных рабочих местах на аппаратной платформе под управлением операционной системы семейства UNIX™.

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.

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

Kaspersky Endpoint Security имеет следующие аппаратные и программные требования:

Минимальные аппаратные требования:

- процессор Core™ 2 Duo 1.86 ГГц;
- раздел подкачки не менее 1 ГБ;
- 1 ГБ оперативной памяти для 32-битных операционных систем, 2 ГБ оперативной памяти для 64-битных операционных систем;
- 4 ГБ свободного места на жестком диске для установки программы и хранения временных файлов и файлов журналов.

Программные требования:

- Поддерживаемые 32-битные операционные системы:
  - CentOS 6.7, CentOS 6.8, CentOS 6.9, CentOS 6.10.
  - Debian GNU/Linux® 10.1, Debian GNU/Linux 10.2, Debian GNU/Linux 10.3, Debian GNU/Linux 10.4, Debian GNU/Linux 10.5, Debian GNU/Linux 10.6, Debian GNU/Linux 10.7, Debian GNU/Linux 10.8, Debian GNU/Linux 10.9, Debian GNU/Linux 10.10, Debian GNU/Linux 10.11, Debian GNU/Linux 10.12.
  - Debian GNU/Linux 11.0, Debian GNU/Linux 11.1, Debian GNU/Linux 11.2, Debian GNU/Linux 11.3.
  - Mageia™ 4.
  - Red Hat® Enterprise Linux® 6.7, Red Hat Enterprise Linux 6.8, Red Hat Enterprise Linux 6.9, Red Hat Enterprise Linux 6.10.
  - Альт 8 СП Рабочая Станция.
  - Альт 8 СП Сервер.
  - Альт Образование 10.
  - Альт Рабочая Станция 10.
- Поддерживаемые 64-битные операционные системы:
  - AlmaLinux OS 8.5, AlmaLinux OS 8.6.
  - AlmaLinux OS 9.0.
  - AlterOS® 7.5.

- Amazon™ Linux 2.
- Astra Linux Common Edition 2.12.
- Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6).
- Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7).
- CentOS 6.7, CentOS 6.8, CentOS 6.9, CentOS 6.10.
- CentOS 7.2, CentOS 7.3, CentOS 7.4, CentOS 7.5, CentOS 7.6, CentOS 7.7, CentOS 7.8, CentOS 7.9.
- CentOS Stream 9.
- Debian GNU/Linux 10.1, Debian GNU/Linux 10.2, Debian GNU/Linux 10.3, Debian GNU/Linux 10.4, Debian GNU/Linux 10.5, Debian GNU/Linux 10.6, Debian GNU/Linux 10.7, Debian GNU/Linux 10.8, Debian GNU/Linux 10.9, Debian GNU/Linux 10.10, Debian GNU/Linux 10.11, Debian GNU/Linux 10.12.
- Debian GNU/Linux 11.0, Debian GNU/Linux 11.1, Debian GNU/Linux 11.2, Debian GNU/Linux 11.3.
- EMIAS 1.0.
- EulerOS 2.0 SP5.
- LinuxMint 19.3.
- LinuxMint 20.3.
- openSUSE Leap 15.0, openSUSE Leap 15.1, openSUSE Leap 15.2, openSUSE Leap 15.3, openSUSE Leap 15.4.
- Oracle® Linux 7.3, Oracle Linux 7.4, Oracle Linux 7.5, Oracle Linux 7.6, Oracle Linux 7.7, Oracle Linux 7.8, Oracle Linux 7.9.
- Oracle Linux 8.0, Oracle Linux 8.1, Oracle Linux 8.2, Oracle Linux 8.3, Oracle Linux 8.4, Oracle Linux 8.5, Oracle Linux 8.6.
- Red Hat Enterprise Linux 6.7, Red Hat Enterprise Linux 6.8, Red Hat Enterprise Linux 6.9, Red Hat Enterprise Linux 6.10.
- Red Hat Enterprise Linux 7.2, Red Hat Enterprise Linux 7.3, Red Hat Enterprise Linux 7.4, Red Hat Enterprise Linux 7.5, Red Hat Enterprise Linux 7.6, Red Hat Enterprise Linux 7.7, Red Hat Enterprise Linux 7.8, Red Hat Enterprise Linux 7.9.
- Red Hat Enterprise Linux 8.0, Red Hat Enterprise Linux 8.1, Red Hat Enterprise Linux 8.2, Red Hat Enterprise Linux 8.3, Red Hat Enterprise Linux 8.4, Red Hat Enterprise Linux 8.5, Red Hat Enterprise Linux 8.6.
- Red Hat Enterprise Linux 9.
- Rocky Linux 8.5, Rocky Linux 8.6.
- SUSE Linux Enterprise Server 12.5.
- SUSE Linux Enterprise Server 15.3.
- Ubuntu® 20.04 LTS.
- Ubuntu 22.04 LTS.
- Альт 8 СП Рабочая Станция.
- Альт 8 СП Сервер.
- Альт Образование 10.

  - Альт Рабочая Станция 10.
  - Альт Сервер 10.
  - Атлант, сборка Alcyone, версия 2022.02.
  - Гослинукс 7.17.
  - Гослинукс 7.2.
  - РЕД ОС® 7.3.
  - РОСА "Кобальт" 7.9.
  - РОСА "Хром" 12.
- Минимальная версия интерпретатора языка Perl – 5.10.
- Установленные пакеты для компиляции программ и запуска задач (gcc, binutils, glibc, glibc-devel, make, ld) на операционных системах, не поддерживающих технологию fanotify.
- Заголовочные файлы ядра операционной системы для компиляции модулей Kaspersky Endpoint Security на операционных системах, не поддерживающих технологию fanotify.

Перед установкой программы Kaspersky Endpoint Security и Агента администрирования Kaspersky Security Center в операционной системе SUSE Linux Enterprise Server 15 требуется установить пакет insserv-compat.

Перед установкой Агента администрирования Kaspersky Security Center в операционных системах Red Hat Enterprise Linux 9 и Ubuntu 22.04 LTS требуется установить системный пакет initscripts.

Для работы программы в операционной системе Red Hat Enterprise Linux 8 требуется установить пакет perl-Getopt-Long.

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

Для работы плагина управления Kaspersky Endpoint Security должен быть установлен Microsoft® Visual C++® 2015 Redistributable Update 3 RC (https://www.microsoft.com/ru-ru/download/details.aspx?id=52685).

Поддерживаемые версии Kaspersky Security Center

Программа Kaspersky Endpoint Security совместима с программой Kaspersky Security Center следующих версий:

- Kaspersky Security Center 12. Поддерживается управление программой Kaspersky Endpoint Security через Консоль администрирования с помощью mmc-плагина управления (см. раздел "Об mmc-плагине управления Kaspersky Endpoint Security" на стр. 36).
- Kaspersky Security Center 13.2. Поддерживается управление программой Kaspersky Endpoint Security через Консоль администрирования с помощью mmc-плагина управления.
- Kaspersky Security Center 14. Поддерживается управление программой Kaspersky Endpoint Security через Консоль администрирования с помощью mmc-плагина управления и через Kaspersky Security Center Web Console с помощью веб-плагина управления (см. раздел "О веб-плагине управления Kaspersky Endpoint Security" на стр. 36).
- Kaspersky Security Center 14 Linux. Поддерживается управление программой Kaspersky Endpoint Security через Kaspersky Security Center Web Console с помощью веб-плагина управления.

  Kaspersky Security Center на базе Linux имеет в составе версию Сервера администрирования, предназначенную для установки на устройство с операционной системой Linux. Взаимодействие с

Сервером администрирования Kaspersky Security Center Linux осуществляется с помощью Kaspersky Security Center Web Console.

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

Подробнее о Kaspersky Security Center Linux см. в документации Kaspersky Security Center Linux.

Для управления программой Kaspersky Endpoint Security через Kaspersky Security Center используется Агент администрирования Kaspersky Security Center, который входит в комплект поставки программы Kaspersky Endpoint Security.

Указания по эксплуатации и требования к среде

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 (см. стр. 17)".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
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

Подготовка к установке программы

Перед установкой программы убедитесь, что программные и аппаратные ресурсы компьютера, на который будет произведена установка, удовлетворяют требованиям, приведенным в разделе "Аппаратные и программные требования (см. стр. 17)".

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

Установка программы

Сценарий описывает установку и первоначальную настройку программы Kaspersky Endpoint Security, а также установку и настройку Агента администрирования Kaspersky Security Center и установку плагинов управления Kaspersky Endpoint Security.

Установка и первоначальная настройка Kaspersky Endpoint Security и Kaspersky Security Center состоит из следующих этапов:

a. **Удаление сторонних антивирусных программ**

   Перед установкой программы Kaspersky Endpoint Security убедитесь, что на вашем компьютере не установлены другие сторонние антивирусные программы. При необходимости удалите эти программы.

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

   Если вы планируете управлять программой Kaspersky Endpoint Security с помощью Kaspersky Security Center, установите Агент администрирования Kaspersky Security Center и настройте его параметры (см. раздел "Установка и настройка Агента администрирования Kaspersky Security Center" на стр. 33).

c. **Установка плагинов управления Kaspersky Endpoint Security**

   Если вы планируете управлять программой Kaspersky Endpoint Security с помощью Kaspersky Security Center, установите следующие плагины управления Kaspersky Endpoint Security (см. раздел "Установка плагинов управления Kaspersky Endpoint Security" на стр. 35) в зависимости от консоли управления, которую вы хотите использовать для взаимодействия с Kaspersky Security Center:

   - mmc-плагин управления Kaspersky Endpoint Security позволяет управлять работой программы через Консоль администрирования Kaspersky Security Center;
   - веб-плагин управления Kaspersky Endpoint Security позволяет управлять работой программы через Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console.

d. **Установка пакетов программы и графического пользовательского интерфейса**

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

   Вы можете установить Kaspersky Endpoint Security с помощью командной строки (см. раздел "Установка Kaspersky Endpoint Security с помощью командной строки" на стр. 25) или через Kaspersky Security Center (см. раздел "Развертывание программы с помощью Kaspersky Security Center" на стр. 38), используя Консоль администрирования или Kaspersky Security Center Web Console.

e. **Первоначальная настройка Kaspersky Endpoint Security**

   Выполнение первоначальной настройки требуется для включения защиты компьютера.

   Если вы установили программу Kaspersky Endpoint Security с помощью командной строки, запустите скрипт первоначальной настройки (см. раздел "Первоначальная настройка Kaspersky Endpoint Security" на стр. 26) или выполните первоначальную настройку в автоматическом режиме (см. раздел "Автоматический режим первоначальной настройки программы" на стр. 31).

   Если вы установили программу Kaspersky Endpoint Security с помощью Kaspersky Security Center, выполните подготовку программы к работе (см. раздел "Подготовка программы к работе через Kaspersky Security Center" на стр. 50) и активируйте программу (см. раздел "Активация программы через Kaspersky Security Center" на стр. 50).

Для запуска программы требуется, чтобы учетная запись root была владельцем следующих директорий и только владелец имел право на запись в них: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

В этом разделе

Развертывание программы с помощью командной строки

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

Вы можете выполнить следующие действия при установке программы:

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

  Невозможно установить пакет графического пользовательского интерфейса на компьютер, где не установлен пакет программы.

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

После завершения установки Kaspersky Endpoint Security с помощью командной строки требуется выполнить первоначальную настройку программы путем запуска скрипта первоначальной настройки (см. раздел "Первоначальная настройка Kaspersky Endpoint Security" на стр. 26) или в автоматическом режиме (см. раздел "Автоматический режим первоначальной настройки программы" на стр. 31).

В этом разделе

kaspersky

Установка Kaspersky Endpoint Security с помощью командной строки

Установка пакета программы без графического пользовательского интерфейса

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

```
# rpm -i kesl-11.3.0-<номер сборки>.i386.rpm
```

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

```
# rpm -i kesl-11.3.0-<номер сборки>.x86_64.rpm
```

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

```
# apt-get install ./kesl_11.3.0-<номер сборки>_i386.deb
```

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

```
# apt-get install ./kesl_11.3.0-<номер сборки>_amd64.deb
```

Установка пакета графического интерфейса

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

```
# rpm -i kesl-gui-11.3.0-<номер сборки>.i386.rpm
```

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

```
# rpm -i kesl-gui-11.3.0-<номер сборки>.x86_64.rpm
```

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

```
# apt-get install ./kesl-gui_11.3.0-<номер сборки>_i386.deb
```

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

```
# apt-get install ./kesl-gui_11.3.0-<номер сборки>_amd64.deb
```

kaspersky

Первоначальная настройка Kaspersky Endpoint Security

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

Если вы не выполнили процедуру первоначальной настройки Kaspersky Endpoint Security после установки с помощью командной строки, антивирусная защита компьютера не будет работать.

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

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

Скрипт первоначальной настройки необходимо запустить с root-правами после завершения установки пакета Kaspersky Endpoint Security. Скрипт пошагово запрашивает значения параметров Kaspersky Endpoint Security. Завершение работы скрипта и освобождение консоли означает, что процесс настройки завершен.

► *Чтобы проверить код возврата, выполните следующую команду:*

```
echo $?
```

Если команда вернула код 0 (см. раздел "Приложение 3. Коды возврата командной строки" на стр. 403), первоначальная настройка программы успешно завершена.

В этом разделе

Выбор языкового стандарта

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

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

Локализация графического интерфейса и командной строки программы зависит от локализации, указанной в переменной окружения LANG. Если в переменной окружения LANG указана локализация, которую не поддерживает программа Kaspersky Endpoint Security, то графический интерфейс и командная строка отображаются в английской локализации.

Просмотр Лицензионного соглашения и Политики конфиденциальности

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

Принятие Лицензионного соглашения

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

После выхода из режима просмотра введите одно из следующих значений:

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

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

Принятие Политики конфиденциальности

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

После выхода из режима просмотра введите одно из следующих значений:

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

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

Участие в Kaspersky Security Network

В сертифицированной версии программы Kaspersky Endpoint Security используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается, так как приводит к выходу программы из сертифицированного состояния.

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

Введите одно из следующих значений:

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

Отказ от участия в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 202) не прерывает процесс установки программы Kaspersky Endpoint Security. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент.

Назначение пользователю роли администратора

На этом шаге вы можете назначить пользователю роль администратора (admin) (см. раздел "Разделение доступа к функциям программы по пользовательским ролям" на стр. 66).

Введите имя пользователя, которому вы хотите назначить роль администратора.

Вы можете назначить пользователю роль администратора позже в любой момент (см. раздел "Назначение роли пользователю" на стр. 68).

Определение типа перехватчика файловых операций

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

Если в процессе компиляции модуля ядра не обнаружены необходимые пакеты, Kaspersky Endpoint Security предлагает установить их. Если скачать пакеты не удалось, выводится сообщение об ошибке.

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

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

Включение автоматической настройки SELinux

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

На этом шаге вы можете включить автоматическую настройку системы SELinux для работы с Kaspersky Endpoint Security.

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

Введите `no`, если вы не хотите, чтобы программа автоматически настроила систему SELinux.

По умолчанию программа предлагает значение `yes`.

При необходимости вы можете вручную настроить систему SELinux (см. раздел "Настройка разрешающих правил в системе SELinux" на стр. 54) для работы с программой позже, после завершения первоначальной настройки программы Kaspersky Endpoint Security.

Настройка источника обновлений

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

Введите 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 вашей организации Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновлений, если вы используете программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации.
- `<веб-адрес>` – программа загружает обновления из пользовательского источника. Вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.
- `<путь>` – путь к директории, в которой расположены автономные базы программы.

Настройка параметров прокси-сервера

На этом шаге вам нужно указать параметры прокси-сервера, если вы используете прокси-сервер для доступа в интернет. Для загрузки баз программы (см. раздел "Загрузка баз программы" на стр. 30) с серверов обновлений требуется подключение к интернету.

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

- Если при подключении к интернету вы используете прокси-сервер, укажите адрес прокси-сервера в одном из следующих форматов:
  - `proxy_server_IP:port_number`, если для подключения к прокси-серверу не требуется аутентификация;
  - `user_name:password@proxy_server_IP_address:port_number`, если для подключения к прокси-серверу требуется аутентификация.

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

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

По умолчанию программа предлагает значение `no`.

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

Загрузка баз программы

На этом шаге вы можете загрузить на компьютер базы программы. Базы содержат описания сигнатур угроз и методов борьбы с ними. Программа использует эти записи при поиске и нейтрализации угроз. Вирусные аналитики "Лаборатории Касперского" регулярно добавляют записи о новых угрозах.

Если вы хотите загрузить базы программы на компьютер, введите `yes`.

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

По умолчанию программа предлагает значение `yes`.

Kaspersky Endpoint Security обеспечивает антивирусную защиту компьютера только после загрузки баз программы.

Вы можете запустить задачу обновления (см. раздел "Запуск и остановка задачи" на стр. 98) без использования скрипта первоначальной настройки.

Включение автоматического обновления баз программы

На этом шаге вы можете включить автоматическое обновление баз программы.

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

Введите `no`, если вы не хотите, чтобы программа автоматически обновляла базы.

Вы можете включить автоматическое обновление баз без использования скрипта первоначальной настройки, настроив расписание задачи обновления.

Активация программы

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

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

Если вы не указали файл ключа, программа будет активирована с помощью пробного ключа на один месяц.

Вы можете активировать программу (см. раздел "Задача Лицензирование (License, ID:9)" на стр. 151) без использования скрипта первоначальной настройки.

Автоматический режим первоначальной настройки программы

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

При необходимости вы можете изменить значения параметров в конфигурационном файле первоначальной настройки.

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

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

Завершение работы скрипта первоначальной настройки и освобождение консоли означает, что процесс первоначальной настройки программы завершен.

► *Чтобы проверить код возврата, выполните следующую команду:*

```
echo $?
```

Если команда вернула код 0 (см. раздел "Приложение 3. Коды возврата командной строки" на стр. 403), первоначальная настройка программы успешно завершена.

Параметры конфигурационного файла первоначальной настройки

Конфигурационный файл первоначальной настройки программы содержит параметры, приведенные в таблице ниже.

Таблица 1. Параметры конфигурационного файла первоначальной настройки

Параметр	Описание	Значения
EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения.	`yes` – принять условия Лицензионного соглашения, чтобы продолжить процедуру установки 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.

Параметр	Описание	Значения
USE_KSN	Согласие с Положением о Kaspersky Security Network.	`yes` – принять Положение о Kaspersky Security Network. `no` – не принимать Положение о Kaspersky Security Network. В сертифицированной версии программы используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается, так как приводит к выходу программы из сертифицированного состояния.
LOCALE	Дополнительный параметр. Языковой стандарт, используемый для локализации событий программы, отправляемых в Kaspersky Security Center.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр `LOCALE` не указан, устанавливается язык локализации операционной системы. Если программе не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию `en_US.utf8`. Локализация графического интерфейса и командной строки программы зависит от локализации, указанной в переменной окружения LANG. Если в переменной окружения LANG указана локализация, которую не поддерживает программа Kaspersky Endpoint Security, то графический интерфейс и командная строка отображаются в английской локализации.
INSTALL_LICENSE	Файл ключа.	
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.

Параметр	Описание	Значения
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.
ADMIN_USER	Пользователь, которому вы можете назначить роль администратора (см. раздел "Разделение доступа к функциям программы по пользовательским ролям" на стр. 66) (admin).	
CONFIGURE_SELINUX	Автоматическая настройка SELinux для работы с Kaspersky Endpoint Security.	yes – настроить SELinux для работы с Kaspersky Endpoint Security. no – не настраивать SELinux для работы с Kaspersky Endpoint Security.

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

Установка и настройка Агента администрирования Kaspersky Security Center

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

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

Вы можете выполнить установку и первоначальную настройку (см. раздел "Первоначальная настройка Агента администрирования с помощью командной строки" на стр. 34) Агента администрирования с помощью командной строки. Установка и настройка Агента администрирования также может быть выполнена удаленно с помощью Kaspersky Security Center. См. подробнее в документации Kaspersky Security Center (https://support.kaspersky.com/KSC/14/ru-RU/5022.htm).

Файлы, необходимые для установки и первоначальной настройки Агента администрирования, входят в комплект поставки Kaspersky Endpoint Security.

kaspersky

В этом разделе

Установка Агента администрирования с помощью командной строки

Процесс установки Агента администрирования требуется запускать с root-правами.

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

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

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

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

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

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

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

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

После установки пакета выполните первоначальную настройку Агента администрирования. (см. раздел "Первоначальная настройка Агента администрирования с помощью командной строки" на стр. 34)

Первоначальная настройка Агента администрирования с помощью командной строки

► *Чтобы настроить параметры Агента администрирования:*

1. Выполните команду:
   - для 32-битных операционных систем:

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

   - для 64-битных операционных систем:

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

2. Примите условия Лицензионного соглашения.

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

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

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

   По умолчанию SSL-соединение включено.
7. При необходимости укажите режим использования шлюза соединений:
   - `1` – не настраивать шлюз соединений.
   - `2` – не использовать шлюз соединений.
   - `3` – подключаться к Серверу администрирования через шлюз соединений.
   - 4 – использовать Агент администрирования в качестве шлюза соединений.

   По умолчанию используется вариант `1`.

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

Установка плагинов управления Kaspersky Endpoint Security

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

- mmc-плагин управления Kaspersky Endpoint Security (см. раздел "Об mmc-плагине управления Kaspersky Endpoint Security" на стр. 36) позволяет управлять работой программы через Консоль администрирования Kaspersky Security Center;
- веб-плагин управления Kaspersky Endpoint Security (см. раздел "О веб-плагине управления Kaspersky Endpoint Security" на стр. 36) позволяет управлять работой программы через Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console.

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

kaspersky

В этом разделе

Об mmc-плагине управления Kaspersky Endpoint Security

Mmc-плагин управления Kaspersky Endpoint Security (далее также *mmc-плагин*) обеспечивает взаимодействие программы Kaspersky Endpoint Security с Kaspersky Security Center через Консоль администрирования. Mmc-плагин позволяет управлять программой Kaspersky Endpoint Security с помощью политик (см. раздел "Управление политиками в Консоли администрирования Kaspersky Security Center" на стр. 214) и задач (см. раздел "Управление задачами в Консоли администрирования Kaspersky Security Center" на стр. 259).

Mmc-плагин требуется установить на том компьютере, где установлена Консоль администрирования Kaspersky Security Center.

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

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

О веб-плагине управления Kaspersky Endpoint Security

Веб-плагин управления Kaspersky Endpoint Security (далее также *веб-плагин*) обеспечивает взаимодействие программы Kaspersky Endpoint Security с Kaspersky Security Center через Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console. Веб-плагин позволяет управлять программой Kaspersky Endpoint Security с помощью политик и задач (см. раздел "Управление задачами в Web Console" на стр. 339).

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

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

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

Установка веб-плагина

Вы можете установить веб-плагин следующими способами:

- Установить веб-плагин с помощью мастера первоначальной настройки Kaspersky Security Center Web Console.

  Kaspersky Security Center Web Console автоматически предлагает запустить мастер первоначальной настройки при первом подключении Web Console к Серверу администрирования. Также вы можете запустить мастер первоначальной настройки в интерфейсе Web Console (**Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер первоначальной настройки**). Мастер первоначальной настройки также может проверить актуальность установленных веб-плагинов и загрузит необходимые обновления для них. Дополнительная информация о мастере первоначальной настройки Kaspersky Security Center Web Console приведена в документации Kaspersky Security Center.

- Установить веб-плагин из списка доступных дистрибутивов в Kaspersky Security Center Web Console.

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

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

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

Обновление веб-плагина

При появлении новой версии веб-плагина Kaspersky Security Center Web Console отобразит уведомление *Доступны обновления для используемых плагинов*. Вы можете перейти к обновлению версии веб-плагина из уведомления Web Console. Также вы можете проверить наличие обновлений веб-плагина вручную в интерфейсе Web Console (**Параметры Консоли** → **Плагины**). Предыдущая версия веб-плагина будет автоматически удалена во время обновления.

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

Вы можете обновить веб-плагин следующими способами:

- Обновить веб-плагин в списке веб-плагинов в онлайн-режиме.

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

- Обновить веб-плагин из файла.

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

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

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

Развертывание программы с помощью Kaspersky Security Center

Вы можете установить программу Kaspersky Endpoint Security на компьютер удаленно с рабочего места администратора с помощью программы Kaspersky Security Center используя Консоль администрирования (см. раздел "Установка Kaspersky Endpoint Security с помощью Консоли администрирования Kaspersky Security Center" на стр. 39) или Kaspersky Security Center Web Console (см. раздел "Установка Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console" на стр. 43).

Программу Kaspersky Endpoint Security можно развернуть на компьютерах в сети организации несколькими способами:

- Установка программы с помощью мастера развертывания защиты.

  Этот способ установки удобен, если вам подходят параметры программы, заданные по умолчанию, и в вашей организации используется простая инфраструктура, которая не требует специальной настройки.

- Установка программы с помощью задачи удаленной установки.

  Универсальный способ установки, который позволяет настроить параметры программы и гибко управлять задачами удаленной установки.

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

Kaspersky Security Center также поддерживает другие способы установки программы Kaspersky Endpoint Security, например, развертывание в составе образа операционной системы. Вы можете выбрать наиболее подходящий для вашей организации способ развертывания, а также использовать несколько способов развертывания одновременно. Дополнительная информация о других способах развертывания приведена в документации Kaspersky Security Center.

Чтобы управлять работой программы Kaspersky Endpoint Security, установленной на компьютерах, с помощью Kaspersky Security Center, вам нужно поместить эти компьютеры в группы администрирования. Перед началом установки программы Kaspersky Endpoint Security вы можете создать в Kaspersky Security Center группы администрирования, в которые вы хотите поместить компьютеры с установленной программой Kaspersky Endpoint Security, и настроить правила автоматического перемещения компьютеров в группы администрирования. Если правила перемещения компьютеров в группы администрирования не настроены, Kaspersky Security Center помещает все компьютеры с установленным Агентом администрирования, подключенным к Серверу администрирования, в список **Нераспределенные устройства**. В этом случае вам нужно вручную переместить компьютеры в группы администрирования (см. подробнее в документации Kaspersky Security Center).

kaspersky

В этом разделе

Установка Kaspersky Endpoint Security с помощью Консоли администрирования Kaspersky Security Center

Вы можете установить программу Kaspersky Endpoint Security на компьютер удаленно с рабочего места администратора с помощью Консоли администрирования Kaspersky Security Center.

Установка выполняется с помощью мастера удаленной установки или с помощью задачи удаленной установки программы (см. подробнее в документации Kaspersky Security Center).

Для удаленной установки используется инсталляционный пакет Kaspersky Endpoint Security, который содержит набор параметров, необходимых для установки программы. Вы можете создать инсталляционный пакет (см. раздел "Создание инсталляционного пакета программы" на стр. 39) вручную.

В этом разделе

Создание инсталляционного пакета программы

► *Чтобы создать инсталляционный пакет программы Kaspersky Endpoint Security:*

1. Скачайте архив kesl.zip на странице загрузки программ https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint?utm_content=downloads в разделе **Kaspersky Endpoint Security** в подразделе **Files for Product remote installation**.
2. Распакуйте файлы из архива kesl.zip в папку, доступную для Сервера администрирования Kaspersky Security Center. В ту же папку поместите файлы дистрибутива, соответствующие типу операционной системы, на которую вы хотите установить программу, и типу менеджера пакетов на ней:
   - для установки Kaspersky Endpoint Security:
     - kesl-11.3.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm);
     - kesl_11.3.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg);
     - kesl-11.3.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm);
     - kesl_11.3.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg);
   - для установки графического интерфейса:
     - kesl-gui-11.3.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm);
     - kesl-gui_11.3.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg);

- kesl-gui-11.3.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm);
- kesl-gui_11.3.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg).

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

Обратите внимание, что если графический пользовательский интерфейс не будет использоваться, то на следующем шаге инструкции требуется установить значение параметра `USE_GUI=No` в конфигурационном файле autoinstall.ini. В противном случае установка завершается с ошибкой.

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

3. При необходимости настройте параметры установки программы с помощью конфигурационного файла autoinstall.ini.
4. Откройте Консоль администрирования Kaspersky Security Center.
5. В дереве консоли выберите **Дополнительно → Удаленная установка → Инсталляционные пакеты**.
6. Нажмите на кнопку **Создать инсталляционный пакет**.

   Запустится мастер создания инсталляционного пакета.
7. В открывшемся окне мастера нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
8. Введите имя нового инсталляционного пакета и перейдите к следующему шагу мастера.
9. Выберите дистрибутив программы Kaspersky Endpoint Security. Для этого откройте стандартное окно Windows с помощью кнопки **Обзор** и укажите путь к файлу kesl.kud.

   В окне мастера отобразится название программы.

   Перейдите к следующему шагу мастера.
10. Ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и с Политикой конфиденциальности, которая описывает обработку и передачу данных.

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

    Перейдите к следующему шагу мастера.
11. Мастер загружает файлы, необходимые для установки программы, на Сервер администрирования Kaspersky Security Center. Дождитесь окончания загрузки.
12. Завершите работу мастера.

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

kaspersky

Параметры конфигурационного файла autoinstall.ini

Конфигурационный файл autoinstall.ini содержит параметры, приведенные в таблице ниже.

Таблица 2. Параметры конфигурационного файла autoinstall.ini

Параметр	Описание	Значения
EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения.	`yes` – принять условия Лицензионного соглашения, чтобы продолжить процедуру установки программы. `no` – не принимать условия Лицензионного соглашения. Установка программы будет прервана.
PRIVACY_POLICY_AGREED	Обязательный параметр. Согласие с условиями Политики конфиденциальности.	`yes` – принять условия Политики конфиденциальности, чтобы продолжить процедуру установки программы. `no` – не принимать условия Политики конфиденциальности. Установка программы будет прервана.
USE_KSN	Согласие с условиями Положения о Kaspersky Security Network.	`yes` – принять условия Положения о Kaspersky Security Network. `no` – не принимать условия Положения о Kaspersky Security Network. В сертифицированной версии программы используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается, так как приводит к выходу программы из сертифицированного состояния.

Параметр	Описание	Значения
LOCALE	Дополнительный параметр. Языковой стандарт, используемый для локализации событий программы, отправляемых в Kaspersky Security Center.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр `LOCALE` не указан, устанавливается язык локализации операционной системы. Если программе не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию `en_US.utf8`. Локализация графического интерфейса и командной строки программы зависит от локализации, указанной в переменной окружения LANG. Если в переменной окружения LANG указана локализация, которую не поддерживает программа Kaspersky Endpoint Security, то графический интерфейс и командная строка отображаются в английской локализации.
INSTALL_LICENSE	Файл ключа.	
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.
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.
ADMIN_USER	Пользователь, которому назначается роль администратора (см. раздел "Разделение доступа к функциям программы по пользовательским ролям" на стр. 66) (admin).	Нет

Параметр	Описание	Значения
CONFIGURE_SELINUX	Автоматическая настройка SELinux для работы с Kaspersky Endpoint Security.	yes – выполнить автоматическую настройку SELinux для работы с Kaspersky Endpoint Security. no – не выполнять автоматическую настройку SELinux для работы с Kaspersky Endpoint Security.

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

Установка Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console

Kaspersky Security Center Web Console поддерживает следующие основные способы развертывания:

- Установка программы с помощью мастера развертывания защиты (см. раздел "Установка с помощью мастера развертывания защиты" на стр. 46).
- Установка программы с помощью задачи удаленной установки.

Установка состоит из следующих этапов:

1. Создание инсталляционного пакета. Мастер развертывания защиты создает пакет автоматически, если он не был создан раньше. Инсталляционный пакет расположен в списке инсталляционных пакетов, загруженных в Kaspersky Security Center Web Console: **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**. Вы также можете создать инсталляционный пакет и настроить его параметры вручную (см. раздел "Создание инсталляционного пакета" на стр. 44).
2. Создание задачи удаленной установки. Мастер развертывания защиты создает и запускает задачу удаленной установки автоматически. Вы также можете создать и запустить задачу вручную (см. раздел "Создание задачи удаленной установки" на стр. 48).

В этом разделе

Создание инсталляционного пакета

► *Чтобы создать инсталляционный пакет:*

1. В главном окне Web Console выберите **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Web Console.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

3. На первой странице мастера выберите вариант **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.

   Мастер создаст инсталляционный пакет из дистрибутива, размещенного на серверах "Лаборатории Касперского". Список обновляется автоматически по мере выпуска новых версий программ. Для установки Kaspersky Endpoint Security рекомендуется выбрать этот вариант.

   Также вы можете создать инсталляционный пакет из файла.

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

4. Выберите дистрибутив программы Kaspersky Endpoint Security. Справа откроется информация о дистрибутиве.

5. Ознакомьтесь с информацией и нажмите на кнопку **Загрузить и создать инсталляционный пакет**. Запустится процесс создания инсталляционного пакета.

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

Инсталляционный пакет будет создан и добавлен в Web Console. С помощью инсталляционного пакета вы можете установить программу на компьютеры сети организации или обновить версию программы.

В параметрах инсталляционного пакета вы можете настроить параметры установки программы (см. таблицу ниже).

Инсталляционный пакет содержит базы из хранилища Сервера администрирования. Вы можете обновить базы в инсталляционном пакете (см. раздел "Обновление баз в инсталляционном пакете" на стр. 45), чтобы снизить потребление трафика при обновлении баз после установки программы.

Таблица 3. Параметры инсталляционного пакета

Раздел	Описание
Параметры программы	**Укажите языковой стандарт**. Установите флажок, чтобы указать языковой стандарт, используемый при работе программы. Языковой стандарт в формате, определенном в RFC 3066. Если этот параметр не указан, используется языковой стандарт по умолчанию. **Активировать программу**. Установите флажок, чтобы указать код активации или лицензионный ключ для активации программы.

Раздел	Описание
Источник обновлений	Вы можете указать источник обновлений: • **Серверы обновлений "Лаборатории Касперского"**. • **Сервер администрирования Kaspersky Security Center**. • **Другие источники в локальной или глобальной сети**.
Параметры установки	**Запустить задачу обновления после установки**. Установите флажок, чтобы запустить задачу обновления после установки программы. **Задайте параметры прокси-сервера**. Установите флажок, чтобы указать адрес прокси-сервера, используемого для подключения к интернету. **Установить исходный код ядра**. Установите флажок, чтобы автоматически начать компиляцию модулей ядра. **Использовать GUI**. Установите флажок, чтобы включить использование графического пользовательского интерфейса.

Обновление баз в инсталляционном пакете

Инсталляционный пакет содержит базы из хранилища Сервера администрирования, актуальные при создании инсталляционного пакета. После создания инсталляционного пакета вы можете обновлять базы в инсталляционном пакете. Это позволяет уменьшить расход трафика на обновление баз после установки программы.

Чтобы обновить базы в хранилище Сервера администрирования, используйте задачу Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования*. Дополнительная информация об обновлении баз в хранилище Сервера администрирования приведена в документации Kaspersky Security Center.

Kaspersky Security Center Cloud Console не поддерживает обновление баз в инсталляционном пакете.

► *Чтобы обновить базы в инсталляционном пакете:*

1. В главном окне Web Console выберите **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Web Console.

2. Нажмите на название инсталляционного пакета программы Kaspersky Endpoint Security, в котором вы хотите обновить базы.

   Откроется окно свойств инсталляционного пакета.

3. На закладке **Общая информация** нажмите на ссылку **Обновить базы**.

Базы в инсталляционном пакете будут обновлены из хранилища Сервера администрирования. Файл bases.cab, который входит в комплект поставки, будет заменен директорией bases. Внутри директории будут находиться файлы пакетов обновлений.

Установка с помощью мастера развертывания защиты

На клиентском компьютере требуется открыть порты TCP 139 и 445, UDP 137 и 138.

► *Чтобы развернуть программу,*

в главном окне Web Console выберите **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер развертывания защиты**.

Запустится мастер развертывания защиты. Следуйте его указаниям.

Шаг 1. Выбор инсталляционного пакета

На этом шаге в списке инсталляционных пакетов выберите инсталляционный пакет Kaspersky Endpoint Security. Если пакет в списке отсутствует, нажмите на кнопку **Добавить** и выберите в списке дистрибутив программы Kaspersky Endpoint Security. Создание инсталляционного пакета выполняется автоматически.

Вы можете настроить параметры инсталляционного пакета (см. раздел "Создание инсталляционного пакета программы" на стр. 39) с помощью Web Console.

Шаг 2. Активация программы

На этом шаге вы можете добавить лицензионный ключ в инсталляционный пакет для активации программы. Этот шаг не является обязательным. Если на Сервере администрирования размещен лицензионный ключ с функцией автоматического распространения, ключ будет добавлен автоматически позднее. Также вы можете активировать программу позднее (см. раздел "Активация программы через Kaspersky Security Center" на стр. 50) с помощью задачи *Добавление ключа*.

Шаг 3. Выбор Агента администрирования

На этом шаге выберите версию Агента администрирования, который будет установлен вместе с программой Kaspersky Endpoint Security. *Агент администрирования* обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

Шаг 4. Выбор компьютеров для установки

На этом шаге выберите компьютеры, на которые будет установлена программа. Возможны следующие варианты:

- Указать группу администрирования. Задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Указать выборку устройств. Задача назначается устройствам, входящим в выборку устройств. Вы можете указать одну из существующих выборок.

Шаг 5. Настройка дополнительных параметров

На этом шаге настройте следующие дополнительные параметры программы:

- **Принудительно загрузить инсталляционный пакет**. Выбор средства установки программы:
  - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее программа Kaspersky Endpoint Security устанавливается средствами Агента администрирования.

- **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. *Точка распространения* – это устройство с установленным Агентом администрирования, используемое для распространения обновлений, удаленной установки программ и получения данных об устройства в сети. Подробнее о точках распространения см. в документации Kaspersky Security Center.
- **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

- **Не устанавливать программу, если она уже установлена**. Снимите этот флажок, если вы хотите, например, установить программу более ранней версии.
- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**. Установка программы Kaspersky Endpoint Security выполняется средствами Агента администрирования или средствами Active Directory® вручную. Для установки Агента администрирования задача удаленной установки должна быть запущена с правами администратора домена.

Шаг 6. Управление перезагрузкой компьютера

На этом шаге вы можете выбрать действие, которое будет выполняться, если потребуется перезагрузка компьютера. При установке программы перезагрузка не требуется. Перезагрузка требуется, только если перед установкой вам нужно удалить несовместимые программы. Также перезагрузка может потребоваться при обновлении версии программы.

Шаг 7. Удаление несовместимых программ

Этот шаг отображается, если на компьютере установлены программы, не совместимые с Kaspersky Endpoint Security.

На этом шаге ознакомьтесь со списком несовместимых программ и разрешите удаление этих программ. Если на компьютере установлены несовместимые программы, установка программы Kaspersky Endpoint Security завершается с ошибкой.

Шаг 8. Перемещение в группу администрирования

На этом шаге выберите группу администрирования, в которую требуется переместить компьютеры после установки Агента администрирования. Перемещение компьютеров в группу администрирования требуется для применения политик и групповых задач (см. раздел "Управление задачами в Web Console" на стр. 339). Если компьютер уже помещен в группу администрирования, он не будет перемещен. Если вы не выберете группу администрирования, компьютеры будут добавлены в группу **Нераспределенные устройства**.

Шаг 9. Выбор учетной записи для доступа к компьютерам

На этом шаге выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки программы Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 10. Запуск установки

Завершение работы мастера. Задача удаленной установки будет запущена автоматически. Вы можете следить за ходом выполнения задачи в свойствах задачи в разделе **Результаты**.

Создание задачи удаленной установки

► *Чтобы создать задачу удаленной установки:*

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

На этом шаге настройте основные параметры задачи:

1. В раскрывающемся списке **Программа** выберите **Kaspersky Security Center**.
2. В раскрывающемся списке **Тип задачи** выберите **Удаленная установка программы**.
3. В поле **Название задачи** введите краткое описание.
4. В блоке **Выбор устройств, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Выбор компьютеров для установки

На этом шаге выберите компьютеры, на которые будет установлена программа, в соответствии с выбранным вариантом области действия задачи.

Шаг 3. Настройка параметров инсталляционного пакета

На этом шаге настройте параметры инсталляционного пакета:

1. Выберите инсталляционный пакет Kaspersky Endpoint Security 11.3.0 для Linux.
2. Выберите инсталляционный пакет Агента администрирования.

   Выбранная версия Агента администрирования будет установлена вместе с программой Kaspersky Endpoint Security. *Агент администрирования* обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

3. В разделе **Принудительно загрузить инсталляционный пакет** выберите способ установки программы:

   - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security устанавливается средствами Агента администрирования.
   - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о точках распространения см. в документации Kaspersky Security Center (https://support.kaspersky.com/KSC/14/ru-RU/5022.htm).

- **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

4. В поле **Максимальное количество одновременных загрузок** установите ограничение на количество запросов к Серверу администрирования для загрузки инсталляционного пакета. Ограничение количества запросов позволит избежать перегрузки сети.
5. В поле **Максимальное количество попыток установок** установите ограничение на количество попыток установить программу. Если установка программы завершается с ошибкой, задача автоматически запускает установку повторно.
6. Если требуется, снимите флажок **Не устанавливать программу, если она уже установлена**. Это позволит, например, установить программу более ранней версии.
7. Если требуется, установите флажок **Назначить установку инсталляционного пакета в групповых политиках Active Directory**. Установка программы выполняется средствами Агента администрирования или средствами Active Directory вручную. Для установки Агента администрирования задача удаленной установки должна быть запущена с правами администратора домена.
8. Если требуется, установите флажок **Предлагать пользователю закрыть работающие программы**. Установка программы требует ресурсов компьютера. Для удобства пользователя мастер установки программы предлагает закрыть работающие программы перед началом установки. Это позволит избежать замедление в работе других программ и возможных сбоев в работе компьютера.
9. В разделе **Поведение устройств, управляемых другими Серверами администрирования** выберите способ установки программы Kaspersky Endpoint Security. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

Шаг 4. Управление перезагрузкой компьютера

На этом шаге вы можете выбрать действие, которое будет выполняться, если потребуется перезагрузка компьютера.

Шаг 5. Выбор учетной записи для доступа к компьютерам

На этом шаге выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки программы Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 6. Завершение создания задачи

Завершите работу мастера по кнопке **Создать**. В списке задач отобразится новая задача. Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**. Установка программы будет выполнена в тихом режиме.

kaspersky

Подготовка программы к работе через Kaspersky Security Center

После развертывания Kaspersky Endpoint Security для работы с программой через Kaspersky Security Center вам нужно выполнить следующие действия:

- Активировать программу. Вы можете создать и выполнить задачу активации через Консоль администрирования (см. раздел "Добавление ключа" на стр. 271) или через Kaspersky Security Center Web Console (см. раздел "Добавление ключа" на стр. 365), а также распространить на компьютеры лицензионный ключ из хранилища ключей Kaspersky Security Center (см. раздел "Активация программы через Kaspersky Security Center" на стр. 50).
- Обновить базы и модули программы через Консоль администрирования или через Kaspersky Security Center Web Console.
- Создать и настроить политику для централизованного управления работой программы на компьютерах. Для работы с политиками вы можете использовать Консоль администрирования (см. раздел "Управление политиками в Консоли администрирования Kaspersky Security Center" на стр. 214) или Web Console.

  Также вы можете настроить задачи управления программой с помощью Консоли администрирования (см. раздел "Управление задачами в Консоли администрирования Kaspersky Security Center" на стр. 259) или Web Console (см. раздел "Управление задачами в Web Console" на стр. 339).

Активация программы через Kaspersky Security Center

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

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

- С помощью задачи активации программы.

  Этот способ позволяет добавить лицензионный ключ на конкретный компьютер или компьютеры, входящие в группу администрирования. Вы можете создать и выполнить задачу активации через Консоль администрирования (см. раздел "Добавление ключа" на стр. 271) или через Kaspersky Security Center Web Console (см. раздел "Добавление ключа" на стр. 365).
- Путем распространения на компьютеры лицензионного ключа, размещенного на Сервере администрирования Kaspersky Security Center.

  Этот способ позволяет автоматически добавлять ключ на компьютеры, уже подключенные к Kaspersky Security Center, а также на новые компьютеры. Для использования этого способа требуется сначала добавить ключ в хранилище ключей на Сервере администрирования Kaspersky Security Center.

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

Активация в Kaspersky Security Center Web Console

Перед созданием задачи активации или распространением ключа необходимо добавить ключ в хранилище Сервера администрирования Kaspersky Security Center.

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

1. В главном окне Web Console выберите **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне выберите **Добавить файл ключа**, чтобы добавить ключ с помощью файла ключа.
4. Нажмите на кнопку **Выберите файл ключа** и в открывшемся окне выберите файл с расширением key.
5. Нажмите на кнопку **Закрыть**.

Добавленный ключ отобразится в списке ключей.

► *Чтобы активировать программу через Web Console с помощью задачи активации программы:*

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

   Откроется список задач.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. Настройте параметры задачи:
   a. В раскрывающемся списке **Программа** выберите название программы Kaspersky Endpoint Security.
   b. В раскрывающемся списке **Тип задачи** выберите **Добавление ключа**.
   c. В поле **Название задачи** введите короткое описание, например, `Активация Kaspersky Endpoint Security`.
   d. В разделе **Выбор устройств, которым будет назначена задача** выберите область действия задачи. Нажмите на кнопку **Далее**.
4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

   Откроется окно **Хранилище ключей Kaspersky Security Center**.
5. Если вы добавили ключ в хранилище ключей Kaspersky Security Center предварительно, выберите ключ в списке и нажмите на кнопку **Далее**.
6. Если нужный ключ в хранилище ключей отсутствует, нажмите на кнопку **Добавить ключ**.
   a. В открывшемся окне выберите **Добавить файл ключа**, чтобы добавить ключ с помощью файла ключа.
   b. Нажмите на кнопку **Выбрать файл ключа** и в открывшемся окне выберите файл с расширением key.
   c. Ознакомьтесь с информацией о ключе и нажмите на кнопку **Закрыть**.
   d. Добавленный ключ отобразится в хранилище ключей. Выберите его в списке и нажмите на кнопку **Далее**.
7. Ознакомьтесь с информацией о лицензии и нажмите на кнопку **Далее**.

8. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.

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

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

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

1. В главном окне Web Console выберите **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Откройте свойства ключа по ссылке с названием программы, для активации которой предназначен ключ.
3. Включите переключатель **Распространять лицензионный ключ автоматически**.
4. Нажмите на кнопку **Сохранить**.

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

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

- Просмотреть Отчет об использовании ключей в инфраструктуре организации (**Мониторинг и отчеты** → **Отчеты**).
- Просмотреть статусы компьютеров (**Устройства** → **Управляемые устройства**). Если программа не активирована, то у компьютера будет статус  и описание статуса **Программа не активирована**.
- Просмотреть информацию о лицензии в свойствах компьютера.
- Просмотреть свойства ключа (**Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**).

Особенности активации в Kaspersky Security Center Cloud Console

Для Kaspersky Security Center Cloud Console предусмотрена пробная версия. *Пробная версия* – это специальная версия Kaspersky Security Center Cloud Console, предназначенная для ознакомления пользователя с функциями Kaspersky Security Center Cloud Console. В этой версии вы можете выполнять действия в рабочем пространстве в течении 30 дней. Все управляемые программы, включая программу Kaspersky Endpoint Security, активируются по пробной лицензии Kaspersky Security Center Cloud Console автоматически. При этом активировать программу Kaspersky Endpoint Security по собственной пробной лицензии по истечении пробной лицензии Kaspersky Security Center Cloud Console невозможно. Дополнительная информация о Kaspersky Security Center Cloud Console приведена в документации Kaspersky Security Center Cloud Console.

Пробная версия Kaspersky Security Center Cloud Console не позволяет впоследствии перейти на коммерческую версию. Любое пробное рабочее пространство будет автоматически удалено со всем его содержимым по истечении тридцати дней.

Запуск программы в Astra Linux в режиме замкнутой программной среды

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

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

► *Чтобы запустить программу в операционной системе Astra Linux Special Edition (очередное обновление 1.7) или Astra Linux Special Edition (очередное обновление 1.6):*

1. Укажите следующие параметры в файле /etc/digsig/digsig_initramfs.conf:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Установите пакет совместимости:

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

3. Создайте директорию для ключа программы:

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

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

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

5. Обновите образ initramfs:

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

Для Astra Linux Special Edition (очередное обновление 1.5)

► *Чтобы запустить программу в операционной системе Astra Linux Special Edition (очередное обновление 1.5):*

1. Укажите следующие параметры в файле /etc/digsig/digsig_initramfs.conf:

   ```
   DIGSIG_LOAD_KEYS=1
   ```

   ```
   DIGSIG_ENFORCE=1
   ```

2. Создайте директорию для ключа программы:

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

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

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

4. Обновите образ initramfs:

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

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

Настройка разрешающих правил в системе SELinux

Если во время первоначальной настройки программе не удалось настроить систему SELinux автоматически (см. раздел "Включение автоматической настройки SELinux" на стр. 28) или вы отказались от автоматической настройки, вы можете настроить систему SELinux для работы с Kaspersky Endpoint Security вручную.

► *Чтобы настроить SELinux для работы с Kaspersky Endpoint Security:*

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

     ```
     # setenforce Permissive
     ```

   - Если SELinux был выключен, в конфигурационном файле /etc/selinux/config задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.
2. Убедитесь, что в системе установлена утилита semanage. Если утилита не установлена, установите пакет policycoreutils-python*.
3. Если вы используете пользовательскую политику SELinux, то есть отличную от заданной по умолчанию targeted policy, назначьте метку для следующих исходных исполняемых файлов программы Kaspersky Endpoint Security в соответствии с используемой политикой SELinux:
   - /var/opt/kaspersky/kesl/11.3.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/11.3.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/11.3.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/11.3.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/shared/kesl
4. Запустите следующие задачи:
   - задачу Защита от файловых угроз:

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

   - задачу Проверка важных областей:

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

   Рекомендуется запустить все задачи, которые вы планируете запускать при использовании программы Kaspersky Endpoint Security.
5. Запустите графический пользовательский интерфейс, если вы планируете его использовать.

6. Убедитесь, что в файле audit.log нет ошибок:

   ```
   grep kesl /var/log/audit/audit.log
   ```

7. Если в файле audit.log присутствуют ошибки, создайте и загрузите новый модуль правил на основе блокирующих записей, чтобы устранить ошибки, и снова запустите задачи, которые вы планируете запускать при использовании программы Kaspersky Endpoint Security.

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

8. Переведите SELinux в блокирующий режим:

   ```
   # setenforce Enforcing
   ```

Если вы используете пользовательскую политику SELinux, то после установки обновлений программы вам нужно вручную назначить метку для исходных исполняемых файлов Kaspersky Endpoint Security (выполните шаги 1, 3–8).

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

kaspersky

Процедура приемки

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

В этом разделе

Сертифицированное состояние программы

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

- Программа активирована: добавлен лицензионный ключ.
- Обновлены базы программы.
- Настроена и запущена задача Защита от файловых угроз.
- Параметры программы находятся в рамках допустимых значений, приведенных в "Приложении 4" к этому документу (см. раздел "Приложение 4. Значения параметров программы в сертифицированной конфигурации" на стр. 403).

Проверка работоспособности. Тестовый файл EICAR

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

Тестовый файл EICAR предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

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

Вы можете загрузить тестовый файл EICAR со страницы веб-сайта организации EICAR https://secure.eicar.org/eicar.com.

Перед сохранением файла в директории на диске компьютера убедитесь, что задача Защита от файловых угроз (File_Threat_Protection ID:1) остановлена.

► *Чтобы проверить работоспособность программы:*

1. Убедитесь, что параметры программы находятся в рамках допустимых значений, приведенных в Приложении 4 к этому документу (см. раздел "Приложение 4. Значения параметров программы в сертифицированной конфигурации" на стр. 403).
2. Убедитесь, что программа активирована и базы программы обновлены. Для этого выполните команду:

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

   Ожидаемый результат: программа выводит на экран следующую информацию:

   ```
   Информация о лицензии: Ключ действителен
   Базы программы загружены: Да
   Защита от файловых угроз: Задача доступна и выполняется
   ```

3. Убедитесь, что запущена задача Защита от файловых угроз. Для этого выполните команду:

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

   Ожидаемый результат: задача Защита от файловых угроз присутствует в списке задач, статус задачи `Started`.

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

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

   Скачайте EICAR-файл на сайте https://secure.eicar.org/eicar.com.

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

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

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

6. 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.

7. Убедитесь, что зараженный файл был удален из директории компьютера.
8. 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 Kaspersky Endpoint Security.

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 текст файла license.<ID языка>. Этот файл включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения (см. раздел "Принятие Лицензионного соглашения" на стр. 27), подтверждая свое согласие с текстом Лицензионного соглашения во время первоначальной настройки программы. Если вы не согласны с условиями Лицензионного соглашения, вы не должны использовать программу.

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, вам нужно продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

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

  Пробная лицензия имеет небольшой 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.

О лицензионном ключе

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

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

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

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

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

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

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

Лицензионный ключ может быть активным и резервным.

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

Резервный лицензионный ключ – лицензионный ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Резервный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Резервный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

kaspersky

О лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

kaspersky

О предоставлении и обработке данных

Данные, предоставляемые при использовании кода активации

Если программа была активирована с использованием кода активации, с целью проверки законности использования программы и получения статистической информации о распространении и использовании программы вы соглашаетесь предоставлять в автоматическом режиме следующую информацию:

- идентификатор регионального центра активации;
- список соглашений, показываемых пользователю программы;
- тип сжатия данных;
- семейство операционной системы;
- тип контрольной суммы обрабатываемого объекта;
- тип лицензии, по которой активирована программа;
- идентификатор программы, полученный из лицензии;
- полную версию программы;
- уникальный идентификатор устройства;
- идентификатор программы;
- дату и время истечения срока действия лицензии на использование программы;
- идентификатор лицензии программы;
- дату и время создания лицензионного ключа;
- текущий статус лицензионного ключа;
- заголовок лицензии на использование программы;
- идентификатор информационной модели, примененной при предоставлении лицензии на использование программы;
- набор идентификаторов программ, которые могут быть активированы на устройстве пользователя;
- тип используемой лицензии;
- локализацию программы;
- идентификатор установки программы (PCID);
- идентификатор ребрендинга программы;
- размер содержимого запроса к инфраструктуре Правообладателя;
- формат данных в запросе к инфраструктуре Правообладателя;
- тип юридического соглашения, условия которого были приняты пользователем в ходе использования программы;
- версию юридического соглашения, условия которого были приняты пользователем в ходе использования программы;
- идентификатор протокола;

- IP-адрес (IPv4) веб-службы, на который осуществлялось обращение.

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

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

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

Данные, предоставляемые при переходе по ссылкам из интерфейса программы

При переходе по ссылкам из интерфейса программы Kaspersky Endpoint Security вы соглашаетесь предоставлять в автоматическом режиме следующую информацию:

- полную версию программы;
- локализацию программы;
- группу программы;
- имя ссылки.

Данные, передаваемые программе Kaspersky Security Center

Во время работы программа Kaspersky Endpoint Security сохраняет и передает программе Kaspersky Security Center следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Информацию о базах, используемых в программе:
  - список категорий баз, необходимых программе;
  - дату и время выпуска и загрузки используемых баз в программу;
  - дату выпуска загруженных обновлений баз программы;
  - время последнего обновления баз программы.
- Информацию о лицензии на использование программы:
  - серийный номер и тип лицензии;
  - срок действия лицензии в днях;
  - количество устройств, на которые распространяется лицензия;
  - даты начала и окончания срока действия лицензии;
  - статус лицензионного ключа;

  - дату и время последней удачной синхронизации с серверами активации в случае, если программа активирована с помощью кода активации;
  - идентификатор программы, для которой предоставлена лицензия;
  - доступную по лицензии функциональность;
  - название организации, которой предоставлена лицензия;
  - дополнительную информацию в случае использования программы по подписке (признак подписки, дату истечения периода подписки и количество дней, доступных для продления подписки, веб-адрес провайдера подписки, текущий статус и причину перехода в этот статус), дату и время активации программы на устройстве;
  - дату и время окончания срока действия лицензии на устройстве.
- Информацию об обновлениях программы:
  - список обновлений, которые требуется установить или удалить;
  - дату выпуска обновления и наличие статуса Критическое;
  - название, версию и краткое описание обновления;
  - ссылку на статью с полным описанием обновления;
  - идентификатор и текст Лицензионного соглашения и Политики конфиденциальности для обновления программы;
  - идентификатор и текст Положения о Kaspersky Security Network для обновления программы;
  - признак возможности удаления обновления;
  - версии политики и плагина управления программы;
  - веб-адрес для загрузки плагина управления программы;
  - названия установленных обновлений программы, версии и даты их установки;
  - код и описание ошибки, если установка или удаление обновления завершились с ошибкой;
  - признак и причину необходимости перезагрузки устройства или программы по причине обновления программы.
- Согласие или несогласие пользователя с условиями Положения о Kaspersky Security Network, Лицензионного соглашения и Политики конфиденциальности.
- Список тегов, назначенных устройству.
- Список статусов устройства и их причины.
- Общий статус программы и статус всех ее компонентов; информацию о соответствии политике, статус постоянной защиты устройства.
- Дату и время последней проверки устройства; количество проверенных объектов; количество обнаруженных вредоносных объектов; количество заблокированных, удаленных и вылеченных объектов; количество объектов, которые не удалось вылечить; количество ошибок проверки; количество обнаруженных сетевых атак.
- Данные о текущих примененных значениях параметров программы.
- Текущий статус и результат выполнения групповых и локальных задач и значения их параметров.
- Информацию о внешних устройствах, подключенных к клиентскому устройству (идентификатор, имя, класс, производитель, описание, серийный номер и VID/PID).

- Информацию о файлах, помещенных в резервное хранилище (имя, путь, размер и тип объекта, описание объекта, имя обнаруженной угрозы, версия баз программы, с помощью которых была обнаружена угроза, дату и время помещения объекта в резервное хранилище, действия над объектом в резервном хранилище (удален, восстановлен), а также сами файлы по запросу администратора.
- Информацию о работе каждого компонента программы и о выполнении каждой задачи в виде событий:
  - дату и время возникновения события;
  - название и тип события;
  - уровень важности события;
  - имя задачи или компонента программы, во время работы которых произошло событие;
  - информацию о программе, которая вызвала событие: название программы, путь к файлу на диске, идентификатор процесса, значения параметров в случае публикации события о запуске или изменении параметров работы программы;
  - идентификатор пользователя;
  - имя инициатора (планировщика задач, или программы, или Kaspersky Security Center, или имя пользователя), действия которого привели к возникновению события;
  - имя и идентификатор пользователя, инициировавшего доступ к файлу;
  - результат обработки объекта или действия (описание, тип, название, уровень угрозы и точность, имя файла и тип операции над устройством, решение программы по этой операции);
  - информацию об объекте (имя и тип объекта, путь к объекту на диске, версия объекта, размер, информация о выполненном действии, описание причины возникновения события, описание причины необработки и пропуска объекта);
  - информацию об устройстве (имя производителя, имя устройства, путь, тип устройства, тип шины, идентификатор, VID/PID);
  - информацию о блокировке и разблокировке устройства; информацию о заблокированных подключениях (название, описание, имя устройства, протокол, удаленный адрес и порт, локальный адрес и порт, пакетные правила, действия);
  - информацию о запрошенном веб-адресе;
  - информацию об обнаруженных объектах;
  - тип и метод обнаружения;
  - информацию о выполненном действии;
  - информацию о базах программы (дату выпуска загруженных обновлений баз, информацию о применении баз, ошибки применения баз, информацию об отмене установленных обновлений баз);
  - информацию об обнаружении шифрования (имя шифровальщика; имя устройства, на котором обнаружено шифрование; информацию о блокировке и разблокировке устройства);
  - параметры программы и сетевые параметры;
  - информацию о сработавшем правиле Контроля программ (имя и тип) и результат его применения;
  - информацию о контейнерах и образах контейнеров, URL-адрес репозитория;

  - информацию об активных и заблокированных подключениях (название, описание и тип);
  - информацию о блокировке и разблокировке доступа к недоверенным компьютерам;
  - информацию о KSN (принятые соглашения, режимы работы, ошибки);
  - информацию о сертификатах (доменное имя, название субъекта, название издателя, дату окончания срока действия, статус сертификата, тип сертификата, время добавления сертификата).
- Информацию о работе задачи проверки целостности системы (имя, тип, путь) и информацию о снимке состояния системы.
- Информацию о сетевой активности, о пакетных правилах и о сетевых атаках.
- Информацию о роли пользователя:
  - имя и идентификатор пользователя, инициировавшего изменение роли пользователя;
  - роль пользователя;
  - имя пользователя, которому назначена или у которого отозвана роль.
- Информацию об исполняемых файлах, обнаруженных на компьютере (имя, путь, тип и хеш файла; список категорий, к которым отнесено приложение; первое время запуска файла; имя и версию программы; название производителя программы; информацию о сертификате, которым подписана программа: серийный номер, отпечаток, издатель, субъект, дату выпуска, дату окончания действия и публичный ключ).
- Информацию о контейнерах (имена контейнеров или образов контейнеров, пути к контейнерам или образам контейнеров, URL-адрес репозитория).

Данные, предоставляемые при использовании Kaspersky Security Network

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

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

Более подробная информация об отправке в "Лабораторию Касперского" статистических данных, полученных во время использования Kaspersky Security Network, их хранении и уничтожении приведена в Лицензионном соглашении, Положении о Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 202) и Политике конфиденциальности на веб-сайте "Лаборатории Касперского" https://www.kaspersky.ru/products-and-services-privacy-policy. Файлы license.<ID языка> и ksn_license.<ID языка> с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки программы.

kaspersky

Разделение доступа к функциям программы по пользовательским ролям

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

В операционной системе создаются четыре группы пользователей системы: *kesladmin*, *kesluser*, *keslaudit* и *nokesl*. Когда роль программы назначается пользователю (см. раздел "Назначение роли пользователю" на стр. 68) системы, этот пользователь добавляется в соответствующую группу ролей (см. таблицу *Роли* ниже). При отзыве роли у пользователя (см. раздел "Отзыв роли у пользователя" на стр. 68) пользователь удаляется из соответствующей группы ролей.

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

Таким образом, роли соответствуют четырем группам пользователей операционной системы:

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

В таблице ниже описаны три роли Kaspersky Endpoint Security и их права.

Таблица 4. Роли

Название роли	Роль в программе	Пользователь ОС	Права
Администратор	admin	kesladmin	Управление параметрами всех программ и задач. Управление лицензированием программы. Назначение ролей пользователям. Отзыв ролей у пользователей (администратор не имеет права отозвать роль `admin` у себя самого). Просмотр и управление хранилищами пользователей.
Пользователь	user	kesluser	Управление только задачами Scan_File. Запуск и остановка задач обновления. Просмотр отчетов для созданных пользователем задач. Просмотр особых событий, общих для всех пользователей программы.
Аудитор	audit	keslaudit	Просмотр параметров программы. Просмотр статуса программы. Просмотр всех задач, их параметров и расписания запуска. Просмотр всех событий. Просмотр всех объектов в Хранилище.
—	—	nokesl	Роль Kaspersky Endpoint Security не назначена, права отсутствуют.

В этом разделе

Просмотр списка пользователей и ролей

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

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

kaspersky

Назначение роли пользователю

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

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

Пример:

Назначить роль audit пользователю test15:

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

Отзыв роли у пользователя

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

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

Пример:

Отозвать роль audit у пользователя test15:

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

Интерфейсы управления программой

Вы можете управлять программой Kaspersky Endpoint Security следующими способами:

- С помощью команд управления программой из командной строки (см. раздел "Управление программой с помощью командной строки" на стр. 70).
- С помощью Консоли администрирования Kaspersky Security Center (см. раздел "Управление программой с помощью Консоли администрирования Kaspersky Security Center" на стр. 210).
- С помощью Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console (см. раздел "Управление программой с помощью Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console" на стр. 294).
- С помощью графического пользовательского интерфейса (см. раздел "Управление программой с помощью графического пользовательского интерфейса" на стр. 368).

kaspersky

Управление программой с помощью командной строки

Вы можете управлять программой Kaspersky Endpoint Security с помощью командной строки. Из командной строки доступны все действия, включая управление задачами (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92) и настройка параметров программы.

В этом разделе

Запуск и остановка программы

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

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

Для запуска программы требуется, чтобы учетная запись root была владельцем следующих директорий и только владелец имел право на запись в них: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

Запуск, перезапуск и остановка программы Kaspersky Endpoint Security

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

  ```
  systemctl start kesl
  ```

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

  ```
  systemctl stop kesl
  ```

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

  ```
  systemctl restart kesl
  ```

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

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

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

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

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

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

Мониторинг статуса программы Kaspersky Endpoint Security

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

В случае сбоя программы создается файл дампа, и программа автоматически перезапускается.

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

  ```
  systemctl status kesl
  ```

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

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

Вывод справки о командах

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

Синтаксис команды

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

<набор команд программы>

Доступные значения:

`-T` – команды управления задачами (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92) и общими параметрами программы (см. раздел "Изменение общих параметров программы" на стр. 87).

`-C` – команды управления общими параметрами проверки контейнеров (см. раздел "Изменение общих параметров проверки контейнеров" на стр. 91).

`-N` – команды управления параметрами проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 104).

`-L` – команды управления задачей Лицензирование (см. раздел "Задача Лицензирование (License, ID:9)" на стр. 151).

`-E` – команды управления событиями программы (см. раздел "Просмотр событий" на стр. 206).

`-B` – команды управления задачей Управление Хранилищем (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 153).

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

`-H` – команды управления задачей Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 163).

`-D` – команды управления задачей Контроль устройств.

`-A` – команды управления задачей Контроль программ (см. раздел "Задача Контроль программ (Application_Control, ID:21)" на стр. 192).

`-U` – команды управления пользователями и ролями пользователей (см. раздел "Разделение доступа к функциям программы по пользовательским ролям" на стр. 66).

`-S` – команды статистики (см. раздел "Просмотр информации о программе" на стр. 73).

`-W` – вывод событий (см. раздел "Включение вывода событий" на стр. 73).

Включение автоматического дополнения команды kesl-control (bash completion)

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

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

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

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

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

kaspersky

Включение вывода событий

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

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

Кроме того, вы можете использовать команду `kesl-control -W` с флагом `--query`, чтобы указать условия фильтра (см. раздел "Использование фильтра для ограничения результатов запроса" на стр. 79) для вывода определенных событий.

Синтаксис команды

```
kesl-control -W
```

Примеры:

Включить режим вывода текущих событий программы:

```
kesl-control -W
```

Включить вывод текущих событий задачи с ID=1:

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

Включить вывод текущих событий TaskStateChanged:

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

Просмотр информации о программе

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

Синтаксис команды

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

Результат выполнения команды:

- **Название**. Название программы.
- **Версия**. Текущая версия программы.
- **Политика**. Отображается, применяется ли политика Kaspersky Security Center.
- **Информация о лицензии**. Информация о лицензии или статус лицензионного ключа.
- **Статус подписки**. Статус подписки. Это поле отображается, если программа используется по подписке.
- **Дата окончания срока действия лицензии**. Дата и время окончания срока действия лицензии в формате UTC.
- **Статус файла MDR BLOB**. Статус конфигурационного файла BLOB для интеграции с Managed Detection and Response.

- **Дата окончания срока действия лицензии на использование MDR**. Дата и время окончания срока действия лицензии на использование Managed Detection and Response в формате UTC.
- **Состояние Хранилища**. Состояние Хранилища (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 153).
- **Использование Хранилища**. Размер Хранилища (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 153).
- **Дата последнего запуска задачи Scan_My_Computer**. Время последнего запуска задачи Антивирусная проверка (см. раздел "Задача Антивирусная проверка (Scan_My_Computer, ID:2)" на стр. 120).
- **Дата последнего выпуска баз программы**. Время последнего выпуска баз программы (см. раздел "Задача Обновление (Update, ID:6)" на стр. 146).
- **Базы программы загружены**. Отображается, загружены ли баз программы (см. раздел "Задача Обновление (Update, ID:6)" на стр. 146).
- **Состояние Kaspersky Security Network**. Информация об участии в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 202).
- **Состояние Managed Detection and Response**. Состояние Managed Detection and Response: активный, неактивный.
- **Защита от файловых угроз**. Состояние задачи Защита от файловых угроз (см. раздел "Задача Защита от файловых угроз (File_Threat_Protection, ID:1)" на стр. 108).
- **Мониторинг контейнеров**. Отображается информация о параметрах проверки контейнеров (см. раздел "Описание общих параметров проверки контейнеров" на стр. 89).
- **Контроль целостности системы**. Состояние задачи Контроль целостности системы (см. раздел "Задача Контроль целостности системы (System_Integrity_Monitoring, ID:11)" на стр. 156).
- **Управление сетевым экраном**. Состояние задачи Управление сетевым экраном.
- **Защита от шифрования**. Состояние задачи Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 163).
- **Защита от веб-угроз**. Состояние задачи Защита от веб-угроз (см. раздел "Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)" на стр. 169).
- **Контроль устройств**. Состояние задачи Контроль устройств.
- **Проверка съемных дисков**. Состояние задачи Проверка съемных дисков (см. раздел "Задача Проверка съемных дисков (Removable_Drives_Scan, ID:16)" на стр. 172).
- **Защита от сетевых угроз**. Состояние задачи Защита от сетевых угроз.
- **Анализ поведения**. Состояние задачи Анализ поведения (см. раздел "Задача Анализ поведения (Behavior_Detection, ID:20)" на стр. 191).
- **Контроль программ**. Состояние задачи Контроль программ (см. раздел "Задача Контроль программ (Application_Control, ID:21)" на стр. 192).
- **Состояние обновления**. Отображаются действия по обновлению программы и действия, которые требуется выполнить пользователю.
- **Программа работает нестабильно**. Отображается информация о сбое программы и создании файла дампа. Это поле отображается, если при предыдущем запуске программы произошел сбой.

kaspersky

Описание команд программы

Вывод справки о командах программы

--help – выводит справку о командах программы.

Вывод событий программы

-W – включает вывод событий программы (см. раздел "Включение вывода событий" на стр. 73).

Команды статистики

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

[-S] --app-info – выводит информацию о программе (см. раздел "Просмотр информации о программе" на стр. 73).

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

Команды управления параметрами и задачами программы

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

[-T] --get-app-settings --file <имя и путь к файлу> – выводит общие параметры программы (см. раздел "Изменение общих параметров программы" на стр. 87).

[-T] --set-app-settings --file <имя и путь к файлу> – устанавливает общие параметры программы (см. раздел "Изменение общих параметров программы" на стр. 87).

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

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

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

[-T] --get-task-list – выводит список существующих задач программы (см. раздел "Просмотр списка задач" на стр. 95).

[-T] --get-task-state <ID задачи>|<название задачи> – выводит состояние указанной задачи (см. раздел "Просмотр состояния задачи" на стр. 99).

[-T] --create-task <название задачи> --type <тип задачи> --file <имя и путь к файлу> – создает задачу (см. раздел "Создание задачи" на стр. 96) указанного типа, импортирует в задачу параметры из указанного конфигурационного файла.

[-T] --delete-task <ID задачи>|<название задачи> – удаляет задачу (см. раздел "Удаление задачи" на стр. 104).

[-T] --start-task <ID задачи>|<название задачи> [-W] [--progress] [--file <имя и путь к файлу>] – запускает задачу (см. раздел "Запуск и остановка задачи" на стр. 98).

[-T] --stop-task <ID задачи>|<название задачи> – останавливает задачу (см. раздел "Запуск и остановка задачи" на стр. 98).

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

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

[-T] --scan-file <путь> [--action <действие>] – создает и запускает временную задачу Выборочная проверка (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 129).

[-T] --scan-container <контейнер|образ[:тег]> – создает временную задачу Выборочная проверка контейнеров (см. раздел "Задача Выборочная проверка контейнеров (Custom_Container_Scan, ID:19)" на стр. 184). После завершения проверки временная задача автоматически удаляется.

[-T] --get-settings <ID задачи>|<название задачи> --file <имя и директория файла> – выводит параметры задачи (см. раздел "Изменение параметров задачи с помощью командной строки" на стр. 97).

[-T] --set-settings <ID задачи>|<название задачи> [<параметры>] [--file <имя и директория файла>] [--add-path <путь>] [--del-path <путь>] [--add-exclusion <исключение>] [--del-exclusion <исключение>] – устанавливает параметры задачи (см. раздел "Изменение параметров задачи с помощью командной строки" на стр. 97).

[-T] --set-settings [<ID задачи>|<название задачи>] set-to-default – восстанавливает значения по умолчанию для параметров задачи (см. раздел "Восстановление заданных по умолчанию параметров задачи" на стр. 98).

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

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

Команды управления параметрами проверки контейнеров

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

[-C] --get-container-settings --file <имя и путь к файлу> – выводит общие параметры проверки контейнеров (см. раздел "Изменение общих параметров проверки контейнеров" на стр. 91).

[-C] --set-container-settings --file <имя и путь к файлу> – устанавливает общие параметры проверки контейнеров (см. раздел "Изменение общих параметров проверки контейнеров" на стр. 91).

Команды управления параметрами проверки зашифрованных соединений

-N – префикс, указывающий, что команда принадлежит к группе команд управления параметрами проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 104).

-N --query user – выводит список исключений из проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 104), добавленных пользователем.

-N --query auto – выводит список исключений из проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 104), добавленных программой.

-N --query kl – выводит список исключений из проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 104), полученных из баз "Лаборатории Касперского".

-N --clear-web-auto-excluded – очищает список доменов, которые программа автоматически исключила из проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 104).

[-N] --get-net-settings [--file <имя и путь к файлу>] – выводит параметры проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 104) в файл формата INI.

[-N] --set-net-settings [--file <имя и путь к файлу>] – устанавливает параметры проверки зашифрованных соединений (см. раздел "Проверка зашифрованных соединений" на стр. 104).

[-N] --add-certificate <путь к файлу сертификата> – добавляет сертификат в список доверенных сертификатов (см. раздел "Управление доверенными сертификатами" на стр. 107).

[-N] --remove-certificate <субъект сертификата> – удаляет сертификат из списка доверенных сертификатов (см. раздел "Управление доверенными сертификатами" на стр. 107).

[-N] --list-certificates – выводит список доверенных сертификатов (см. раздел "Управление доверенными сертификатами" на стр. 107).

Команды управления пользователями и ролями

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

[-U] --get-user-list – выводит список пользователей и ролей (см. раздел "Просмотр списка пользователей и ролей" на стр. 67).

[-U] --grant-role <роль> <пользователь> – присваивает роль (см. раздел "Назначение роли пользователю" на стр. 68) определенному пользователю.

[-U] --revoke-role <роль> <пользователь> – отзывает роль (см. раздел "Отзыв роли у пользователя" на стр. 68) у определенного пользователя.

Команды лицензирования

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

[-L] --add-active-key <код активации>|<файл ключа> – добавляет активный ключ (см. раздел "Добавление активного ключа" на стр. 151).

[-L] --add-reserve-key <код активации>|<файл ключа> – добавляет резервный ключ (см. раздел "Добавление резервного ключа" на стр. 151).

[-L] --remove-active-key – удаляет активный ключ (см. раздел "Удаление активного ключа" на стр. 152).

[-L] --remove-reserve-key – удаляет резервный ключ (см. раздел "Удаление резервного ключа" на стр. 152).

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

Команды управления задачей Управление сетевым экраном

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

[-F] --add-rule [--name <строка>] [--action <действие>] [--protocol <протокол>] [--direction <директория>] [--remote <удаленная>] [--local <локальная>] [--at <индекс>] – добавляет новое правило.

[-F] --del-rule [--name <строка>] [--index <индекс>] – удаляет правило.

[-F] --move-rule [--name <строка>] [--index <индекс>] [--at <индекс>] – изменяет приоритет выполнения 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 – выводит информацию о задаче.

Команды управления задачей Защита от шифрования

-H –префикс, указывающий, что команда принадлежит к группе команд управления задачей Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 163).

[-H] --get-blocked-hosts – отображает список заблокированных компьютеров (см. раздел "Просмотр списка заблокированных компьютеров" на стр. 167).

[-H] --allow-hosts – разблокирует недоверенные компьютеры (см. раздел "Разблокировка заблокированных компьютеров" на стр. 167).

Команды управления задачей Контроль устройств

-D – префикс, указывающий, что команда принадлежит к группе команд Контроля устройств.

[-D] --get-device-list – отображает список устройств, подключенных к компьютеру.

Команды управления задачей Контроль программ

-A – префикс, указывающий, что команда принадлежит к группе команд Контроля программ (см. раздел "Задача Контроль программ (Application_Control, ID:21)" на стр. 192).

[-A] --get-app-list – отображает список программ (см. раздел "Просмотр списка обнаруженных программ" на стр. 200), обнаруженных на компьютере во время выполнения задачи Инвентаризация (см. раздел "Задача Инвентаризация (Inventory_Scan, ID:22)" на стр. 198).

[-A] --get-categories – отображает список созданных категорий Контроля программ (см. раздел "Просмотр списка созданных категорий" на стр. 197).

Команды управления Хранилищем

-B – префикс, указывающий, что команда принадлежит к группе команд управления Хранилищем (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 153).

[-B] --mass-remove --query – очищает Хранилище (см. раздел "Удаление объектов из Хранилища" на стр. 155), полностью или выборочно.

-B --query <фильтр> – выводит информацию об объектах в Хранилище, соответствующих условиям фильтра (см. раздел "Использование фильтра для ограничения результатов запроса" на стр. 79).

[-B] --restore <ID объекта> --file <имя и путь к файлу> – восстанавливает объект (см. раздел "Восстановление объектов из Хранилища" на стр. 154) из Хранилища.

Команды управления журналом событий

-E – префикс, указывающий, что команда принадлежит к группе команд управления журналом событий (см. раздел "Просмотр событий" на стр. 206).

-E --query <фильтр> --db <файл базы данных> -n <количество> --file <имя и путь к файлу> [--json] – выводит информацию о событиях, соответствующих условиям фильтра (см. раздел "Использование фильтра для ограничения результатов запроса" на стр. 79), из базы данных журнала событий в указанный файл.

Где:

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

<фильтр> – условия фильтра для ограничения результатов запроса (см. раздел "Использование фильтра для ограничения результатов запроса" на стр. 79);

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

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

Использование фильтра для ограничения результатов запроса

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

- Получение информации о событиях программы:

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

- Получение информации об объектах в Хранилище (см. раздел "Просмотр идентификаторов объектов в Хранилище" на стр. 154):

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

- Удаление выбранных объектов из Хранилища (см. раздел "Удаление объектов из Хранилища" на стр. 155):

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

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

Синтаксис

```
"<поле> <логическое выражение> '<значение>'"
```

```
"<поле> <логическое выражение> '<значение>' и <поле> <логическое выражение> '<значение>'"
```

Таблица 5. Описание логических выражений

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

Примеры:

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

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

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

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

Вывести события с типом ThreatDetected (обнаружена угроза):

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

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

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

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

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

Экспорт и импорт параметров программы

Kaspersky Endpoint Security позволяет 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 программа должна быть запущена. После импорта параметров требуется перезапустить программу.

При импорте или экспорте параметров из более старой версии программы для новых параметров устанавливаются значения по умолчанию. Импорт параметров в более старую версию программы недоступен.

Экспорт параметров

Для экспорта параметров предназначена команда `kesl-control --export-settings`.

Синтаксис команды

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

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут сохранены параметры программы;

`--json` – формат конфигурационного файла, в который будут сохранены параметры программы. Если вы не укажете формат файла, экспорт будет выполнен в файл формата INI.

Импорт параметров

Для импорта параметров предназначена команда `kesl-control --import-settings`.

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

Синтаксис команды

```
kesl-control --import-settings --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры программы;

`--json` – формат конфигурационного файла, из которого будут импортированы параметры программы. Если вы не укажете формат файла, программа попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

При импорте параметров программы в сертифицированной версии программы для параметра `UseKSN` устанавливается значение `No`. Чтобы начать или возобновить участие в Kaspersky Security Network (см. стр. 202), вам нужно указать значение `UseKSN=Basic` или `UseKSN=Extended`. Параметры задач Управление сетевым экраном, Контроль устройств и Защита от сетевых угроз не импортируются, так как эти задачи недоступны.

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

Установка ограничения на использование памяти программой

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

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

Минимальное значение параметра: 2048 МБ. Значение по умолчанию: 8192 МБ. Если указанное значение меньше 2048 МБ, программа будет использовать минимальное значение (2048 МБ). Если указанное значение превышает размер оперативной памяти, будет использоваться до 40% оперативной памяти. Это значение изменить невозможно.

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

1. Остановите Kaspersky Endpoint Security (см. раздел "Запуск и остановка программы" на стр. 70).

2. Откройте файл /var/opt/kaspersky/kesl/common/kesl.ini на редактирование.
3. Добавьте следующий параметр в секцию `[General]`:

   `ScanMemoryLimit=<ограничение на использование памяти в мегабайтах>`
4. Запустите Kaspersky Endpoint Security (см. раздел "Запуск и остановка программы" на стр. 70).

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

Общие параметры программы

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

В этом разделе

Описание общих параметров программы

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

Таблица 6. Общие параметры программы

Параметр	Описание	Значения
`SambaConfigPath`	Директория, в которой хранится конфигурационный файл Samba. Конфигурационный файл Samba нужен для обеспечения работы значений `AllShared` или `Shared:SMB` для параметра `Path`.	По умолчанию указана стандартная директория конфигурационного файла Samba на компьютере. Значение по умолчанию: /etc/samba/smb.conf. После изменения значения этого параметра требуется перезапустить программу.
`NfsExportPath`	Директория, в которой хранится конфигурационный файл NFS. Конфигурационный файл NFS нужен для обеспечения работы значений `AllShared` или `Shared:NFS` для параметра `Path`.	По умолчанию указана стандартная директория конфигурационного файла NFS на компьютере. Значение по умолчанию: /etc/exports. После изменения значения этого параметра требуется перезапустить программу.

Параметр	Описание	Значения
`TraceLevel`	Включение создания и уровень детализации файла трассировки (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 381).	`Detailed` – создавать детализированный файл трассировки. `MediumDetailed` – создавать файл трассировки, содержащий информационные сообщения и сообщения об ошибках. `NotDetailed` – создавать файл трассировки, содержащий сообщения об ошибках. `None` (значение по умолчанию) – не создавать файл трассировки.
`TraceFolder`	Директория, в которой хранятся файлы трассировки программы. В файлах трассировки (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 381) содержится информация об операционной системе, а также могут содержаться персональные данные (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 381).	Значение по умолчанию: /var/log/kaspersky/kesl. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, с правами которой работает Kaspersky Endpoint Security. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права. После изменения значения этого параметра требуется перезапустить программу.
`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.	`1-10000` Значение по умолчанию: `5`. После изменения значения этого параметра требуется перезапустить программу.
`TraceMaxFileSize`	Максимальный размер файла трассировки программы (в мегабайтах).	`1-1000` Значение по умолчанию: `500`. После изменения значения этого параметра требуется перезапустить программу.

Параметр	Описание	Значения
`BlockFilesGreaterMaxFileNamePath`	Блокировка доступа к файлам, длина полного пути к которым превышает заданное значение параметра (в байтах). Если длина полного пути к проверяемому файлу превышает значение этого параметра, задачи антивирусной проверки пропускают такой файл при проверке. Этот параметр недоступен для операционных систем, в которых используется технология fanotify.	`4096-33554432` Значение по умолчанию: `16384`. После изменения значения этого параметра требуется перезапустить задачу Защита от файловых угроз.
`DetectOtherObjects`	Включение обнаружения легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.	`Yes` – включить обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя. `No` (значение по умолчанию) – выключить обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.
`NamespaceMonitoring`	Включение проверки пространств имен и контейнеров.	`Yes` (значение по умолчанию) – включить проверку пространств имен и контейнеров. `No` – выключить проверку пространств имен и контейнеров.
`InterceptorProtectionMode`	Режим работы файлового перехватчика, включающий или выключающий блокировку файлов, в которых обнаружены угрозы при выполнении задачи Защита от файловых угроз. Этот параметр также влияет на работу задач Защита от шифрования, Контроль устройств и Проверка съемных дисков.	`Block` (значение по умолчанию) – блокировать файлы, в которых обнаружены угрозы. `Notify` – не блокировать файлы, в которых обнаружены угрозы, при обнаружении угрозы записывать событие в журнал событий. Выбор значения `Notify` снижает уровень защиты компьютера.

Параметр	Описание	Значения
`UseKSN`	Включение участия в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 202).	`Basic` – включить участие в Kaspersky Security Network без отправки статистики. `Extended` – включить участие в Kaspersky Security Network с отправкой статистики. `No` (значение по умолчанию) – выключить участие в Kaspersky Security Network. В сертифицированной версии программы используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается, так как приводит к выходу программы из сертифицированного состояния.
`UseMDR`	Включение Managed Detection and Response.	`Yes` – включить Managed Detection and Response. `No` (значение по умолчанию) – выключить Managed Detection and Response. В сертифицированной версии программы интеграция с Kaspersky Managed Detection and Response не поддерживается.
`UseProxy`	Включение использования прокси-сервера компонентами программы Kaspersky Endpoint Security. Прокси-сервер может использоваться для взаимодействия с Kaspersky Security Network, для активации программы и при обновлении баз программы.	`Yes` – включить использование прокси-сервера. `No` (значение по умолчанию) – выключить использование прокси-сервера.

Параметр	Описание	Значения
ProxyServer	Параметры прокси-сервера в формате [пользователь[:пароль]@]узел[:порт]. Для подключения через HTTP-прокси рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси использует незащищенное соединение, и учетная запись может быть скомпрометирована.	—
MaxEventsNumber	Максимальное количество событий, которые будет хранить программа. При превышении заданного количества событий программа удаляет наиболее давние события.	Значение по умолчанию: 500000. Если задано значение 0, то события не сохраняются.
LimitNumberOfScanFileTasks	Максимальное количество задач типа Scan_File, которые непривилегированный пользователь может одновременно запустить на компьютере. Этот параметр не ограничивает количество задач, которые может запустить пользователь с root-правами.	0–4294967295 Значение по умолчанию: 0. Если задано значение 0, непривилегированный пользователь не может запускать задачи типа Scan_File. Если во время установки программы вы также установили пакет графического интерфейса, для параметра LimitNumberOfScanFileTasks по умолчанию используется значение 5.
UseSyslog	Включение записи информации о событиях в syslog. Для доступа к syslog требуются root-права.	Yes – включить запись информации о событиях в syslog. No (значение по умолчанию) – выключить запись информации о событиях в syslog.
EventsStoragePath	Директория базы данных, в которой программа сохраняет информацию о событиях. Для доступа к заданной по умолчанию базе данных событий требуются root-права.	Значение по умолчанию: /var/opt/kaspersky/kesl/private/storage/events.db.

Параметр	Описание	Значения
ExcludedMountPoint.item_#	Точка монтирования, которую требуется исключить из области проверки для задач, использующих перехватчик файловых операций (Защита от файловых угроз и Защита от шифрования). Вы можете указать несколько точек монтирования, которые требуется исключить из проверки. Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды mount. Параметр ExcludedMountPoint.item_# по умолчанию не указан.	AllRemoteMounted – исключать из 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 SMB. Mounted:<тип файловой системы> – исключать из проверки все смонтированные директории с указанным типом файловой системы. /mnt – исключать из проверки объекты, находящиеся в директории /mnt (включая вложенные директории), используемой в качестве временной точки монтирования съемных дисков. <путь, содержащий маску /mnt/user* или /mnt/**/user_share> – исключать из проверки объекты, находящиеся в директориях, имена которых содержат указанную маску.
MemScanExcludedProgramPath.item_#	Исключение памяти процесса из проверки. Программа не будет проверять память указанного процесса.	<полный путь к процессу> – исключать из проверки процесс в указанной локальной директории. Для указания пути можно использовать маски.

Изменение общих параметров программы

Для изменения параметров программы требуется наличие root-прав.

► *Чтобы изменить общие параметры программы:*

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

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

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

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

Программа применит новые значения параметров после перезапуска (см. раздел "Запуск и остановка программы" на стр. 70).

Вы можете использовать созданный конфигурационный файл для импорта параметров в программу, установленную на другом компьютере.

Команда kesl-control --get-app-settings

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

Синтаксис команды

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

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут сохранены параметры программы. Если вы укажете имя файла, не указав пути к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, конфигурационный файл не будет создан. Если вы не укажете ключ --file, общие параметры программы будут выведены в консоль.

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

Пример:

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

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

Команда kesl-control --set-app-settings

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

Синтаксис команды

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

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

Аргументы и ключи

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

`--json` – формат конфигурационного файла, параметры из которого будут импортированы в программу. Если вы не укажете формат файла, программа попытается выполнить импорт из файла формата INI.

Примеры:

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

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

Установить низкий уровень детализации 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"
```

Описание общих параметров проверки контейнеров

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

Включение проверки пространств имен и контейнеров выполняется с помощью параметра `NamespaceMonitoring`, описанного в общих параметрах программы.

Таблица 7. Общие параметры проверки контейнеров и пространств имен

Параметр	Описание	Значения
`OnAccessContainerScanAction`	Действие над контейнером при обнаружении зараженного объекта. Этот параметр доступен при использовании программы по лицензии, которая включает эту функцию. Действие над контейнером при обнаружении зараженного объекта также зависит от заданных параметров задачи Защита от файловых угроз (см. таблицу ниже). Действия над зараженным объектом внутри контейнера описаны в параметрах задачи Проверка контейнеров (см. раздел "Параметры задачи Проверка контейнеров" на стр. 174).	`StopContainerIfFailed` (значение по умолчанию) – остановить контейнер, если не удалось вылечить или удалить зараженный объект. `StopContainer` – остановить контейнер при обнаружении зараженного объекта. `Skip` – не выполнять никаких действий над контейнерами при обнаружении зараженного объекта.
`UseDocker`	Использование среды Docker.	`Yes` (значение по умолчанию) – использовать среду Docker. `No` – не использовать среду Docker.
`DockerSocket`	Путь или URI (универсальный идентификатор ресурса) Docker-сокета.	Значение по умолчанию: /var/run/docker.sock.
`UseCrio`	Использование среды CRI-O.	`Yes` (значение по умолчанию) – использовать среду CRI-O. `No` – не использовать среду CRI-O.
`CrioConfigFilePath`	Путь к конфигурационному файлу CRI-O.	Значение по умолчанию: /etc/crio/crio.conf.
`UsePodman`	Использование утилиты Podman.	`Yes` (значение по умолчанию) – использовать утилиту Podman. `No` – не использовать утилиту Podman.
`PodmanBinaryPath`	Путь к исполняемому файлу утилиты Podman.	Значение по умолчанию: /usr/bin/podman.
`PodmanRootFolder`	Путь к корневой директории хранилища контейнеров.	Значение по умолчанию: /var/lib/containers/storage.

Параметр	Описание	Значения
UseRunc	Использование утилиты runc.	Yes (значение по умолчанию) – использовать утилиту runc. No – не использовать утилиту.
RuncBinaryPath	Путь к исполняемому файлу утилиты runc.	Значение по умолчанию: /usr/bin/runc.
RuncRootFolder	Путь к корневой директории хранилища состояний контейнеров.	Значение по умолчанию: /run/runc-ctrs.

Действие над контейнером при обнаружении зараженного объекта может меняться в зависимости от заданных значений параметров FirstAction и SecondAction задачи Защита от файловых угроз (см. раздел "Параметры задачи Защита от файловых угроз" на стр. 109) и от значения параметра InterceptorProtectionMode общих параметров программы (см. таблицу ниже).

Таблица 8. Зависимость действия над контейнером от заданного действия над зараженными объектами

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

Изменение общих параметров проверки контейнеров

Изменение общих параметров проверки контейнеров

Для изменения параметров программы требуется наличие root-прав.

► *Чтобы изменить общие параметры проверки контейнеров:*

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

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

5. Откройте созданный конфигурационный файл, измените нужные параметры проверки контейнеров и сохраните изменения.

6. Импортируйте параметры проверки контейнеров из конфигурационного файла в программу Kaspersky Endpoint Security с помощью команды --set-app-settings:

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

Программа применит новые значения параметров после перезапуска (см. раздел "Запуск и остановка программы" на стр. 70).

Команда kesl-control --get-container-settings

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

Синтаксис команды

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

Аргументы и ключи

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

Если вы укажете имя файла, не указав пути к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, конфигурационный файл не будет создан.

Команда kesl-control --set-container-settings

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

Синтаксис команды

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

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

Аргументы и ключи

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

Управление задачами программы с помощью командной строки

Вы можете управлять работой программы с помощью задач как локально на компьютере (с помощью командной строки или конфигурационных файлов), так и с помощью Консоли администрирования (см. раздел "Управление задачами в Консоли администрирования Kaspersky Security Center" на стр. 259) или Kaspersky Security Center Web Console (см. раздел "Управление задачами в Web Console" на стр. 339).

Для работы с программой предусмотрено два типа задач:

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

- *Пользовательская задача* – задача, которую вы можете создавать или удалять самостоятельно. Вы можете создавать пользовательские задачи следующих типов: ODS, Update, Rollback, ODFIM и ContainerScan.

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

Предустановленные задачи Kaspersky Endpoint Security перечислены в таблице.

Таблица 9. Задачи Kaspersky Endpoint Security

Имя задачи	Имя задачи в командной строке	ID задачи	Тип задачи
Защита от файловых угроз (см. раздел "Задача Защита от файловых угроз (File_Threat_Protection, ID:1)" на стр. 108)	File_Threat_Protection	1	OAS
Антивирусная проверка (см. раздел "Задача Антивирусная проверка (Scan_My_Computer, ID:2)" на стр. 120)	Scan_My_Computer	2	ODS
Выборочная проверка (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 129)	Scan_File	3	ODS
Проверка важных областей (см. раздел "Задача Проверка важных областей (Critical_Areas_Scan, ID:4)" на стр. 138)	Critical_Areas_Scan	4	ODS
Обновление (см. раздел "Задача Обновление (Update, ID:6)" на стр. 146)	Update	6	Update
Откат обновления баз (см. раздел "Задача Откат обновления баз (Rollback, ID:7)" на стр. 150)	Rollback	7	Rollback
Лицензирование (см. раздел "Задача Лицензирование (License, ID:9)" на стр. 151)	License	9	License
Управление хранилищем (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 153)	Backup	10	Backup
Контроль целостности системы (см. раздел "Задача Контроль целостности системы (System_Integrity_Monitoring, ID:11)" на стр. 156)	System_Integrity_Monitoring	11	OAFIM
Управление сетевым экраном	Firewall_Management	12	Firewall
Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 163)	Anti_Cryptor	13	AntiCryptor

Имя задачи	Имя задачи в командной строке	ID задачи	Тип задачи
Защита от веб-угроз (см. раздел "Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)" на стр. 169)	Web_Threat_Protection	14	WTP
Контроль устройств	Device_Control	15	DeviceControl
Проверка съемных дисков (см. раздел "Задача Проверка съемных дисков (Removable_Drives_Scan, ID:16)" на стр. 172)	Removable_Drives_Scan	16	RDS
Защита от сетевых угроз	Network_Threat_Protection	17	NTP
Проверка контейнеров (см. раздел "Задача Проверка контейнеров (Container_Scan, ID:18)" на стр. 174)	Container_Scan	18	ContainerScan
Выборочная проверка контейнеров (см. раздел "Задача Выборочная проверка контейнеров (Custom_Container_Scan, ID:19)" на стр. 184)	Custom_Container_Scan	19	ContainerScan
Анализ поведения (см. раздел "Задача Анализ поведения (Behavior_Detection, ID:20)" на стр. 191)	Behavior_Detection	20	BehaviorDetection
Контроль программ (см. раздел "Задача Контроль программ (Application_Control, ID:21)" на стр. 192)	Application_Control	21	AppControl
Инвентаризация (см. раздел "Задача Инвентаризация (Inventory_Scan, ID:22)" на стр. 198)	Inventory_Scan	22	InventoryScan

Вы можете выполнять следующие действия над задачами:

- запускать и останавливать задачи;
- создавать и удалять пользовательские задачи;
- изменять параметры задач.

kaspersky

В этом разделе

Просмотр списка задач

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

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

где:

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

Отобразится список задач программы Kaspersky Endpoint Security.

Для каждой задачи отображается следующая информация:

- `Name`. Имя задачи (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92).
- `ID`. Идентификатор задачи (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92).
- `Type`. Тип задачи (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92).
- `State`. Текущее состояние задачи.

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

kaspersky

Создание задачи

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

Вы можете создавать только задачи следующих типов: ODS, Update (см. раздел "Задача Обновление (Update, ID:6)" на стр. 146), Rollback (см. раздел "Задача Откат обновления баз (Rollback, ID:7)" на стр. 150), ODFIM (см. раздел "Контроль целостности системы по требованию (ODFIM)" на стр. 157) и ContainerScan.

► *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>` – тип задачи (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92).

Задача указанного типа создается с параметрами по умолчанию.

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

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

где:

- `<имя задачи>` – имя, которое вы указываете для новой задачи;
- `<тип задачи>` – тип задачи (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92);
- `<полный путь к конфигурационному файлу>` – полный путь к конфигурационному файлу (см. раздел "Приложение 2. Конфигурационные файлы программы" на стр. 389).

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:*

1. Сохраните параметры задачи в конфигурационный файл:

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

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

4. Сохраните изменения в конфигурационном файле.
5. Импортируйте в задачу параметры из конфигурационного файла:

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

Параметры задачи обновятся.

> В случае, если в параметрах задачи Контроль программ (см. раздел "Задача Контроль программ (Application_Control, ID:21)" на стр. 192) вы меняете разрешающий список или запрещаете запуск всех программ и / или программ, влияющих на работу Kaspersky Endpoint Security, требуется запускать команду `--set-settings` с флагом `--accept`.

Изменение параметров задачи с помощью командной строки

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

1. Укажите нужное значение параметра:

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

   Программа изменит указанный параметр.

   > В случае, если в параметрах задачи Контроль программ (см. раздел "Задача Контроль программ (Application_Control, ID:21)" на стр. 192) вы меняете разрешающий список или запрещаете запуск всех программ и / или программ, влияющих на работу программы Kaspersky Endpoint Security, требуется запускать команду `--set-settings` с флагом `--accept`.

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

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

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

Пример:

Чтобы указать новую область проверки, выполните следующую команду:

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

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

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

Восстановление заданных по умолчанию параметров задачи

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

Восстановление заданных по умолчанию параметров недоступно для задач Откат обновления баз (см. раздел "Задача Откат обновления баз (Rollback, ID:7)" на стр. 150) и Управление Хранилищем (см. раздел "Задача Управление Хранилищем (Backup, ID:10)" на стр. 153).

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

1. Выполните следующую команду:

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

   Программа изменит значения параметров на заданные по умолчанию.

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

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

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

Запуск и остановка задачи

По умолчанию при запуске программы автоматически запускаются задачи Защита от файловых угроз, Контроль устройств и Анализ поведения. Остальные задачи остановлены (см. раздел "Просмотр состояния задачи" на стр. 99) (имеют статус *Stopped*).

Вы можете запустить задачу в любой момент.

Вы не можете запускать и останавливать задачи 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>
```

Просмотр состояния задачи

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

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

где:

- `<ID задачи>` – идентификатор задачи, который программа присвоила задаче в момент создания.
- `<имя задачи>` – название задачи.

Задачи программы могут находиться в одном из следующих состояний:

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

Задачи Scan_My_Computer, Scan_File, Critical_Areas_Scan, Container_Scan и Custom_Container_Scan могут также находиться в одном из следующих состояний:

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

Задачи Backup и License нельзя запускать, приостанавливать и останавливать. Они могут находиться только в состоянии `Started`.

Настройка расписания задачи

Вы можете просмотреть и настроить параметры расписания запуска задач следующих типов (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92): ODS, Update и Rollback.

kaspersky

Изменение параметров расписания задачи

► *Чтобы настроить параметры расписания задачи:*

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

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

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

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

Программа применит новые значения параметров расписания немедленно.

Параметры расписания задачи

В программе предусмотрены следующие параметры для настройки расписания запуска задачи:

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

где:

PS – запускать задачу после запуска программы.

BR – запускать задачу после обновления баз программы.

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 – включение запуска пропущенной задачи после запуска программы.

Примеры:

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

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2020/May/30 23:05:00;10
RandomInterval=0
```

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

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

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

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

Чтобы настроить запуск задачи каждый вторник, укажите следующие параметры:

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

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

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

Команда kesl-control --get-schedule

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

Синтаксис команды

```
kesl-control [-T] --get-schedule <ID задачи>|<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 программе.

`<имя задачи>` – имя задачи.

`--file <имя конфигурационного файла>` – имя конфигурационного файла, в который будут сохранены параметры расписания. Если вы укажете имя файла, не указав пути к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, конфигурационный файл не будет создан.

Примеры:

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

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

Вывести расписание задачи обновления:

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

Команда kesl-control --set-schedule

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

Синтаксис команды

```
kesl-control --set-schedule <ID задачи>|<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 программе.

`<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
```

kaspersky

Управление областями проверки из командной строки

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

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

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

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

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

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

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

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

Управление областями исключения из командной строки

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

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

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

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

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

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

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

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

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

Удаление задачи

Вы можете удалять только те задачи, которые вы создали. Вы не можете удалять предустановленные задачи.

► *Чтобы удалить задачу, выполните следующую команду:*

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

Проверка зашифрованных соединений

Вы можете настраивать параметры проверки зашифрованных соединений, которые используются в задаче Защита от веб-угроз (см. раздел "Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)" на стр. 169).

Также вы можете настраивать список доверенных сертификатов (см. раздел "Управление доверенными сертификатами" на стр. 107), который используется при проверке зашифрованных соединений.

В этом разделе

Параметры проверки зашифрованных соединений

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

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

Таблица 10. Параметры проверки зашифрованных соединений

Параметр	Описание	Значения
EncryptedConnectionsScan	Включает или выключает проверку зашифрованного трафика. Для FTP-протокола проверка зашифрованных соединений выключена по умолчанию.	Yes (значение по умолчанию) – включить проверку зашифрованных соединений. No – выключить проверку зашифрованных соединений. Программа не расшифровывает зашифрованный трафик.
EncryptedConnectionsScanErrorAction	Действие, выполняемое программой при возникновении ошибки проверки зашифрованных соединений на веб-сайте.	AddToAutoExclusions (значение по умолчанию) – добавить домен, на котором возникла ошибка, в список доменов с ошибками проверки. Программа не будет контролировать зашифрованный сетевой трафик при посещении этого домена. Disconnect – заблокировать сетевое соединение.
CertificateVerificationPolicy	Задает способ проверки сертификатов программой Kaspersky Endpoint Security. Если сертификат является самозаверяющим, программа не выполняет дополнительную проверку.	FullCheck (значение по умолчанию) – программа использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата. LocalCheck – программа не использует интернет для проверки сертификата.
UntrustedCertificateAction	Действие, выполняемое программой при возникновении ошибки проверки зашифрованных соединений на веб-сайте.	Allow (значение по умолчанию) – разрешить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом. Block – запретить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом.
ManageExclusions	Включает или выключает использование исключений при проверке зашифрованного трафика.	Yes – не проверять веб-сайты, указанные в разделе [Exclusions.item_#]. No (значение по умолчанию) – проверять все веб-сайты.
MonitorNetworkPorts	Способ контроля сетевых портов программой Kaspersky Endpoint Security.	Selected (значение по умолчанию) – контролировать только сетевые порты, указанные в разделе [NetworkPorts.item_#] (см. ниже). All – контролировать все сетевые порты. Выбор этого значения может значительно увеличить нагрузку на операционную систему.

Параметр	Описание	Значения
Секция **[Exclusions.item_#]** содержит домены, исключенные из проверки. Программа не проверяет зашифрованные соединения, установленные при посещении указанных доменов.		
`DomainName`	Имя домена. Для указания домена можно использовать маски.	Значение по умолчанию не задано.
Секция **[NetworkPorts.item_#]** содержит сетевые порты, контролируемые программой.		
`PortName`	Описание сетевого порта.	Значение по умолчанию не задано.
`Port`	Номера сетевых портов, контролируемые программой.	`1` – `65535` Значение по умолчанию не задано.

Управление параметрами проверки зашифрованных соединений

Вы можете управлять параметрами проверки зашифрованных соединений из командной строки.

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

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

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

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

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

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

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

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

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

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

  Выходной файл имеет формат INI.

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

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

kaspersky

Управление доверенными сертификатами

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

Вы можете управлять списком доверенных сертификатов из командной строки.

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

```
kesl-control [-N] --add-certificate <путь к сертификату>
```

где:

`<путь к сертификату>` – путь к файлу сертификата, который вы хотите добавить, в формате PEM или DER.

► *Чтобы удалить сертификат из списка доверенных сертификатов, выполните следующую команду:*

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

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

```
kesl-control [-N] --list-certificates
```

Для каждого сертификата отображается следующая информация:

- субъект сертификата;
- серийный номер;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- отпечаток сертификата SHA-256.

kaspersky

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

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

Во время работы задачи Защита от файловых угроз программа выполняет проверку всех пространств имен во всех поддерживаемых операционных системах, если в общих параметрах программы для параметра `NamespaceMonitoring` задано значение `Yes`.

Дополнительно для операционной системы Astra Linux пользовательская задача антивирусной проверки (Scan_File) позволяет проверять файлы из других пространств имен (в рамках обязательной проверки).

Для запуска и остановки задачи Защита от файловых угроз из командной строки требуются права роли Администратор (см. раздел "Разделение доступа к функциям программы по пользовательским ролям" на стр. 66).

Вы не можете создавать пользовательские задачи Защита от файловых угроз. Вы можете изменить параметры задачи Защита от файловых угроз (см. стр. 109), созданной по умолчанию.

Значения параметров задачи Защита от файловых угроз содержатся в конфигурационном файле (см. раздел "Конфигурационный файл задачи Защита от файловых угроз" на стр. 396).

В этом разделе

Особенности проверки символических и жестких ссылок

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

Проверка символических ссылок

Программа проверяет символические ссылки, только если файл, на который ссылается символическая ссылка, входит в область защиты задачи Защита от файловых угроз.

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

Проверка жестких ссылок

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

- Если выбрано действие **Выполнять рекомендуемое действие** (Perform recommended action), программа 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), программа удаляет обрабатываемую жесткую ссылку. Остальные жесткие ссылки на этот файл обработаны не будут.
- Если выбрано действие **Лечить** (Disinfect), программа 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, программа создает копию исходного файла с именем жесткой ссылки, которая была помещена в хранилище. Связи с остальными жесткими ссылками на исходный файл восстановлены не будут.

Параметры задачи Защита от файловых угроз

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Защита от файловых угроз.

Таблица 11. Параметры задачи Защита от файловых угроз

Параметр	Описание	Значения
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2; .tbz; .tbz2; .gz; .tgz; .arj.	`Yes` – проверять архивы. Если указано значение `FirstAction=Recommended`, то в зависимости от типа архива программа удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` (значение по умолчанию) – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` – проверять самораспаковывающиеся архивы. `No` (значение по умолчанию) – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook®, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронной почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.

Параметр	Описание	Значения
SkipPlainTextFiles	Временное исключение из проверки файлов в текстовом формате. Если значение этого параметра SkipPlainTextFiles=Yes, программа не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течении 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов работы программ.	Yes – не проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течении 10 минут после последней проверки. No (значение по умолчанию) – проверять файлы в текстовом формате.
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, программа пропускает объект при проверке.	0 – 999,999 0 – программа проверяет объекты любого размера. Значение по умолчанию: 0.
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Программа прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 60.

Параметр	Описание	Значения
FirstAction	Выбор первого действия, которое программа будет выполнять 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.	Disinfect (лечить) – программа пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), программа оставляет объект неизменным. Если первым действием выбрано Disinfect, рекомендуется задать второе действие в параметре SecondAction. Remove (удалять) – программа удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – программа 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) – программа блокирует доступ к зараженному объекту. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Recommended.
SecondAction	Выбор второго действия, которое программа будет выполнять над зараженными объектами. Программа 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, программа в качестве второго действия выполняет Block (блокировать). Значение по умолчанию: Block.
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.

Параметр	Описание	Значения

ExcludeMasks	Исключение из проверки объектов по именам или маскам.
	С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.
		Значение по умолчанию не задано.
		Пример:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром ExcludeThreats.	Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats. No (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.

ExcludeThreats	Исключение из проверки объектов 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 программы о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа 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 программы. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.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`

Параметр	Описание	Значения
ReportCleanObjects	Включение записи в журнал информации о проверенных объектах, которые программа признала незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой.	Yes – записывать в журнал информацию о незараженных объектах. No (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен программой.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
ReportUnprocessed Objects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет программе распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор. No – выключить эвристический анализатор.
HeuristicLevel	Уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная загрузка системы. Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. Deep – наиболее тщательная проверка, максимальная загрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.
UseIChecker	Включение использования технологии iChecker.	Yes (значение по умолчанию) – включить использование технологии iChecker. No – выключить использование технологии iChecker.

Параметр	Описание	Значения
ScanByAccessType	Режим работы задачи Защита от файловых угроз. Этот параметр ScanByAccessType применяется только в задаче Защита от файловых угроз.	SmartCheck (значение по умолчанию) – проверять файл при попытке открытия, и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс во время своей работы многократно обращается к файлу в течение некоторого времени и изменяет его, повторно проверять файл только при последней попытке закрытия файла этим процессом. OpenAndModify – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Open – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
AreaDesc	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects. **Пример:** AreaDesc="Проверка почтовых баз"
UseScanArea	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	Yes (значение по умолчанию) – проверять указанную область. No – не проверять указанную область.
AreaMask	Ограничение области проверки. В области проверки программа проверяет только файлы, указанные помощью масок в формате shell. Если параметр не указан, программа проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты). **Пример:** AreaMask_<номер элемента>=*doc

Параметр	Описание	Значения
Path	Путь к директории с проверяемыми объектами.	<путь к локальной директории> – проверять объекты в указанной директории. Для указания пути можно использовать маски. 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 Samba. Mounted:NFS – проверять удаленные директории, смонтированные на компьютере по протоколу NFS. Mounted:SMB – проверять удаленные директории, смонтированные на компьютере по протоколу Samba. AllRemoteMounted – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов Samba и NFS. AllShared – проверять все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам Samba и NFS. <тип файловой системы> – проверять все ресурсы указанной файловой системы компьютера.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры:		
AreaDesc	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.
AreaMask	Ограничение области исключения из проверки. В области исключения программа не проверяет только файлы, указанные с помощью масок в формате shell.	Значение по умолчанию: * (исключать из проверки все объекты). Если параметр не указан, программа исключает из проверки все объекты в области исключения. Вы можете указать несколько значений этого параметра.

Параметр	Описание	Значения
Path	Путь к директории с исключаемыми объектами.	<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. Mounted:NFS – исключать из проверки удаленные директории, смонтированные на компьютере по протоколу NFS. Mounted:SMB – исключать из проверки удаленные директории, смонтированные на компьютере по протоколу Samba. AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов Samba и NFS. AllShared – исключать из проверки все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам Samba и NFS. <тип файловой системы> – исключать из проверки все ресурсы указанной файловой системы компьютера.
Секция **[ExcludedForProgram.item_#]** содержит следующие параметры:		
ProgramPath	Путь к исключаемому процессу.	<полный путь к процессу> – исключать из проверки процесс в указанной локальной директории.
ApplyToDescendants	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром ProgramPath.	Yes – исключать из проверки указанный процесс и все его дочерние процессы. No (значение по умолчанию) – исключать из проверки только указанный процесс, не исключать из проверки дочерние процессы.
AreaDesc	Описание области исключения процессов.	Значение по умолчанию: All objects.
UseExcludedForProgram	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.

Параметр	Описание	Значения
AreaMask	Ограничение области исключения процессов. В области исключения процессов программа не проверяет только файлы, указанные помощью масок в формате shell.	Значение по умолчанию: * (исключать из проверки все объекты). Если параметр не указан, программа исключает из проверки все объекты в области исключения процессов. Вы можете указать несколько значений этого параметра.
Path	Путь к директории с файлами, которые изменяет процесс.	<путь к локальной директории> – исключать из проверки объекты в указанной директории. Для указания пути можно использовать маски. Shared:NFS – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS. Shared:SMB – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу Samba. Mounted:NFS – исключать из проверки удаленные директории, смонтированные на компьютере по протоколу NFS. Mounted:SMB – исключать из проверки удаленные директории, смонтированные на компьютере по протоколу Samba. AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов Samba и NFS. AllShared – исключать из проверки все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам Samba и NFS. <тип файловой системы> – исключать из проверки все ресурсы указанной файловой системы компьютера.

Формирование глобальной области исключения

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

► *Чтобы создать глобальную область исключения:*

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

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

2. Добавьте в созданный файл секцию `[ExcludedFromScanScope.item_#]`. Секция `[ExcludedFromScanScope.item_#]` содержит следующие параметры:
   - `AreaDesc` – описание области исключения, содержащее дополнительную информацию об области исключения.
   - `Path` – путь к файлам или директориям, которые вы хотите исключить из области защиты.
   - `AreaMask` – маска имени файла для файлов, которые вы хотите исключить из области защиты.

   Пример:

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

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

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

Вы также можете управлять областями исключения из командной строки (см. раздел "Управление областями исключения из командной строки" на стр. 103).

Оптимизация проверки сетевых директорий

Для оптимизации работы задачи Защита от файловых угроз вы можете настроить исключение из проверки файлов, копируемых из сетевых директорий. Файлы будут проверяться только после завершения копирования в локальную директорию. Для исключения из проверки файлов в сетевых директориях вам нужно настроить исключение из проверки для утилиты, предназначенной для копирования из сетевых директорий (например, для утилиты `cp`).

► *Чтобы настроить исключение сетевых директорий из проверки:*

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

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

2. Добавьте в созданный файл секцию `[ExcludedForProgram.item_#]`. Секция `[ExcludedFromScanScope.item_#]` содержит следующие параметры:
   - `ProgramPath` – путь к исключаемому процессу или к директории с исключаемыми процессам.
   - `AreaDesc` – описание области исключения по процессам, содержащее дополнительную информацию об области исключения.

- `Path` – путь к файлам или к директории с файлами, которые изменяет процесс.
- `AreaMask` – маска имени файла для файлов, которые вы хотите исключить из проверки. Вы также можете указать полный путь к файлу.

Пример:

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/cp
ApplyToDescendants=No
AreaDesc=
UseExcludedForProgram=Yes
Path=AllRemoteMounted
AreaMask.item_0000=*
```

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

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

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

kaspersky

Задача Антивирусная проверка (Scan_My_Computer, ID:2)

Этот раздел содержит информацию о задаче Антивирусная проверка.

В этом разделе

О задаче Антивирусная проверка

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

По умолчанию в программе создается предустановленная задача антивирусной проверки – *полная проверка*. При полной проверке программа проверяет все объекты, расположенные на локальных дисках компьютера, а также все смонтированные и общие объекты, доступ к которым предоставляется по протоколам Samba и NFS, с рекомендуемыми параметрами безопасности.

Вы можете создавать пользовательские задачи антивирусной проверки. По умолчанию в программе также создается предустановленная пользовательская задача антивирусной проверки.

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

Параметры задачи Антивирусная проверка

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

Таблица 12. Параметры задачи Антивирусная проверка

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` (значение по умолчанию) – проверять файлы. `No` – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` (значение по умолчанию) – проверять загрузочные секторы. `No` – не проверять загрузочные секторы.

Параметр	Описание	Значения
ScanComputerMemory	Включение проверки памяти процессов и памяти ядра.	Yes (значение по умолчанию) – проверять память процессов и память ядра. No – не проверять память процессов и память ядра.
ScanStartupObjects	Включение проверки объектов автозапуска.	Yes (значение по умолчанию) – проверять объекты автозапуска. No – не проверять объекты автозапуска.
ScanArchived	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2; .tbz; .tbz2; .gz; .tgz; .arj.	Yes (значение по умолчанию) – проверять архивы. Если указано значение FirstAction=Recommended, то в зависимости от типа архива программа удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. No – не проверять архивы.
ScanSfxArchived	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	Yes (значение по умолчанию) – проверять самораспаковывающиеся архивы. No – не проверять самораспаковывающиеся архивы.
ScanMailBases	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	Yes – проверять файлы почтовых баз. No (значение по умолчанию) – не проверять файлы почтовых баз.
ScanPlainMail	Включение проверки сообщений электронной почты в текстовом формате (plain text).	Yes – проверять сообщения электронной почты в текстовом формате. No (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
ScanPriority	Приоритет задачи. Приоритет задачи – это параметр, сочетающий несколько внутренних параметров программы Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.	Idle – запустить задачу с низким приоритетом: не более 10% потребления ресурсов процессора. Выберите это значение, если вы хотите выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени. Normal (значение по умолчанию) – запустить задачу со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. High – запустить задачу с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.

Параметр	Описание	Значения
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, программа пропускает объект при проверке.	0 – 999,999 0 – программа проверяет объекты любого размера. Значение по умолчанию: 0.
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Программа прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
FirstAction	Выбор первого действия, которое программа будет выполнять над зараженными объектами. Если зараженный объект обнаружен в файле, обращение к которому происходит по символической ссылке, входящей в область проверки (в то время как сам файл, обращение к которому происходит по символической ссылке, не входит в область проверки), над этим файлом будет выполнено указанное действие. Например, если выбрано действие Remove (удалять), программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.	Disinfect (лечить) – программа пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), программа оставляет объект неизменным. Если первым действием выбрано Disinfect, рекомендуется задать второе действие в параметре SecondAction. Remove (удалять) – программа удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – программа 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) – программа не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Recommended.

Параметр	Описание	Значения
SecondAction	Выбор второго действия, которое программа будет выполнять над зараженными объектами. Программа 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, программа в качестве второго действия выполняет Skip (пропускать). Значение по умолчанию: Skip.
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.
ExcludeMasks	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр UseExcludeMasks.	Значение по умолчанию не задано. **Пример:** UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром ExcludeThreats.	Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats. No (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.

Параметр	Описание	Значения

ExcludeThreats	Исключение из проверки объектов 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 программы о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа 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 программы. Вы также можете найти полное название угрозы на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.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	Включение записи в журнал информации о проверенных объектах, которые программа признала незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой.	`Yes` – записывать в журнал информацию о незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.

Параметр	Описание	Значения
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен программой.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
ReportUnprocessed Objects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет программе распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор. No – выключить эвристический анализатор.
HeuristicLevel	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная загрузка системы. Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. Deep – наиболее тщательная проверка, максимальная загрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.
UseIChecker	Включение использования технологии iChecker.	Yes (значение по умолчанию) – включить использование технологии iChecker. No – выключить использование технологии iChecker.

Параметр	Описание	Значения
DeviceNameMasks.item_#	Список названий устройств, загрузочные секторы которых будет проверять программа. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску названия устройства.	AllObjects – проверять загрузочные секторы всех устройств. <маска названия устройства> – проверять загрузочные секторы устройств, названия которых содержат указанную маску. Значение по умолчанию: /** – любой набор символов в названии устройства, включая символ /.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
AreaDesc	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects. **Пример:** AreaDesc="Mail bases scan"
UseScanArea	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	Yes (значение по умолчанию) – проверять указанную область. No – не проверять указанную область.
AreaMask	Ограничение области проверки. В области проверки программа проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, программа проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты). **Пример:** AreaMask_<номер элемента>=*doc

Параметр	Описание	Значения
`Path`	Путь к директории с проверяемыми объектами.	`<путь к локальной директории>` – проверять объекты в указанной директории. `Shared:NFS` – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS. `Shared:SMB` – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу Samba. `Mounted:NFS` – проверять удаленные директории, смонтированные на компьютере по протоколу NFS. `Mounted:SMB` – проверять удаленные директории, смонтированные на компьютере по протоколу Samba. `AllRemoteMounted` – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов Samba и NFS. `AllShared` – проверять все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам Samba и NFS. `<тип файловой системы>` – проверять все ресурсы указанной файловой системы компьютера.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры.		
`AreaDesc`	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из проверки.	`Yes` (значение по умолчанию) – исключать указанную область. `No` – не исключать указанную область.
`AreaMask`	Ограничение области исключения из проверки. В области исключения программа исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, программа исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать все объекты).

Параметр	Описание	Значения
`Path`	Путь к директории с исключаемыми объектами.	`<путь к локальной директории>` – исключать из проверки объекты в указанной директории. Для указания пути можно использовать маски. В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида `/.snapshots/*/snapshot/`. `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. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на компьютере по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на компьютере по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов Samba и NFS. `AllShared` – исключать из проверки все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам Samba и NFS. `<тип файловой системы>` – исключать из проверки все ресурсы указанной файловой системы компьютера.

kaspersky

Задача Выборочная проверка (Scan_File, ID:3)

Этот раздел содержит информацию о задаче Выборочная проверка.

В этом разделе

О задаче Выборочная проверка

Если вы хотите проверить файл или директорию, вы можете запустить задачу Выборочная проверка. Программа создаст временную задачу антивирусной проверки (типа ODS) с параметрами задачи (см. раздел "Параметры задачи Выборочная проверка" на стр. 129) Scan_File. После завершения проверки временная задача автоматически удаляется.

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

► *Чтобы проверить файл или директорию, выполните следующую команду:*

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

Параметры задачи Выборочная проверка

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

Таблица 13. Параметры задачи Выборочная проверка

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` (значение по умолчанию) – проверять файлы. `No` – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` – проверять загрузочные секторы. `No` (значение по умолчанию) – не проверять загрузочные секторы.
`ScanComputerMemory`	Включение проверки памяти процессов и памяти ядра.	`Yes` – проверять память процессов и память ядра. `No` (значение по умолчанию) – не проверять память процессов и память ядра.

Параметр	Описание	Значения
ScanStartupObjects	Включение проверки объектов автозапуска.	Yes – проверять объекты автозапуска. No (значение по умолчанию) – не проверять объекты автозапуска.
ScanArchived	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2; .tbz; .tbz2; .gz; .tgz; .arj.	Yes (значение по умолчанию) – проверять архивы. Если указано значение FirstAction=Recommended, то в зависимости от типа архива программа удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. No – не проверять архивы.
ScanSfxArchived	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	Yes (значение по умолчанию) – проверять самораспаковывающиеся архивы. No – не проверять самораспаковывающиеся архивы.
ScanMailBases	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	Yes – проверять файлы почтовых баз. No (значение по умолчанию) – не проверять файлы почтовых баз.
ScanPlainMail	Включение проверки сообщений электронной почты в текстовом формате (plain text).	Yes – проверять сообщения электронной почты в текстовом формате. No (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
ScanPriority	Приоритет задачи. Приоритет задачи проверки – это параметр, сочетающий несколько внутренних параметров программы Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.	Idle – запустить задачу с низким приоритетом: не более 10% потребления ресурсов процессора. Выберите это значение, если вы хотите выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени. Normal – запустить задачу со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. High (значение по умолчанию) – запустить задачу с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.

Параметр	Описание	Значения
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, программа пропускает объект при проверке.	0 – 999,999 0 – программа проверяет объекты любого размера. Значение по умолчанию: 0.
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Программа прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
FirstAction	Выбор первого действия, которое программа будет выполнять над зараженными объектами. Если зараженный объект обнаружен в файле, обращение к которому происходит по символической ссылке, входящей в область проверки (в то время как сам файл, обращение к которому происходит по символической ссылке, не входит в область проверки), над этим файлом будет выполнено указанное действие. Например, если выбрано действие Remove (удалять), программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.	Disinfect (лечить) – программа пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), программа оставляет объект неизменным. Если первым действием выбрано Disinfect, рекомендуется задать второе действие в параметре SecondAction. Remove (удалять) – программа удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – программа 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) – программа не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Recommended.

Параметр	Описание	Значения
SecondAction	Выбор второго действия, которое программа будет выполнять над зараженными объектами. Программа 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, программа в качестве второго действия выполняет Skip (пропускать). Значение по умолчанию: Skip.
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.
ExcludeMasks	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.	Значение по умолчанию не задано. **Пример:** UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром ExcludeThreats.	Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats. No (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.

Параметр	Описание	Значения

ExcludeThreats	Исключение из проверки объектов 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 программы о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа 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 программы. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.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	Включение записи в журнал информации о проверенных объектах, которые программа признала незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой.	Yes – записывать в журнал информацию о незараженных объектах. No (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.

Параметр	Описание	Значения
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен программой.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
ReportUnprocessed Objects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет программе распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор. No – выключить эвристический анализатор.
HeuristicLevel	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная загрузка системы. Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. Deep – наиболее тщательная проверка, максимальная загрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.
UseIChecker	Включение использования технологии iChecker.	Yes (значение по умолчанию) – включить использование технологии iChecker. No – выключить использование технологии iChecker.

Параметр	Описание	Значения
DeviceNameMasks.item_#	Список названий устройств, загрузочные секторы которых будет проверять программа. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску названия устройства.	AllObjects – проверять загрузочные секторы всех устройств. <маска названия устройства> – проверять загрузочные секторы устройств, названия которых содержат указанную маску. Значение по умолчанию: /** – любой набор символов в названии устройства, включая символ /.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
AreaDesc	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects. **Пример:** AreaDesc="Проверка почтовых баз"
UseScanArea	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	Yes (значение по умолчанию) – проверять указанную область. No – не проверять указанную область.
AreaMask	Ограничение области проверки. В области проверки программа проверяет только файлы, указанные с помощью масок в формате shell.	Значение по умолчанию: * (проверять все объекты). **Пример:** AreaMask_<номер элемента>=*doc Если параметр не указан, программа проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.

Параметр	Описание	Значения
Path	Путь к директории с проверяемыми объектами.	<путь к локальной директории> – проверять объекты в указанной директории. Shared:NFS – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS. Shared:SMB – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу Samba. Mounted:NFS – проверять удаленные директории, смонтированные на компьютере по протоколу NFS. Mounted:SMB – проверять удаленные директории, смонтированные на компьютере по протоколу Samba. AllRemoteMounted – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов Samba и NFS. AllShared – проверять все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам Samba и NFS. <тип файловой системы> – проверять все ресурсы указанной файловой системы компьютера.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры:		
AreaDesc	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.
AreaMask	Ограничение области исключения из проверки. В области исключения программа исключает только файлы, указанные с помощью масок в формате shell.	Значение по умолчанию: * (исключать все объекты). Если параметр не указан, программа исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.

Параметр	Описание	Значения
`Path`	Путь к директории с исключаемыми объектами.	`<путь к локальной директории>` – исключать из проверки объекты в указанной директории. Для указания пути можно использовать маски. В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида `/.snapshots/*/snapshot/`. `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. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на компьютере по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на компьютере по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов Samba и NFS. `AllShared` – исключать из проверки все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам Samba и NFS. `<тип файловой системы>` – исключать из проверки все ресурсы указанной файловой системы компьютера.

kaspersky

Задача Проверка важных областей (Critical_Areas_Scan, ID:4)

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

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

Таблица 14. Параметры задачи Проверка важных областей

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` – проверять файлы. `No` (значение по умолчанию) – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` (значение по умолчанию) – проверять загрузочные секторы. `No` – не проверять загрузочные секторы.
`ScanComputerMemory`	Включение проверки памяти процессов и памяти ядра.	`Yes` (значение по умолчанию) – проверять память процессов и память ядра. `No` – не проверять память процессов и память ядра.
`ScanStartupObjects`	Включение проверки объектов автозапуска.	`Yes` (значение по умолчанию) – проверять объекты автозапуска. `No` – не проверять объекты автозапуска.
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2; .tbz; .tbz2; .gz; .tgz; .arj.	`Yes` (значение по умолчанию) – проверять архивы. Если указано значение `FirstAction=Recommended`, то в зависимости от типа архива программа удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (значение по умолчанию) – проверять самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.

Параметр	Описание	Значения
ScanPlainMail	Включение проверки сообщений электронной почты в текстовом формате (plain text).	Yes – проверять сообщения электронной почты в текстовом формате. No (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
ScanPriority	Приоритет задачи. Приоритет задачи – это параметр, сочетающий несколько внутренних параметров программы Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.	Idle – запустить задачу с низким приоритетом: не более 10% потребления ресурсов процессора. Выберите это значение, если вы хотите выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени. Normal (значение по умолчанию) – запустить задачу со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. High – запустить задачу с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, программа пропускает объект при проверке.	0 – 999,999 0 – программа проверяет объекты любого размера. Значение по умолчанию: 0.
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Программа прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.

Параметр	Описание	Значения
FirstAction	Выбор первого действия, которое программа будет выполнять над зараженными объектами. Если зараженный объект обнаружен в файле, обращение к которому происходит по символической ссылке, входящей в область проверки (в то время как сам файл, обращение к которому происходит по символической ссылке, не входит в область проверки), над этим файлом будет выполнено указанное действие. Например, если выбрано действие Remove (удалять), программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.	Disinfect (лечить) – программа пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), программа оставляет объект неизменным. Если первым действием выбрано Disinfect, рекомендуется задать второе действие в параметре SecondAction. Remove (удалять) – программа удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – программа 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) – программа не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Recommended.
SecondAction	Выбор второго действия, которое программа будет выполнять над зараженными объектами. Программа 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, программа в качестве второго действия выполняет Skip (пропускать). Значение по умолчанию: Skip.
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.

Параметр	Описание	Значения
ExcludeMasks	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр UseExcludeMasks.	Значение по умолчанию не задано. **Пример:** UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром ExcludeThreats.	Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats. No (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.
ExcludeThreats	Исключение из проверки объектов 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 программы о том, что объект является зараженным. Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа 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 программы. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.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

Параметр	Описание	Значения
ReportCleanObjects	Включение записи в журнал информации о проверенных объектах, которые программа признала незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой.	Yes – записывать в журнал информацию о незараженных объектах. No (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен программой.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
ReportUnprocessed Objects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет программе распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор. No – выключить эвристический анализатор.
HeuristicLevel	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная загрузка системы. Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. Deep – наиболее тщательная проверка, максимальная загрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.

Параметр	Описание	Значения
UseIChecker	Включение использования технологии iChecker.	Yes (значение по умолчанию) – включить использование технологии iChecker. No – выключить использование технологии iChecker.
DeviceNameMasks.item_#	Список названий устройств, загрузочные секторы которых будет проверять программа. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску названия устройства.	AllObjects – проверять загрузочные секторы всех устройств. <маска имени устройства> – проверять загрузочные секторы устройств, названия которых содержат указанную маску. Значение по умолчанию: /** – любой набор символов в названии устройства, включая символ /.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
AreaDesc	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects. **Пример:** AreaDesc="Mail bases scan"
UseScanArea	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	Yes (значение по умолчанию) – проверять указанную область. No – не проверять указанную область.
AreaMask	Ограничение области проверки. В области проверки программа проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, программа проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты). **Пример:** AreaMask_<номер элемента>=*doc

Параметр	Описание	Значения
Path	Путь к директории с проверяемыми объектами.	<путь к локальной директории> – проверять объекты в указанной директории. Shared:NFS – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS. Shared:SMB – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу Samba. Mounted:NFS – проверять удаленные директории, смонтированные на компьютере по протоколу NFS. Mounted:SMB – проверять удаленные директории, смонтированные на компьютере по протоколу Samba. AllRemoteMounted – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов Samba и NFS. AllShared – проверять все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам Samba и NFS. <тип файловой системы> – проверять все ресурсы указанной файловой системы компьютера.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры:		
AreaDesc	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.
AreaMask	Ограничение области исключения из проверки. В области исключения программа исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, программа исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (исключать все объекты).

Параметр	Описание	Значения
`Path`	Путь к директории с исключаемыми объектами.	`<путь к локальной директории>` – исключать из проверки объекты в указанной директории. Для указания пути можно использовать маски. В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида `/.snapshots/*/snapshot/`. `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. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на компьютере по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на компьютере по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов Samba и NFS. `AllShared` – исключать из проверки все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам Samba и NFS. `<тип файловой системы>` – исключать из проверки все ресурсы указанной файловой системы компьютера.

kaspersky

Задача Обновление (Update, ID:6)

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 программы. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули программы.

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

Основным источником обновлений (см. раздел "Об источниках обновлений" на стр. 147) программы 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. Загрузка пакета обновлений выполняется с помощью задачи Обновление.

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

Если загрузка обновлений баз прерывается или завершается с ошибкой, программа продолжает использовать предыдущую установленную версию баз. Если ранее базы программы не устанавливались, программа продолжает 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* (*BasesAreOutOfDate*), если последние установленные обновления баз были опубликованы на сервере "Лаборатории Касперского" более трех, но менее семи дней назад. Если базы не обновляются в течение семи дней, программа записывает в журнал событие *Базы сильно устарели* (*BasesAreTotallyOutOfDate*). Базы актуальны, если они были загружены менее трех дней назад.

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

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт). Объем занимаемого дискового пространства может достигать 3 ГБ.

kaspersky

В этом разделе

Об источниках обновлений

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

В предустановленной задаче Обновление в качестве источника обновлений по умолчанию выбраны серверы обновлений "Лаборатории Касперского". На серверы обновлений выкладываются обновления баз и программных модулей для многих 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 локальной или сетевой директории (SMB/NFS), смонтированной пользователем, а также с FTP-, HTTP или HTTPS-сервера. Вы можете указать пользовательский источник обновлений в параметрах задачи Обновление (см. раздел "Параметры задачи Обновление" на стр. 147).

Параметры задачи Обновление

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

Таблица 15. Параметры задачи Обновление

Параметр	Описание	Значения
`SourceType`	Источник (см. раздел "Об источниках обновлений" на стр. 147), из которого программа будет получать обновления.	`KLServers` (значение по умолчанию) – программа получает обновления с одного из серверов обновлений "Лаборатории Касперского". Обновления загружаются по протоколу HTTPS. `SCServer` – программа загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. `Custom` – программа загружает обновления из пользовательского источника, указанного в секции `[CustomSources.item_#]`. Вы можете указывать директории FTP-, HTTP- и HTTPS-серверов или директории на любом смонтированном устройстве защищаемого компьютера, включая директории на удаленных компьютерах, смонтированные по протоколам Samba или NFS.

Параметр	Описание	Значения
UseKLServersWhenUnavailable	Обращение программы к серверам обновлений "Лаборатории Касперского" в случае, если все пользовательские источники недоступны.	Yes (значение по умолчанию) – программа подключается к серверам обновлений "Лаборатории Касперского", если все пользовательские источники обновлений недоступны. No – программа не подключается к серверам обновлений "Лаборатории Касперского", если все пользовательские источники обновлений недоступны.
ApplicationUpdateMode	Режим загрузки и установки обновлений программы.	Disabled (значение по умолчанию) – не загружать и не устанавливать обновления программы. DownloadOnly – загружать обновления программы, но не устанавливать их. DownloadAndInstall – автоматически загружать и устанавливать обновления программы. Для сохранения сертифицированной конфигурации программы требуется установить значение параметра ApplicationUpdateMode=Disabled.
ConnectionTimeout	Время ожидания (в секундах) ответа от источника обновлений – HTTP-сервера – при попытке соединения с ним. Если в течение указанного промежутка времени от источника обновлений не приходит ответ, программа обращается к другому указанному источнику обновлений.	Вы можете указывать только целые числа в диапазоне от 0 до 120. Значение по умолчанию: 10.
Секция **[CustomSources.item_#]** содержит следующие параметры:		
URL	Адрес пользовательского источника обновлений в локальной сети или в интернете.	Значение по умолчанию не задано. **Примеры:** URL=http://example.com/bases/ – адрес HTTP-сервера, на котором расположена директория с обновлениями. URL=/home/bases/ – директория на защищаемом компьютере, в которой содержатся базы программы.

Параметр	Описание	Значения
`Enabled`	Включение использования источника обновлений, указанного в параметре `URL`. Для выполнения задачи требуется включить использование хотя бы одного источника обновлений.	`Yes` – Kaspersky Endpoint Security использует источник обновлений. `No` – Kaspersky Endpoint Security не использует источник обновлений. Значение по умолчанию не задано.

Установка обновления модулей программы вручную

Вы можете вручную установить обновления модулей программы из командной строки. Для установки обновлений на вашем компьютере должна быть установлена программа Kaspersky Endpoint Security. Для обновления программы Kaspersky Endpoint Security требуется остановить ее работу. Если процесс обновления завершается с ошибкой, программа автоматически откатывает обновления до предыдущей версии.

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

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

Задача Откат обновления баз (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 программой Kaspersky Endpoint Security.

Задача Откат обновления баз не имеет параметров.

kaspersky

Задача Лицензирование (License, ID:9)

Задача Лицензирование позволяет управлять лицензионными ключами программы Kaspersky Endpoint Security.

В этом разделе

Добавление активного ключа

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

Синтаксис команды

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

Аргументы и ключи

`<путь к файлу ключа>` – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

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

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

Добавление резервного ключа

Команда `kesl-control --add-reserve-key` добавляет резервный ключ.

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

Синтаксис команды

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

Аргументы и ключи

`<путь к файлу ключа>` – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

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

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

Удаление активного ключа

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

Синтаксис команды

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

Удаление резервного ключа

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

Синтаксис команды

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

kaspersky

Задача Управление Хранилищем (Backup, ID:10)

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

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

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, пользователь может попытаться восстановить файл (см. раздел "Восстановление объектов из Хранилища" на стр. 154) из его вылеченной копии в директорию исходного размещения файла.

В этом разделе

Параметры задачи Управление Хранилищем

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

Таблица 16. Параметры задачи Управление Хранилищем

Параметр	Описание	Значение
`DaysToLive`	Интервал времени, в течение которого объекты хранятся в Хранилище (в сутках). Чтобы снять ограничение для времени хранения объектов в Хранилище, укажите значение `0`.	`0` – время хранения объектов в Хранилище не ограничено. Значение по умолчанию: `90`.
`BackupSizeLimit`	Максимальный размер Хранилища (в мегабайтах). При достижении максимального размера Хранилища, программа удаляет самые старые объекты. Чтобы снять ограничение для размера Хранилища, укажите значение `0`.	`0 - 999,999` `0` – размер Хранилища не ограничен. Значение по умолчанию: `0`.

Параметр	Описание	Значение
`BackupFolder`	Путь к директории Хранилища. Вы можете указать в качестве Хранилища пользовательскую директорию, отличную от директории, заданной по умолчанию. В качестве Хранилища можно использовать директории на любых устройствах. Не рекомендуется указывать директории, расположенные на удаленных компьютерах, например смонтированных по протоколам Samba и NFS. Kaspersky Endpoint Security начинает перемещать объекты в выбранную директорию после изменения параметров и перезапуска программы. Если указанной директории не существует или она недоступна, программа использует директорию, заданную по умолчанию.	Значение по умолчанию: /var/opt/kaspersky/kesl/common/objects-backup/ Для доступа к заданной по умолчанию директории Хранилища требуются root-права.

Просмотр идентификаторов объектов в Хранилище

Когда объект помещается в Хранилище, программа присваивает ему числовой идентификатор. Этот идентификатор используется для выполнения действий над объектом, таких как восстановление (см. раздел "Восстановление объектов из Хранилища" на стр. 154) или удаление объекта из Хранилища (см. раздел "Удаление объектов из Хранилища" на стр. 155).

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

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

Идентификатор объекта будет выведен в строке `ObjectId`.

Восстановление объектов из Хранилища

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

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

Восстановление зараженных объектов может привести к заражению компьютера.

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

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

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

  где `<ID объекта>` – это идентификатор объекта (см. раздел "Просмотр идентификаторов объектов в Хранилище" на стр. 154) в Хранилище.

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

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

Если указанной директории не существует, Kaspersky Endpoint Security создает ее.

Удаление объектов из Хранилища

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

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

  Пример:

  Чтобы удалить объект с ID=15:

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

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

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

  Пример:

  Чтобы удалить объекты, в названии которых или в пути к которым содержится "test":

  ```
  kesl-control -B --mass-remove --query "FileName like '%test%'"
  ```

- *Чтобы удалить все объекты из Хранилища, выполните одну из следующих команд:*

  ```
  kesl-control -B --mass-remove
  ```

  или

  ```
  kesl-control -B --mass-remove --query
  ```

kaspersky

Задача Контроль целостности системы (System_Integrity_Monitoring, ID:11)

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

Для использования задачи требуется лицензия, которая включает эту функцию.

Контроль целостности системы может выполняться в режиме реального времени при запуске задачи Контроль целостности системы при доступе (OAFIM) (см. стр. 156). Кроме того, вы можете создавать и запускать задачи Контроль целостности системы по требованию (ODFIM) (см. стр. 157).

Оба типа задачи отправляют уведомления об изменениях в списках контроля доступа к объектам. В случае задачи OAFIM в отчет не включаются данные о том, какие именно изменения внесены. В случае задачи ODFIM в отчет включаются данные об измененных атрибутах и перемещенных файлах и директориях.

В этом разделе

Контроль целостности системы при доступе (OAFIM)

Во время работы задачи OAFIM каждое изменение объекта определяется путем перехвата файловых операций в режиме реального времени. При изменении объекта программа 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. Программа отслеживает операции с конкретными файлами или в областях мониторинга, указанных в параметрах задачи.

Области мониторинга

Для задачи Контроль целостности системы требуется указать области мониторинга. Администратор может изменять области проверки и мониторинга в режиме реального времени. Если область мониторинга не указана, параметры задачи нельзя сохранить в конфигурационном файле. 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 из мониторинга.

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

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

При добавлении области мониторинга или области исключения программа не проверяет, существует ли такая директория.

Контролируемые параметры

Во время работы задачи Контроль целостности системы контролируется изменение следующих параметров:

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

Технологические ограничения операционной системы Linux не позволяют задаче Контроль целостности системы определять, какой администратор или процесс внес изменение в файл.

Контроль целостности системы по требованию (ODFIM)

В процессе выполнения задачи ODFIM изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.

Снимок состояния системы создается во время первого выполнения задачи ODFIM на компьютере. Вы можете создать несколько задач ODFIM. Для каждой задачи ODFIM создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы относится к области мониторинга. Если снимок состояния системы не соответствует области мониторинга, программа Kaspersky Endpoint Security создает событие о нарушении целостности системы. Снимок состояния системы содержит пути к контролируемым объектам и их метаданные. Снимок состояния системы может также содержать персональные данные.

Снимок состояния системы создается заново после завершения задачи ODFIM. Вы можете заново создать снимок для задачи с помощью параметра `RebuildBaseline` (см. раздел "Параметры задачи Контроль целостности системы по требованию" на стр. 159). Снимок состояния системы также создается при изменении параметров задачи, например, при добавлении новой области мониторинга. При следующем выполнении задачи снимок состояния системы формируется заново. Вы можете удалить снимок состояния системы, удалив соответствующую задачу ODFIM.

Задача ODFIM создает хранилище для снимков состояния системы на компьютере с установленным компонентом Контроль целостности системы. По умолчанию снимки состояния системы хранятся в базе

данных /var/opt/kaspersky/kesl/private/fim.db. Для доступа к базе данных, в которой хранятся снимки состояния системы, требуются root-права.

Параметры задачи Контроль целостности системы при доступе

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Контроль целостности системы при доступе.

Таблица 17. Параметры задачи Контроль целостности системы при доступе

Параметр	Описание	Значения
`UseExcludeMasks`	Включение исключения из области мониторинга объектов, указанными параметром `ExcludeThreats`. Этот параметр работает, только если указано значение параметра `ExcludeMasks`.	`Yes` – исключать объекты, указанные параметром `ExcludeMasks`, из области мониторинга. `No` (значение по умолчанию) – не исключать объекты, указанные параметром `ExcludeMasks`, из области мониторинга.
`ExcludeMasks`	Исключение из мониторинга объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`. 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.
Секция **[ScanScope.item_#]** содержит области мониторинга для задачи Контроль целостности системы. Для задачи должна быть указана минимум одна область мониторинга. Вы можете указать в конфигурационном файле несколько секций [ScanScope.item_#] в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области мониторинга, содержит дополнительную информацию об области мониторинга.	Значение по умолчанию не задано.
`UseScanArea`	Включение мониторинга указанной области.	`Yes` (значение по умолчанию) – контролировать указанную область. `No` – не контролировать указанную область.

Параметр	Описание	Значения
Path	Путь к директории для мониторинга.	Значение по умолчанию: /opt/kaspersky/kesl/
AreaMask.item_#	Ограничение области мониторинга. В области мониторинга программа проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (контролировать все объекты).
Секция **[ExcludedFromScanScope.item_#]** содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#]. Объекты, удовлетворяющие правилам любой из секций [ExcludedFromScanScope.item_#], будут исключены из мониторинга. Формат секции [ExcludedFromScanScope.item_#] аналогичен формату секции [ScanScope.item_#]. Вы можете указать в конфигурационном файле несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области исключения из мониторинга, содержит дополнительную информацию об области исключения из мониторинга.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из мониторинга.	Yes (значение по умолчанию) – исключать указанную область из мониторинга. No – не исключать указанную область из мониторинга.
Path	Путь к директории с объектами, исключаемыми из мониторинга. Для указания пути можно использовать маски.	Значение по умолчанию не задано.
AreaMask.item_#	Ограничение области исключения из мониторинга. В области исключения из мониторинга программа исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (исключать из мониторинга все объекты).

Параметры задачи Контроль целостности системы по требованию

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Контроль целостности системы по требованию.

Таблица 18. Параметры задачи Контроль целостности системы по требованию

Параметр	Описание	Значения
`RebuildBaseline`	Включение повторного создания снимка состояния системы после завершения задачи ODFIM.	`Yes` – создавать снимок состояния системы повторно после завершения задачи ODFIM. `No` (значение по умолчанию) – не создавать снимок состояния системы повторно после завершения задачи ODFIM.
`CheckFileHash`	Включение проверки хеша (SHA-256).	`Yes` – включить проверку хеша. `No` (значение по умолчанию) – выключить проверку хеша.
`TrackDirectoryChanges`	Включение мониторинга директорий.	`Yes` – контролировать директории. `No` (значение по умолчанию) – не контролировать директории.
`TrackLastAccessTime`	Включение проверки времени последнего доступа к файлу. В операционных системах Linux это параметр `noatime`.	`Yes` – проверять время последнего доступа к файлу. `No` (значение по умолчанию) – не проверять время последнего доступа к файлу.
`UseExcludeMasks`	Включение исключения из области мониторинга объектов, указанными параметром `ExcludeThreats`. Этот параметр работает, только если указано значение параметра `ExcludeMasks`.	`Yes` – исключать объекты, указанные параметром `ExcludeMasks`, из области мониторинга. `No` (значение по умолчанию) – не исключать объекты, указанные параметром `ExcludeMasks`, из области мониторинга.
`ExcludeMasks`	Исключение из мониторинга объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`. 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.

Параметр	Описание	Значения
Секция **[ScanScope.item_#]** содержит области мониторинга для задачи Контроль целостности системы. Для задачи должна быть указана минимум одна область мониторинга. Вы можете указать в конфигурационном файле несколько секций [ScanScope.item_#] в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области мониторинга, содержит дополнительную информацию об области мониторинга.	Значение по умолчанию не задано.
`UseScanArea`	Включение мониторинга указанной области.	`Yes` (значение по умолчанию) – контролировать указанную область. `No` – не контролировать указанную область.
`Path`	Путь к директории для мониторинга.	Значение по умолчанию: `/opt/kaspersky/kesl/`
`AreaMask.item_#`	Ограничение области мониторинга. В области мониторинга программа проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (контролировать все объекты).
Секция **[ExcludedFromScanScope.item_#]** содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#]. Объекты, удовлетворяющие правилам любой из секций [ExcludedFromScanScope.item_#], будут исключены из мониторинга. Формат секции [ExcludedFromScanScope.item_#] аналогичен формату секции [ScanScope.item_#]. Вы можете указать в конфигурационном файле несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области исключения из мониторинга, содержит дополнительную информацию об области исключения из мониторинга.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из мониторинга.	`Yes` (значение по умолчанию) – исключать указанную область из мониторинга. `No` – не исключать указанную область из мониторинга.
`Path`	Путь к директории с объектами, исключаемыми из мониторинга. Для указания пути можно использовать маски.	Значение по умолчанию не задано.

Параметр	Описание	Значения
`AreaMask.item_#`	Ограничение области исключения из мониторинга. В области исключения из мониторинга программа исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (исключать из мониторинга все объекты).

kaspersky

Задача Защита от шифрования (Anti_Cryptor, ID:13)

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

В процессе выполнения задачи Защита от шифрования Kaspersky Endpoint Security проверяет обращения удаленных компьютеров сети к файлам, расположенным в общих сетевых директориях защищаемого устройства. Если программа расценивает действия удаленного компьютера, получающего доступ к общим сетевым ресурсам, как вредоносное шифрование, она добавляет этот компьютер в список недоверенных устройств и запрещает ему доступ к общим сетевым директориям. По умолчанию Kaspersky Endpoint Security блокирует доступ недоверенных устройств к сетевым файловым ресурсам на 30 минут. Kaspersky Endpoint Security не расценивает действия как шифрование, если активность шифрования обнаружена в директориях, исключенных из области защиты (см. раздел "Параметры задачи Защита от шифрования" на стр. 164) задачи Защита от шифрования.

Для использования задачи требуется лицензия, которая включает эту функцию.

Для корректной работы задачи Защита от шифрования требуется, чтобы в операционной системе была установлена хотя бы одна из служб: Samba или NFS. Для службы NFS требуется установленный пакет rpcbind.

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

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

В этом разделе

О блокировке доступа к недоверенным компьютерам

При обнаружении вредоносного шифрования программа создает и включает правило для сетевого экрана операционной системы, которое блокирует сетевой трафик от скомпрометированного компьютера. Скомпрометированный компьютер добавляется в список недоверенных компьютеров. Программа 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 сетевого экрана, созданные задачей Защита от шифрования, нельзя удалить с помощью утилиты iptables, так как программа восстанавливает набор правил каждую минуту. Используйте команду `--allow-hosts` (см. раздел "Разблокировка заблокированных компьютеров" на стр. 167), чтобы разблокировать компьютер.

По умолчанию программа 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 будут автоматически разблокированы.

Параметры задачи Защита от шифрования

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

Таблица 19. Параметры задачи Защита от шифрования

Параметр	Описание	Значения
`UseHostBlocker`	Включение блокировки недоверенных компьютеров. Если блокировка недоверенных компьютеров выключена, программа все равно проверяет действия удаленных компьютеров с сетевыми файловыми ресурсами на наличие вредоносного шифрования, когда работает задача Защита от шифрования. В случае обнаружения вредоносного шифрования создается событие `EncryptionDetected`, но атакующий компьютер не блокируется.	`Yes` (значение по умолчанию) – включить блокировку недоверенных компьютеров. `No` – выключить блокировку недоверенных компьютеров.
`BlockTime`	Длительность блокировки доступа к недоверенному компьютеру в минутах. Изменение параметра `BlockTime` не влияет на длительность блокировки ранее заблокированных скомпрометированных компьютеров. Длительность блокировки не является динамическим значением и рассчитывается на момент блокировки.	Целое значение от `1` до `4294967295`. Значение по умолчанию: `30`.

Параметр	Описание	Значения
UseExcludeMasks	Включение исключения из области защиты объектов, указанных параметром ExcludeMasks. Этот параметр работает, только если указано значение параметра ExcludeMasks.	Yes – исключать объекты, указанные параметром ExcludeMasks, из области защиты. No (значение по умолчанию) – не исключать объекты, указанные параметром ExcludeMasks, из области защиты.
ExcludeMasks	Исключение из области защиты объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области защиты отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр UseExcludeMasks. Если вы хотите указать несколько масок, указывайте каждую маску в новой строке с новым индексом (ExcludeMasks.item_0000, ExcludeMasks.item_0001).	Значение по умолчанию не задано.
Секция **[ScanScope.item_#]** содержит области, защищаемые программой. Для задачи Защита от шифрования требуется указать хотя бы одну область защиты, можно указывать только общие директории. Вы можете указать в конфигурационном файле несколько секций [ScanScope.item_#] в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области защиты, содержит дополнительную информацию об области защиты.	Значение по умолчанию: All shared directories.
UseScanArea	Включение защиты указанной области. Для выполнения задачи требуется включить защиту хотя бы одной области.	Yes (значение по умолчанию) – защищать указанную область. No – не защищать указанную область.
AreaMask	Ограничение области защиты. В области защиты программа защищает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (защищать все объекты).

Параметр	Описание	Значения
Path	Путь к директории с защищаемыми объектам.	<путь к локальной директории> – защищать локальную директорию, доступную через SMB/NFS. Для указания пути можно использовать маски. AllShared (значение по умолчанию) – защищать все ресурсы, доступные через SMB/NFS. Shared:SMB <путь> – защищать ресурсы, доступные через SMB. Shared:NFS <путь> – защищать ресурсы, доступные через NFS.
Секция **[ExcludedFromScanScope.item_#]** содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#]. Объекты, удовлетворяющие правилам любой из секций [ExcludedFromScanScope.item_#], не проверяются. Формат секции [ExcludedFromScanScope.item_#] аналогичен формату секции [ScanScope.item_#]. Вы можете указать в конфигурационном файле несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области исключения из защиты, содержит дополнительную информацию об области исключения.	Значение по умолчанию: All objects.
UseScanArea	Исключение указанной области из защиты.	Yes (значение по умолчанию) – исключать указанную область из защиты. No – не исключать указанную область из защиты.
AreaMask	Ограничение области исключения из защиты. В области исключения программа исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Программа будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (исключать все объекты).

Параметр	Описание	Значения
`Path`	Путь к директории с объектами, исключаемыми из защиты.	`<путь к локальной директории>` – исключать из защиты объекты в указанной директории. Для указания пути можно использовать маски. `Mounted:NFS` – исключать из защиты удаленные директории, смонтированные на компьютере по протоколу NFS. `Mounted:SMB` – исключать из защиты удаленные директории, смонтированные на компьютере по протоколу Samba. `AllRemoteMounted` – исключать из защиты все удаленные директории, смонтированные на компьютере с помощью протоколов Samba и NFS.

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.

Разблокировка 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) или подсетей. Таким образом, вы можете указать компьютеры в виде списка.

Указанные компьютеры будут разблокированы.

Примеры:

Адреса IPv4:

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

Адреса IPv6:

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

kaspersky

Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)

Во время работы задачи Защита от веб-угроз программа проверяет входящий трафик, предотвращает загрузку вредоносных файлов из интернета, а также блокирует доступ к фишинговым, рекламным и прочим опасным веб-сайтам. Программа проверяет трафик, передаваемый по протоколам HTTP, HTTPS и FTP. Также выполняется проверка веб-сайтов и IP-адресов. Вы можете указать определенные сетевые порты или диапазоны сетевых портов (см. раздел "Параметры проверки зашифрованных соединений" на стр. 104) для проверки.

По умолчанию задача Защита от веб-угроз не запущена. При этом задача запустится автоматически, если в системе обнаружен один из перечисленных исполняемых файлов браузеров:

- chrome;
- chromium;
- chromium-browser;
- firefox;
- firefox-esr;
- google-chrome;
- opera;
- yandex-browser.

Для проверки HTTPS-трафика вам нужно включить проверку защищенных соединений (см. раздел "Параметры проверки зашифрованных соединений" на стр. 104). Для проверки FTP-трафика вам нужно задать значение параметра `MonitorNetworkPorts=All`.

Программа Kaspersky Endpoint Security добавляет в список таблицы mangle утилит iptables и ip6tables специальную разрешающую цепочку правил kesl_bypass, которая позволяет исключать трафик из проверки программой. Если в цепочке настроены правила исключения трафика, они влияют на работу задачи Защита от веб-угроз.

При открытии веб-сайта задача Защита от веб-угроз выполняет следующие действия:

1. Проверяет надежность веб-сайта с помощью загруженных баз программы.
2. Проверяет надежность веб-сайта с помощью эвристического анализа, если он включен.
3. Проверяет надежность веб-сайта с помощью службы Kaspersky Security Network, если она включена.

   Рекомендуется принять участие в Kaspersky Security Network, чтобы увеличить эффективность работы задачи Защита от веб-угроз.
4. Запрещает или разрешает открыть веб-сайт.

При попытке открытия опасного веб-сайта программа выполняет следующие действия:

- Для HTTP- или FTP-трафика программа блокирует доступ и показывает предупреждение.
- Для HTTPS-трафика в браузере отображается страница с ошибкой.

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Защита от веб-угроз.

Таблица 20. Параметры задачи Защита от веб-угроз

Параметр	Описание	Значения
ActionOnDetect	Действия, выполняемые при обнаружении зараженного объекта в веб-трафике.	Notify – разрешить загрузку обнаруженного объекта, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте. Block (значение по умолчанию) – запретить доступ к обнаруженному объекту, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.
CheckMalicious	Показывает, выполняется ли проверка ссылок по базе вредоносных веб-адресов.	Yes (значение по умолчанию) – проверять ссылки на вхождение в базу вредоносных веб-адресов. No – не проверять ссылки на вхождение в базу вредоносных веб-адресов.
CheckPhishing	Показывает, выполняется ли проверка ссылок по базе фишинговых веб-адресов.	Yes (значение по умолчанию) – проверять ссылки на вхождение в базу фишинговых веб-адресов. No – не проверять ссылки на вхождение в базу фишинговых веб-адресов.
UseHeuristicForPhishing	Показывает, используется ли эвристический анализ для проверки веб-страниц на наличие фишинговых ссылок.	Yes (значение по умолчанию) – использовать эвристический анализ для обнаружения фишинговых ссылок. Если выбрано это значение, используется поверхностный уровень эвристического анализа – Light (наименее тщательная проверка, минимальная загрузка системы). Для задачи Защита от веб-угроз невозможно изменить уровень эвристического анализа. No – не использовать эвристический анализ для обнаружения фишинговых ссылок.
CheckAdware	Показывает, выполняется ли проверка ссылок по базе рекламных веб-адресов.	Yes – проверять ссылки на вхождение в базу рекламных веб-адресов. No (значение по умолчанию) – не проверять ссылки на вхождение в базу рекламных веб-адресов.

Параметр	Описание	Значения
CheckOther	Показывает, будет ли выполняться проверка ссылок на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда компьютеру или персональным данным.	Yes – проверять ссылки на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда компьютеру или персональным данным. No (значение по умолчанию) – не проверять ссылки на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда компьютеру или персональным данным.
UseTrustedAddresses	Включает или выключает использование списка доверенных веб-адресов. Программа не анализирует информацию, полученную с доверенных веб-адресов, и не проверяет их на вирусы и другие вредоносные объекты. Доверенные веб-адреса можно указать с помощью параметра TrustedAddresses.item_#.	Yes (значение по умолчанию) – использовать список доверенных веб-адресов. No – не использовать список доверенных веб-адресов.
TrustedAddresses.item_#	Доверенные веб-адреса. Для указания веб-адресов можно использовать маски. Использование масок для указания IP-адресов не поддерживается.	Значение по умолчанию не задано.

kaspersky

Задача Проверка съемных дисков (Removable_Drives_Scan, ID:16)

Во время работы задачи Проверка съемных дисков, программа проверяет подключенное устройство и его загрузочные секторы на вирусы и вредоносные программы. Выполняется проверка следующих съемных дисков: CD/DVD-приводов, Blu-ray дисков, флеш-накопителей (включая USB-модемы), внешних жестких дисков и дискет.

Если запущена задача Проверка съемных дисков, программа контролирует подключение съемных дисков к компьютеру. При подключении съемного диска программа создает и запускает временную задачу Scan_Boot_Sectors с типом ODS (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92) с параметром `ScanBootSectors=yes` (см. раздел "Параметры задачи Выборочная проверка" на стр. 129). Эту задачу остановить невозможно. После завершения выполнения задачи программа автоматически ее удаляет.

Если вы настроили проверку файлов, программа также запускает одну или несколько пользовательских задач Scan_File с типом ODS (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92) с параметром `ScanFiles=yes` (см. раздел "Параметры задачи Выборочная проверка" на стр. 129). При необходимости пользователь с правами администратора может остановить выполнение этой задачи.

При изменении параметров задачи Проверка съемных дисков, новые значения не применяются к уже запущенным задачам Scan_Boot_Sectors и Scan_File. При остановке задачи Проверка съемных дисков уже запущенные задачи Scan_Boot_Sectors и Scan_File не останавливаются.

По умолчанию задача Проверка съемных дисков не запущена. При необходимости вы можете запустить или остановить (см. раздел "Запуск и остановка задачи" на стр. 98) задачу в любой момент.

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

Таблица 21. Параметры задачи Проверка съемных дисков

Параметр	Описание	Значения
`ScanRemovableDrives`	Включение проверки съемных дисков при подключении к компьютеру. Этот параметр не применяется к CD/DVD-приводам и Blu-ray дискам (см. описание параметра `ScanOpticalDrives`).	`DetailedScan` – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При детализированной проверке используются параметры по умолчанию для задачи Выборочная проверка. `QuickScan` – проверять только файлы определенных типов на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При быстрой проверке используются параметры по умолчанию для задачи Защита от файловых угроз. `NoScan` (значение по умолчанию) – не проверять съемные диски при подключении.

Параметр	Описание	Значения
ScanOpticalDrives	Включение проверки CD/DVD-приводов и Blu-ray дисков при подключении к компьютеру.	DetailedScan – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. При детализированной проверке используются параметры по умолчанию для задачи Выборочная проверка. QuickScan – проверять только файлы определенных типов на CD/DVD-приводах и Blu-ray дисках. При быстрой проверке используются параметры по умолчанию для задачи Защита от файловых угроз. NoScan (значение по умолчанию) – не проверять CD/DVD-приводы и Blu-ray диски при подключении.
BlockDuringScan	Включение блокировки файлов на подключенном диске при проверке. При проверке загрузочных секторов файлы не блокируются.	Yes – блокировать файлы при проверке. No (значение по умолчанию) – не блокировать файлы при проверке.

kaspersky

Задача Проверка контейнеров (Container_Scan, ID:18)

Задача Проверка контейнеров – это однократная полная или пользовательская проверка файлов, выполняемая программой Kaspersky Endpoint Security.

Во время работы задачи Проверка контейнеров программа проверяет контейнеры, образы и пространства имен на вирусы и вредоносные программы. Вы можете одновременно запустить несколько задач Проверка контейнеров.

Поддерживается интеграция с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Для использования задачи требуется лицензия, которая включает эту функцию.

В этом разделе

Параметры задачи Проверка контейнеров

В таблице описаны все доступные значения и значения по умолчанию для всех параметров проверки контейнеров и образов.

Таблица 22. Параметры задачи Проверка контейнеров

Параметр	Описание	Значения
`ScanContainers`	Включает или выключает проверку контейнеров, заданных по маске. Маски можно указывать с помощью параметра `ContainerNameMask`.	`Yes` (значение по умолчанию) – проверять контейнеры, заданные по маске. `No` – не проверять контейнеры, заданные по маске.

Параметр	Описание	Значения

`ContainerNameMask`	Имя или маска имени проверяемого контейнера.
	Маски указываются в формате командной оболочки. Можно использовать символы ? и *.
	Прежде чем указать этот параметр, убедитесь, что для параметра `ScanContainers` выбрано значение `Yes`.
		Значение по умолчанию: `*` (выполнять проверку всех контейнеров).
		Примеры:
		Проверять контейнер с именем my_container:
		`ContainerNameMask=my_container`
		Проверять все контейнеры, имена которых начинаются с my_container:
		`ContainerNameMask=my_container*`
		Проверять все контейнеры, имена которых начинаются с my_, затем содержат пять любых символов, затем слово _container и заканчиваются любой последовательностью символов:
		`ContainerNameMask=my_?????_container*`

`ScanImages`	Включает или выключает проверку образов, заданных по маске. Маски можно указывать с помощью параметра `ImageNameMask`.	`Yes` (значение по умолчанию) – проверять образы, заданные по маске. `No` – не проверять образы, заданные по маске.

`ImageNameMask`	Имя или маска имени проверяемых образов.
	Прежде чем указать этот параметр, убедитесь, что для параметра `ScanImages` выбрано значение `Yes`.
	Маски указываются в формате командной оболочки.
	Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (`item_xxxx`).
		Значение по умолчанию: `*`.
		Выполняется проверка всех образов.
		Примеры:
		Проверять образы с именем my_image и значением тега latest:
		`ImageNameMask=my_image:latest`
		Проверять все образы, имена которых начинаются с my_image_, имеющие любое значения тега:
		`ImageNameMask=my_image*`

`DeepScan`	Включает или включает проверку всех слоев образов и запущенных контейнеров.	`Yes` – проверять все слои. `No` (значение по умолчанию) – не проверять все слои.

Параметр	Описание	Значения
ContainerScanAction	Действие над контейнером при обнаружении зараженного объекта. Действия над зараженным объектом внутри контейнера описаны ниже.	StopContainer – программа останавливает контейнер при обнаружении зараженного объекта. StopContainerIfFailed (значение по умолчанию) – программа останавливает контейнер, если не удалось вылечить зараженный объект. Skip – программа не выполняет никаких действий над контейнерами при обнаружении зараженного объекта.
ImageAction	Действие над образом при обнаружении зараженного объекта. Действия над зараженным объектом внутри образа описаны ниже.	Skip (значение по умолчанию) – программа не выполняет никаких действий над образами при обнаружении зараженного объекта. Delete – программа удаляет образ при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.

Ниже описаны параметры, которые применяются к объектам внутри контейнеров и образов.

Таблица 23. Параметры задачи Проверка контейнеров

Параметр	Описание	Значения
ScanArchived	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2; .tbz; .tbz2; .gz; .tgz; .arj.	Yes (значение по умолчанию) – проверять архивы. Если указано значение FirstAction=Recommended, то в зависимости от типа архива программа удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. No – не проверять архивы.
ScanSfxArchived	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	Yes (значение по умолчанию) – проверять самораспаковывающиеся архивы. No – не проверять самораспаковывающиеся архивы.
ScanMailBases	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	Yes – проверять файлы почтовых баз. No (значение по умолчанию) – не проверять файлы почтовых баз.

Параметр	Описание	Значения
ScanPlainMail	Включение проверки сообщений электронной почты в текстовом формате (plain text).	Yes – проверять сообщения электронной почты в текстовом формате. No (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
ScanPriority	Приоритет задачи. Приоритет задачи – это параметр, сочетающий несколько внутренних параметров программы Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.	Idle – запустить задачу с низким приоритетом: не более 10% потребления ресурсов процессора. Выберите это значение, если вы хотите выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени. Normal (значение по умолчанию) – запустить задачу со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. High – запустить задачу с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Программа прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, программа пропускает объект при проверке.	0 – 999,999 0 – программа проверяет объекты любого размера. Значение по умолчанию: 0.

Параметр	Описание	Значения
FirstAction	Выбор первого действия, которое Kaspersky Endpoint Security будет выполнять над зараженными объектами. Если зараженный объект обнаружен в файле, обращение к которому происходит по символической ссылке, входящей в область проверки (в то время как сам файл, обращение к которому происходит по символической ссылке, не входит в область проверки), над этим файлом будет выполнено указанное действие. Например, если выбрано действие Remove (удалять), программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.	Disinfect (лечить) – программа пытается вылечить объект, сохранив копию объекта в Хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), программа оставляет объект неизменным. Если первым действием выбрано Disinfect, рекомендуется задать второе действие в параметре SecondAction. Remove (удалять) – программа удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – программа 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) – программа не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Recommended.
SecondAction	Выбор второго действия, которое Kaspersky Endpoint Security будет выполнять над зараженными объектами. Программа 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, программа в качестве второго действия выполняет Skip (пропускать). Значение по умолчанию: Skip.
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.

Параметр	Описание	Значения

ExcludeMasks	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.	Значение по умолчанию не задано.
		Пример:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

ExcludeThreats	Исключение из проверки объектов 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 программы о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа 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 программы. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.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`

Параметр	Описание	Значения
ReportCleanObjects	Включение записи в журнал информации о проверенных объектах, которые программа признала незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой.	Yes – записывать в журнал информацию о незараженных объектах. No (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен программой.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
ReportUnprocessedObjects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет программе распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор; No – выключить эвристический анализатор.
HeuristicLevel	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная загрузка системы. Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. Deep – наиболее тщательная проверка, максимальная загрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.

Параметр	Описание	Значения
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.

Интеграция с Jenkins

Программа Kaspersky Endpoint Security поддерживает интеграцию с Jenkins. Плагины Jenkins Pipeline можно использовать для проверки Docker-образов на разных этапах. Например, можно проверять Docker-образы в репозитории в процессе разработки или перед публикацией.

► *Чтобы интегрировать Kaspersky Endpoint Security с Jenkins:*

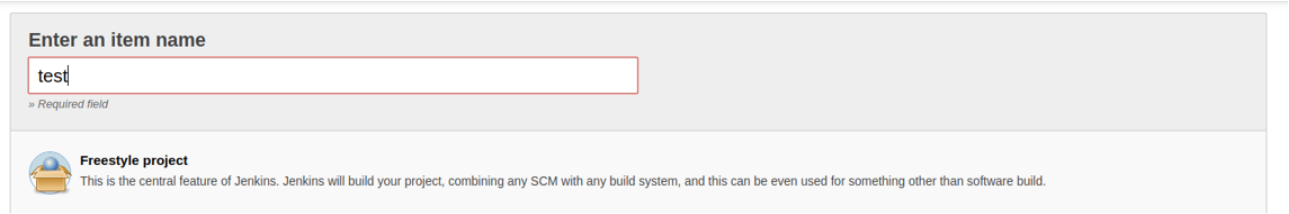
1. Установите Kaspersky Endpoint Security на узле Jenkins.
2. Установите Docker Engine на узле Jenkins.

   Дополнительная информация приведена в документации Docker Engine (https://docs.docker.com/install/).
3. Предоставьте пользователю Jenkins права администратора Kaspersky Endpoint Security:

   ```
   kesl-control --grant-role admin <имя пользователя Jenkins>
   ```
4. Добавьте пользователя Jenkins в группу docker:

   ```
   sudo usermod -aG docker <имя пользователя Jenkins>
   ```

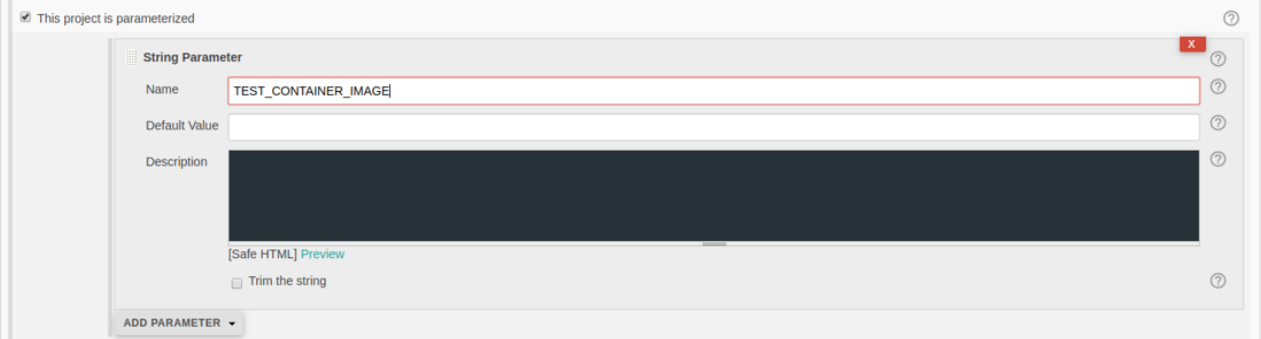
   Обычно используется имя jenkins.
5. В Jenkins создайте новое задание на сборку с названием `test` (**New Item** → **Enter an item name**).

   Настройте проект в соответствии с вашими требованиями. Предполагается, что в результате настройки вы получите образ или запущенный контейнер, который нужно проверить.
6. Чтобы запустить Docker-контейнер, добавьте следующий скрипт в процедуру сборки Jenkins. Если вы используете плагины Jenkins или другой способ запуска Docker-контейнеров, сохраните идентификатор запущенного Docker-контейнера в файл /tmp/kesl_cs_info для дальнейшей проверки:

   ```
   TMP_FILE="/tmp/kesl_cs_info"
   EXIT_CODE=0
   echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
   CONTAINER_ID=$(docker run -d -v /storage:/storage
   ${TEST_CONTAINER_IMAGE} /storage/docker_process.sh)
   ```

```
if [ -z "${CONTAINER_ID}" ] ; then
   echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
   exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
exit ${EXIT_CODE}
```



7. После создания артефактов добавьте следующий сценарий к шагам создания jenkins.

   Этот скрипт поддерживает проверку одного контейнера. При необходимости измените скрипт в соответствии с вашими требованиями.

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
   echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
   exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
   echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
   exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep
'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
   echo "ATTENTION! ${THREATS_AMOUNT} threats detected at:
   '${CONTAINER_ID}'"
   EXIT_CODE=1
else
```

```
   echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

8. Чтобы выполнить проверку Docker-образа из репозитория, выполните следующий скрипт:

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
   echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
   echo "Dockerfile not fetched"
   exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME} .
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container ${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

9. Сохраните задание на сборку.

kaspersky

Задача Выборочная проверка контейнеров (Custom_Container_Scan, ID:19)

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

При запуске задачи Выборочная проверка контейнеров программа создает пользовательскую задачу Проверка контейнеров (Container_Scan, ID=18) с типом ContainerScan с параметрами задачи Custom_Container_Scan. Вы можете изменить значения параметров задачи Custom_Container_Scan из командной строки. После завершения проверки программа автоматически удаляет пользовательскую задачу. Вы не можете удалить задачу Выборочная проверка контейнеров.

► *Чтобы запустить задачу Выборочная проверка контейнеров, выполните следующую команду:*

```
kesl-control --scan-container <идентификатор контейнера или образа|имя контейнера|имя образа[:тег]>
```

Если существует несколько элементов с одинаковым именем, программа проверяет их все.

Для проверки нескольких объектов можно использовать маски.

При создании задачи Выборочная проверка контейнеров с помощью команды `kesl-control --create-task <название задачи> --type ContainerScan` программа использует те же значения параметров, что и для задачи Проверка контейнеров (Container_Scan), за исключением параметра `ScanPriority=Normal` (см. раздел "Параметры задачи Проверка контейнеров" на стр. 174).

Примеры:

Проверка контейнера с именем my_container:

```
kesl-control --scan-container my_container
```

Проверка образа с именем my_image (все теги):

```
kesl-control --scan-container my_image*
```

В таблице описаны все доступные значения и значения по умолчанию для всех параметров проверки контейнеров и образов.

Таблица 24. Параметры задачи Выборочная проверка контейнеров

Параметр	Описание	Значения
`ScanContainers`	Включает или выключает проверку контейнеров, заданных по маске. Маски можно указывать с помощью параметра `ContainerNameMask`.	`Yes` (значение по умолчанию) – проверять контейнеры, заданные по маске. `No` – не проверять контейнеры, заданные по маске.

Параметр	Описание	Значения
ContainerNameMask	Имя или маска имени проверяемого контейнера. Маски указываются в формате командной оболочки. Можно использовать символы ? и *. Прежде чем указать этот параметр, убедитесь, что для параметра ScanContainers выбрано значение Yes.	Значение по умолчанию: *. Выполняется проверка всех контейнеров. **Примеры:** Проверять контейнер с именем my_container: ContainerNameMask=my_container Проверять все контейнеры, имена которых начинаются с my_container: ContainerNameMask=my_container* Проверять все контейнеры, имена которых начинаются с my_, затем содержат пять любых символов, затем слово _container и заканчиваются любой последовательностью символов: ContainerNameMask=my_?????_container*
ScanImages	Включает или выключает проверку образов, заданных по маске. Маски можно указывать с помощью параметра ImageNameMask.	Yes (значение по умолчанию) – проверять образы, заданные по маске. No – не проверять образы, заданные по маске.
ImageNameMask	Имя или маска имени проверяемых образов. Прежде чем указать этот параметр, убедитесь, что для параметра ScanImages выбрано значение Yes. Маски указываются в формате командной оболочки. Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (item_xxxx).	Значение по умолчанию: *. Выполняется проверка всех образов. **Примеры:** Проверять образы с именем my_image и значением тега latest: ImageNameMask=my_image:latest Проверять все образы, имена которых начинаются с my_image_, имеющие любое значения тега: ImageNameMask=my_image*
DeepScan	Включает или выключает проверку всех слоев образа.	Yes – проверять все слои образа. No (значение по умолчанию) – не проверять все слои образа.

Параметр	Описание	Значения
ContainerScanAction	Действие над контейнером при обнаружении зараженного объекта. Действия над зараженным объектом внутри контейнера описаны ниже.	StopContainerIfFailed (значение по умолчанию) – программа останавливает контейнер, если не удалось вылечить зараженный объект. StopContainer – программа останавливает контейнер при обнаружении зараженного объекта. Skip – программа не выполняет никаких действий над контейнерами при обнаружении зараженного объекта.
ImageAction	Действие над образом при обнаружении зараженного объекта. Действия над зараженным объектом внутри образа описаны ниже.	Skip (значение по умолчанию) – программа не выполняет никаких действий над образами при обнаружении зараженного объекта. Delete – программа удаляет образ при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.

Ниже описаны параметры, которые применяются к объектам внутри контейнеров и образов.

Таблица 25. Параметры задачи Выборочная проверка контейнеров

Параметр	Описание	Значения
ScanArchived	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2; .tbz; .tbz2; .gz; .tgz; .arj.	Yes (значение по умолчанию) – проверять архивы. Если указано значение FirstAction=Recommended, то в зависимости от типа архива программа удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. No – не проверять архивы.
ScanSfxArchived	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	Yes (значение по умолчанию) – проверять самораспаковывающиеся архивы. No – не проверять самораспаковывающиеся архивы.
ScanMailBases	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	Yes – проверять файлы почтовых баз. No (значение по умолчанию) – не проверять файлы почтовых баз.

Параметр	Описание	Значения
ScanPlainMail	Включение проверки сообщений электронной почты в текстовом формате (plain text).	Yes – проверять сообщения электронной почты в текстовом формате. No (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
ScanPriority	Приоритет задачи. Приоритет задачи – это параметр, сочетающий несколько внутренних параметров программы и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.	Idle – запустить задачу с низким приоритетом: не более 10% потребления ресурсов процессора. Выберите это значение, если вы хотите выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени. Normal – запустить задачу со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. High (значение по умолчанию) – запустить задачу с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.
TimeLimit	Максимальная продолжительность проверки объекта (в секундах). Программа прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
SizeLimit	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, программа пропускает объект при проверке.	0 – 999,999 0 – программа проверяет объекты любого размера. Значение по умолчанию: 0.

Параметр	Описание	Значения
FirstAction	Выбор первого действия, которое программа будет выполнять над зараженными объектами. Если зараженный объект обнаружен в файле, обращение к которому происходит по символической ссылке, входящей в область проверки (в то время как сам файл, обращение к которому происходит по символической ссылке, не входит в область проверки), над этим файлом будет выполнено указанное действие. Например, если выбрано действие Remove (удалять), программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.	Disinfect (лечить) – программа пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), программа оставляет объект неизменным. Если первым действием выбрано Disinfect, рекомендуется задать второе действие в параметре SecondAction. Remove (удалять) – программа удаляет зараженный объект, предварительно создав его резервную копию. Recommended (выполнять рекомендуемое действие) – программа автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, программа сразу удаляет троянские программы, так как они не заражают другие файлы и поэтому не предполагают лечения. Skip (пропускать) – программа не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Recommended.
SecondAction	Выбор второго действия, которое программа будет выполнять над зараженными объектами. Программа 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, программа в качестве второго действия выполняет Skip (пропускать). Значение по умолчанию: Skip.
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.

Параметр	Описание	Значения

ExcludeMasks	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.	Значение по умолчанию не задано.
		Пример:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

ExcludeThreats	Исключение из проверки объектов 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 программы о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа 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 программы. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии https://encyclopedia.kaspersky.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`

Параметр	Описание	Значения
ReportCleanObjects	Включение записи в журнал информации о проверенных объектах, которые программа признала незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой.	Yes – записывать в журнал информацию о незараженных объектах. No (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
ReportPackedObjects	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен программой.	Yes – записывать в журнал информацию о проверке объектов в составе архивов. No (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
ReportUnprocessedObjects	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	Yes – записывать в журнал информацию о необработанных объектах. No (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
UseAnalyzer	Включение эвристического анализатора. Эвристический анализ позволяет программе распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	Yes (значение по умолчанию) – включить эвристический анализатор; No – выключить эвристический анализатор.
HeuristicLevel	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	Light – наименее тщательная проверка, минимальная загрузка системы. Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. Deep – наиболее тщательная проверка, максимальная загрузка системы. Recommended (значение по умолчанию) – рекомендуемое значение.
UseIChecker	Включение использования технологии iChecker.	Yes (значение по умолчанию) – включить использование технологии iChecker. No – выключить использование технологии iChecker.

kaspersky

Задача Анализ поведения (Behavior_Detection, ID:20)

Задача Анализ поведения контролирует вредоносную активность программ в операционной системе. При обнаружении вредоносной активности Kaspersky Endpoint Security может завершать процесс программы, осуществляющей вредоносную активность.

По умолчанию задача Анализ поведения запускается автоматически при запуске программы. При необходимости вы можете остановить (см. раздел "Запуск и остановка задачи" на стр. 98) задачу в любой момент.

Таблица 26. Параметры задачи Анализ поведения

Параметр	Описание	Значения
TaskMode	Действие, выполняемое программой при обнаружении вредоносной активности в операционной системе.	Block (значение по умолчанию) – завершать процесс программы, осуществляющей вредоносную активность. Notify – не завершать процесс, осуществляющий вредоносную активность, только регистрировать обнаружение вредоносной активности в журнале событий.
UseTrustedPrograms	Исключение процессов из проверки.	Yes – исключать из проверки активность указанных процессов. No (значение по умолчанию) – проверять все процессы.
Секция **[TrustedPrograms.item_#]** содержит процессы, которые исключаются из проверки. Программа Kaspersky Endpoint Security не контролирует активность указанных процессов.		
ProgramPath	Путь к исключаемому процессу.	<полный путь к процессу> – исключать из проверки процесс в указанной локальной директории. Для указания пути можно использовать маски.
ApplyToDescendants	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром ProgramPath.	Yes – исключать из проверки указанный процесс и все его дочерние процессы. No (значение по умолчанию) – исключать из проверки только указанный процесс, не исключать из проверки дочерние процессы.
ProgramDesc	Описание исключаемого процесса.	

kaspersky

Задача Контроль программ (Application_Control, ID:21)

Во время выполнения задачи Контроль программ Kaspersky Endpoint Security управляет запуском программ на компьютерах пользователей. Это позволяет снизить риск заражения компьютера, ограничивая доступ к программам. Запуск программ регулируется с помощью *правил контроля программ* (см. раздел "*О правилах контроля программ*" на стр. 193).

Для использования задачи требуется лицензия, которая включает эту функцию.

Задача Контроль программ может работать в двух режимах:

- *Список запрещенных*. Режим, при котором программа Kaspersky Endpoint Security разрешает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ. Этот режим работы задачи Контроль программ настроен по умолчанию.
- *Список разрешенных*. Режим, при котором программа Kaspersky Endpoint Security запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ.

Таким образом, если правила контроля программ сформированы максимально полно, программа Kaspersky Endpoint Security запрещает запуск всех новых, не проверенных администратором локальной сети организации программ, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

Для каждого режима работы задачи Контроль программ вы можете создать отдельные правила, а также выбрать действие, которое программа Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска программы: *применять правила* или *тестировать правила*.

Если вы меняете список разрешенных программ или запрещаете запуск всех программ и / или программ, влияющих на работу Kaspersky Endpoint Security, то при изменении параметров задачи с помощью конфигурационного файла (см. раздел "Изменение параметров задачи с помощью конфигурационного файла" на стр. 96) или с помощью командной строки (см. раздел "Изменение параметров задачи с помощью командной строки" на стр. 97) требуется запускать команду `--set-settings` с флагом `--accept`.

Kaspersky Endpoint Security поддерживает следующие интерпретаторы: python, perl, bash, ssh. Контроль программ не контролирует запуск скриптов из интерпретаторов, не поддерживаемых программой Kaspersky Endpoint Security и запуск скриптов, передаваемых интерпретатору не через командную строку.

Если запуск интерпретатора разрешен правилами Контроля программ, то Kaspersky Endpoint Security не блокирует скрипт, запущенный из этого интерпретатора. Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами Контроля программ, то Kaspersky Endpoint Security блокирует все скрипты, указанные в командной строке интерпретатора. Исключение: cat script.py | python.

kaspersky

В этом разделе

О правилах контроля программ

Правило контроля программ представляет собой набор параметров, необходимых для работы задачи Контроль программ:

- Принадлежность программы к категории программ. *Категория программ* – это группа программ, обладающих общими признаками. Например, категория, в которую входят исполняемые файлы установленных программ, или категория программ, необходимых для работы, в которую входит стандартный набор программ, используемых в организации. Вы можете использовать одну и ту же категорию только в одном правиле. Использование KL-категорий Kaspersky Security Center не поддерживается.
- Разрешение или запрещение выбранным пользователям и / или группам пользователей запускать программы. Вы можете указать пользователя и / или группу пользователей, которым разрешен или запрещен запуск программ из указанной категории.
- Условие срабатывания правила. Условие представляет собой соответствие "тип условия - критерий условия - значение условия". На основании условий срабатывания правила Kaspersky Endpoint Security применяет или не применяет правило к программе. В правилах используются включающие и исключающие условия:
  - *Включающие условия*. Kaspersky Endpoint Security применяет правило к программе, если программа соответствует хотя бы одному включающему условию.
  - *Исключающие условия*. Kaspersky Endpoint Security не применяет правило к программе, если программа соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию.

  Условия срабатывания правила формируются с помощью следующих критериев:
  - имя исполняемого файла программы;
  - имя директории с исполняемым файлом программы;
  - хеш (SHA-256) исполняемого файла программы.

  Для каждого критерия, используемого в условии, вам нужно указать его значение. Если параметры запускаемой программы соответствуют значениям критериев, указанных во включающем условии, правило срабатывает. В этом случае Контроль программ выполняет действие, указанное в правиле. Если параметры программы соответствуют значениям критериев, указанных в исключающем условии, Контроль программ не контролирует запуск программы.

Для каждого режима работы задачи Контроля программ вам нужно создать отдельные правила, а также выбрать действие, которое задача Контроль программ должна выполнять при обнаружении попытки запуска программы: *применять правила* или *тестировать правила*.

Правила контроля программ имеют три *статуса работы*:

- *Включено* – правило включено, программа Kaspersky Endpoint Security применяет это правило во время работы задачи Контроль программ.

- *Выключено* – правило выключено и не используется во время работы задачи Контроль программ.
- *Тест* – программа Kaspersky Endpoint Security разрешает запуск программ, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих программ в отчете.

Статус работы правила имеет более высокий приоритет чем действие, указанное в правиле.

Параметры задачи Контроль программ

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

Таблица 27. Параметры задачи Контроль программ

Параметр	Описание	Значения
`AppControlMode`	Режим работы задачи Контроль программ (см. раздел "Задача Контроль программ (Application_Control, ID:21)" на стр. 192).	`AllowList` – программа Kaspersky Endpoint Security запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ. `DenyList` (значение по умолчанию) – программа Kaspersky Endpoint Security разрешает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ.
`AppControlRulesAction`	Действие, выполняемое программой Kaspersky Endpoint Security при попытке пользователя запустить программу, запрещенную правилами контроля программ.	`ApplyRules` (значение по умолчанию) – Kaspersky Endpoint Security применяет правила контроля программ и выполняет заданное в правилах действие. `TestRules` – Kaspersky Endpoint Security тестирует правила и формирует событие об обнаружении программы, удовлетворяющей правилу.
Секция **[Categories.item_#]** содержит следующие параметры:		
`Name`	Название создаваемой категории программ, для которой будет применяться правило.	
`UseIncludes`	Использование включающих условий (см. раздел "О правилах контроля программ" на стр. 193) для срабатывания правила.	`Yes` – применять правило к программе, если программа соответствует хотя бы одному включающему условию. `No` (значение по умолчанию) – не применять правило к программе, даже если программа соответствует включающему условию.
`IncludeFileNames.item_#`	Имя исполняемого файла, на которое срабатывает правило.	

Параметр	Описание	Значения
IncludeFolders.item_#	Имя директории с исполняемым файлом программы, на которое срабатывает правило.	
IncludeHashes.item_#	Хеш (SHA-256) исполняемого файла, на который срабатывает правило.	
UseExcludes	Использование исключающих условий (см. раздел "О правилах контроля программ" на стр. 193) для срабатывания правила.	Yes – не применять правило к программе, если программа соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию. No (значение по умолчанию) – применять правило к программе, даже если программа соответствует исключающему условию.
ExcludeFileNames.item_#	Имя исполняемого файла, на которое срабатывает правило.	
ExcludeFolders.item_#	Имя директории с исполняемым файлом программы, на которое срабатывает правило.	
ExcludeHashes.item_#	Хеш (SHA-256) исполняемого файла, на который срабатывает правило.	
Секция **[AllowListRules.item_#]** содержит список правил контроля программ для режима работы AllowList. Каждая секция [AllowListRules.item_#] содержит следующие параметры:		
Description	Описание правила контроля программ.	
AppControlRuleStatus	Статус работы правила контроля программ (см. раздел "О правилах контроля программ" на стр. 193).	On (значение по умолчанию) – правило включено, программа Kaspersky Endpoint Security применяет это правило во время работы задачи Контроль программ. Off – правило не используется во время работы задачи Контроль программ. Test – программа Kaspersky Endpoint Security разрешает запуск программ, на которые распространяется действие правила, но фиксирует информацию о запуске этих программ в отчете.

Параметр	Описание	Значения
Category	Название созданной категории программ, для которой применяется правило. Вы можете указать в качестве категории "Golden Image" (см. раздел "Параметры задачи Инвентаризация" на стр. 198).	
Секция **[AllowListRules.item_#.ACL.item_#]** содержит список пользователей, которым разрешен или запрещен запуск программ.		
Access	Тип доступа, назначаемый пользователю или группе пользователей.	Allow (значение по умолчанию) – разрешать запуск программ. Block – запрещать запуск программ.
Principal	Пользователь или группа пользователей, на которых распространяется правило контроля программ.	\Everyone (значение по умолчанию) – правило доступа применяется для всех пользователей. <имя пользователя> – имя пользователя, для которого применяется правило доступа. @<название группы> – название группы пользователей, для которых применяется правило доступа.
Секция **[DenyListRules.item_#]** содержит список правил контроля программ для режима работы DenyList. Каждая секция [DenyListRules.item_#] содержит следующие параметры:		
Description	Описание правила контроля программ.	
AppControlRuleStatus	Статус работы правила контроля программ (см. раздел "О правилах контроля программ" на стр. 193).	On (значение по умолчанию) – правило включено, программа Kaspersky Endpoint Security применяет это правило во время работы задачи Контроль программ. Off – правило не используется во время работы задачи Контроль программ. Test – программа Kaspersky Endpoint Security разрешает запуск программ, на которые распространяется действие правила, но фиксирует информацию о запуске этих программ в отчете.
Category	Название созданной категории программ, для которой применяется правило. Вы можете указать в качестве категории "Golden Image" (см. раздел "Параметры задачи Инвентаризация" на стр. 198).	

Параметр	Описание	Значения
Секция **[DenyListRules.item_#.ACL.item_#]** содержит список пользователей, которым разрешен или запрещен запуск программ.		
`Access`	Тип доступа, назначаемый пользователю или группе пользователей.	`Allow` (значение по умолчанию) – разрешать запуск программ. `Block` – запрещать запуск программ.
`Principal`	Пользователь или группа пользователей, на которых распространяется правило контроля программ.	`\Everyone` (значение по умолчанию) – правило доступа применяется для всех пользователей. `<имя пользователя>` – имя пользователя, для которого применяется правило доступа. `@<название группы>` – название группы пользователей, для которых применяется правило доступа.

Просмотр списка созданных категорий

Вы можете просматривать список созданных категорий программ.

В списке созданных категорий отображаются следующие категории:

- категории, созданные в Kaspersky Security Center;
- категории, добавленные в параметрах задачи Контроль программ (см. раздел "Параметры задачи Контроль программ" на стр. 194) через командную строку;
- категория GoldenImage, созданная с помощью задачи Инвентаризация (см. раздел "Задача Инвентаризация (Inventory_Scan, ID:22)" на стр. 198) (в политике Kaspersky Endpoint Security или через командную строку).

► *Чтобы просмотреть список созданных категорий программ, выполните следующую команду:*

```
kesl-control [-A] --get-categories
```

Kaspersky Endpoint Security отображает следующую информацию о категории программ:

- уникальный идентификатор (GUID) категории;
- название категории; описание категории (если есть);
- список условий включения программ в категорию;
- список условий исключения программ из категории.

kaspersky

Задача Инвентаризация (Inventory_Scan, ID:22)

Задача Инвентаризация позволяет получить информацию обо всех исполняемых файлах программ, хранящихся на компьютерах. Получение информации о программах, установленных на компьютерах, может быть полезно, например, для создания правил контроля программ (см. раздел "О правилах контроля программ" на стр. 193).

Для использования задачи требуется лицензия, которая включает эту функцию.

В этом разделе

Параметры задачи Инвентаризация

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

Таблица 28. Параметры задачи Инвентаризация

Параметр	Описание	Значения
`ScanScripts`	Включение проверки скриптов.	`Yes` (значение по умолчанию) – проверять скрипты. `No` – не проверять скрипты.
`ScanBinaries`	Включение проверки бинарных файлов (elf, java и pyc).	`Yes` (значение по умолчанию) – проверять бинарные файлы. `No` – не проверять бинарные файлы.
`ScanAllExecutable`	Включение проверки файлов с исполняемым битом.	`Yes` (значение по умолчанию) – проверять файлы с исполняемым битом. `No` – не проверять файлы с исполняемым битом.

Параметр	Описание	Значения
ScanPriority	Приоритет задачи. Приоритет задачи – это параметр, сочетающий несколько внутренних параметров программы Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.	Idle – запустить задачу с низким приоритетом: не более 10% потребления ресурсов процессора. Выберите это значение, если вы хотите выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени. Normal (значение по умолчанию) – запустить задачу со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. High – запустить задачу с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.
CreateGoldenImage	Включение создания категории программ "Golden Image" на основе списка программ, обнаруженных на компьютере задачей Инвентаризация. Если значение параметра CreateGoldenImage=Yes, то в правилах контроля программ вы можете использовать категорию программ "Golden Image".	Yes – создавать категорию программ "Golden Image". No (значение по умолчанию) – не создавать категорию программ "Golden Image".
Секция **[ScanScope.item_#]** содержит следующие параметры:		
AreaDesc	Описание области инвентаризации, содержит дополнительную информацию об области инвентаризации. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects.
UseScanArea	Включение проверки указанной области инвентаризации. Для выполнения задачи требуется включить проверку хотя бы одной области инвентаризации.	Yes (значение по умолчанию) – проверять указанную область инвентаризации. No – не проверять указанную область инвентаризации.

Параметр	Описание	Значения
AreaMask	Ограничение области инвентаризации. В области инвентаризации программа проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, программа проверяет все объекты в области инвентаризации. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты).
Path	Путь к директории с проверяемыми объектами.	<путь к локальной директории> – проверять объекты в указанной директории. Значение по умолчанию: /usr/bin
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры.		
AreaDesc	Описание области исключения из инвентаризации, содержит дополнительную информацию об области инвентаризации.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из инвентаризации.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.
AreaMask	Ограничение области исключения из инвентаризации по маскам в формате shell. Если параметр не указан, программа исключает все объекты в области инвентаризации. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (исключать все объекты).
Path	Путь к директории с исключаемыми объектами.	<путь к локальной директории> – исключать из проверки объекты в указанной директории. Для указания пути можно использовать маски.

Просмотр списка обнаруженных программ

Вы можете просматривать список программ, обнаруженных на компьютере в результате выполнения задачи Инвентаризация. Получение информации о программах, установленных на компьютерах, может быть полезно, например, для создания правил контроля программ (см. раздел "О правилах контроля программ" на стр. 193).

► *Чтобы просмотреть список программ, обнаруженных на компьютере, выполните следующую команду:*

```
kesl-control [-A] --get-app-list
```

Kaspersky Endpoint Security отобразит список обнаруженных программ с разбиением по путям, хешу, типу и категориям, если они были заданы ранее в параметрах задачи Контроль программ (см. раздел "Параметры задачи Контроль программ" на стр. 194).

kaspersky

Участие 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 различные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

В зависимости от расположения инфраструктуры различают Глобальный KSN (инфраструктура расположена на серверах "Лаборатории Касперского") и Локальный KSN (инфраструктура расположена на сторонних серверах, например внутри сети интернет-провайдера).

В сертифицированной версии программы Kaspersky Endpoint Security используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается, так как 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.

После изменения лицензии для использования Локального KSN требуется предоставить поставщику услуг информацию о новом ключе. В противном случае обмен информацией с Локальным KSN будет невозможен из-за ошибки аутентификации.

Участие пользователей в Kaspersky Security Network позволяет "Лаборатории Касперского" разрабатывать решения для нейтрализации угроз и уменьшать количество ложных срабатываний компонентов программы. Участие в Kaspersky Security Network является добровольным. Программа предлагает участвовать в KSN во время установки. Вы можете начать или прекратить использование KSN в любой момент.

Существует два варианта участия в Kaspersky Security Network:

- **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 (https://www.kaspersky.ru/products-and-services-privacy-policy). Файл с текстом Положения о Kaspersky Security Network входит в комплект поставки программы.

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, взаимодействуют с KSN при помощи службы KSN Proxy.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.
- Служба KSN Proxy кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение компьютером пользователя запрошенной информации.

Подробнее о службе KSN Proxy вы можете прочитать в документации Kaspersky Security Center. Параметры KSN Proxy вы можете настроить в свойствах Сервера администрирования Kaspersky Security Center.

► *Чтобы проверить подключение к Kaspersky Security Network, выполните следующую команду:*

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

Строка `Состояние KSN` показывает статус подключения к Kaspersky Security Network:

- Если отображается статус `С отправкой статистических данных`, программа Kaspersky Endpoint Security подключена к Kaspersky Security Network, можно получить информацию из базы знаний, отправляется анонимная статистика и информация о типах и источниках угроз.
- Если отображается статус `Без отправки статистических данных`, программа Kaspersky Endpoint Security подключена к Kaspersky Security Network, можно получить информацию из базы знаний, но анонимная статистика и информация о типах и источниках угроз не отправляется.
- Если отображается статус `Нет`, программа Kaspersky Endpoint Security не подключена к Kaspersky Security Network.

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Ваш компьютер не подключен к интернету.
- Вы не участвуете в Kaspersky Security Network.
- Программа не активирована, или срок действия лицензии истек.
- Выявлены проблемы, связанные с лицензионным ключом. Например, ключ находится в списке запрещенных ключей.

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. Злоумышленники могут заменить один или несколько исполняемых модулей или файлов программы другими файлами, содержащими вредоносный код. Чтобы предотвратить такую замену модулей и файлов, в программе Kaspersky Endpoint Security предусмотрена проверка целостности компонентов программы. Программа проверяет модули и файлы на наличие неавторизованных изменений и повреждений. Если модуль или файл программы имеет некорректную контрольную сумму, то он считается поврежденным.

Проверка целостности выполняется для следующих компонентов программы:

- пакет программы;
- пакет графического пользовательского интерфейса;
- пакет Агента администрирования Kaspersky Security Center;
- плагин управления программой Kaspersky Endpoint Security.

Программа проверяет целостность файлов, перечисленных в специальных списках, которые называются *файлы манифеста*. Для каждого компонента программы существует свой файл манифеста, содержащий список файлов программы, целостность которых важна для корректной работы этого компонента программы. Имя файла манифеста для каждого компонента одно и тоже, но содержимое файлов манифестов различается. Файлы манифеста подписаны цифровой подписью, их целостность также проверяется.

Проверка целостности компонентов программы выполняется с помощью утилиты проверки целостности integrity_checker.

Утилиту проверки целостности требуется запускать под учетной записью с root-правами.

Для проверки целостности вы можете использовать как утилиту, устанавливаемую вместе с программой, так и утилиту, поставляемую на сертифицированном CD-диске.

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

Утилита проверки целостности, устанавливаемая вместе с программой, расположена по следующим путям:

- для проверки пакета программы, пакета графического пользовательского интерфейса и Агента администрирования: /opt/kaspersky/kesl/bin/integrity_checker;
- для проверки плагина управления Kaspersky Endpoint Security – в директории, где расположены исполняемые модули (DLL) плагина управления:
  - C:\Program Files\Kaspersky Lab\Kaspersky Security Center\Plugins\<версия плагина>.linux.plg\integrity_checker.exe – для 32-битных операционных систем;
  - C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\Plugins\<версия плагина>.linux.plg\integrity_checker.exe – для 64-битных операционных систем.

Файлы манифеста расположены по следующим путям:

- /opt/kaspersky/kesl/bin/integrity_check.xml – для проверки целостности пакета программы;
- /opt/kaspersky/kesl/bin/gui_integrity_check.xml – для проверки целостности пакета графического пользовательского интерфейса;
- /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – для проверки Агента администрирования для 32-битных операционных систем;
- /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml – для проверки Агента администрирования для 64-битных операционных систем.

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

- для проверки пакета программы и пакета графического пользовательского интерфейса:

  ```
  integrity_checker [<путь к файлу манифеста>] --signature-type kds-with-filename
  ```

- для проверки плагина управления Kaspersky Endpoint Security и Агента администрирования:

  ```
  integrity_checker [<путь к файлу манифеста>]
  ```

  По умолчанию используется путь к файлу манифеста, расположенному в той же директории, в которой расположена утилита проверки целостности.

Вы можете запустить утилиту со следующими необязательными параметрами:

- `--crl <директория>` – путь к директории, содержащей список отозванных сертификатов (Certificate Revocation List).
- `--version` – отобразить версию утилиты.
- `--verbose` – детализировать вывод информации о выполненных действиях и результатах. Если вы не укажете этот параметр, будут отображаться только ошибки, объекты, не прошедшие проверку, и общая статистика проверки.
- `--trace <имя файла>`, где `<файл>` – имя файла, в который будут записываться события с уровнем детализации DEBUG, произошедшие во время проверки.
- `--signature-type kds-with-filename` – тип проверяемой сигнатуры (этот параметр является обязательным для проверки пакета программы, пакета графического пользовательского интерфейса и Агента администрирования).
- `--single-file <файл>` – проверить только один файл, входящий в состав манифеста, остальные объекты манифеста игнорировать.

Вы можете просмотреть описание всех доступных параметров утилиты проверки целостности в справке параметров утилиты, выполнив команду `integrity_checker --help`.

Результат проверки файла манифеста отображается в следующем виде:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата `0`).
- `FAILED` – целостность файлов не подтверждена (код возврата отличен от `0`).

Если при запуске программы обнаружено нарушение целостности программы или Агента администрирования, программа Kaspersky Endpoint Security формирует событие *IntegrityCheckFailed* в журнале событий и в Kaspersky Security Center.

kaspersky

События и отчеты

В процессе работы программы возникают различного рода *события* (см. раздел "*Просмотр событий*" на стр. 206). Они могут иметь информационный характер или нести важную информацию. Например, с помощью события программа может уведомлять об успешно выполненном обновлении баз программы или может фиксировать ошибку в работе некоторого компонента, которую требуется устранить.

На основе событий, происходящих во время работы программы, программа формирует различные типы *отчетов* (см. раздел "*Просмотр отчетов*" на стр. 209).

В событиях и отчетах могут содержаться следующие персональные данные:

- имена и идентификаторы пользователей в операционной системе;
- пути к файлам пользователя;
- IP-адреса удаленных компьютеров, проверяемых задачей Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 163);
- IP-адреса отправителей и получателей сетевых пакетов, проверяемых задачей Управление сетевым экраном;
- веб-адреса источников обновлений (см. раздел "Об источниках обновлений" на стр. 147);
- общие параметры программы;
- названия и параметры задач (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92);
- обнаруженные вредоносные, фишинговые, рекламные веб-адреса и веб-адреса, содержащие легальное программы, которые могут использоваться злоумышленниками для нанесения вреда компьютеру или персональным данным;
- названия контейнеров и образов;
- пути к контейнерам и образам;
- названия и идентификаторы устройств;
- веб-адреса репозиториев;
- имена файлов, пути к файлам и хеш-суммы исполняемых файлов программ;
- названия категорий программ.

В этом разделе

Просмотр событий

Вы можете просматривать события следующими способами:

- В журнале событий программы. Журнал событий расположен в директории, указанной общим параметром программы `EventsStoragePath`. По умолчанию программа сохраняет информацию

о событиях в директорию базы данных /var/opt/kaspersky/kesl/private/storage/events.db. Для доступа к базе данных событий требуются root-права.

- Если в общих параметрах программы для параметра `UseSysLog` указано значение `Yes`, то данные о событиях также записываются в syslog. Для доступа к syslog требуются root-права.
- Включить вывод текущих событий (см. раздел "Включение вывода событий" на стр. 73) программы с помощью команды `kesl-control -W`.
- Если управление программой Kaspersky Endpoint Security осуществляется с помощью Kaspersky Security Center, данные о событиях могут передаваться на Сервер администрирования Kaspersky Security Center. Если в течение минуты создается три события одного типа от одного инициатора и с одним названием, то программа переключается в режим агрегирования событий и один раз в 10 минут отправляет в Kaspersky Security Center одно агрегированное событие с описанием этих повторяющихся событий. Администратор Kaspersky Endpoint Security может настроить выполнение скрипта при получении события из программы или получение уведомлений о событиях по электронной почте. Подробную информацию о событиях см. в документации Kaspersky Security Center.
- Если включен графический пользовательский интерфейс (GUI), информация о событиях отображается в отчетах (см. раздел "Просмотр отчетов" на стр. 373) и во всплывающих окнах программы.

► *Чтобы получить информацию обо всех событиях в журнале событий, выполните следующую команду:*

```
kesl-control -E --query|less
```

По умолчанию в программе хранится до 500 000 событий. С помощью команды `less` вы можете перемещаться по списку отображаемых событий.

Вы можете просматривать конкретные события с помощью системы запросов (см. раздел "Использование фильтра для ограничения результатов запроса" на стр. 79) к хранилищу событий программы.

При создании запроса требуется указать нужное поле, выбрать логическое выражение и установить для него нужное значение. Значение требуется указывать в одинарных кавычках (‘), а запрос целиком – в двойных кавычках (").

```
--query "<поле> <логическое выражение> '<значение>' [and <поле> <логическое выражение> '<значение>' *]"
```

Значение даты требуется указывать в системе отметок времени UNIX (количество секунд, прошедших с 00:00:00 (UTC), 1 января 1970 года).

kaspersky

Пример события ThreatDetected:

```
EventType=ThreatDetected
EventId=2671
Initiator=Product
Date=2020-04-30 17:17:17
DangerLevel=Critical
FileName=/root/eicar.com.txt
ObjectName=File
TaskName=File_Monitoring
RuntimeTaskId=2
TaskId=1
DetectName=EICAR-Test-File
TaskType=OAS
FileOwner=root
FileOwnerId=0
DetectCertainty=Sure
DetectType=Virware
DetectSource=Local
ObjectId=1
AccessUser=root
AccessUserId=0
```

Примеры запросов:

Вывести все события с заданным значением поля EventType:

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

Вывести все события с заданными значениями полей EventType и FileName:

```
kesl-control -E --query "EventType == 'ThreatDetected' and FileName like
'%eicar%'"
```

Вывести все события, сформированные задачей File_Threat_Protection после указанного момента:

```
kesl-control -E --query "TaskName == 'File_Threat_Protection' and Date >
'1588253494'"
```

Просмотр отчетов

Информация о работе каждого компонента Kaspersky Endpoint Security, результаты выполнения каждой задачи и работы всей программы в целом записываются в отчеты.

Вы можете просматривать отчеты следующими способами:

- Если управление программой Kaspersky Endpoint Security осуществляется с помощью Kaspersky Security Center, вы можете формировать и просматривать отчеты Kaspersky Security Center в Консоли администрирования и в Web Console. С помощью отчетов Kaspersky Security Center вы можете, например, получить сведения о зараженных файлах, использовании ключей и баз программы. Подробную информацию о работе с отчетами Kaspersky Security Center см. в документации Kaspersky Security Center.
- Если включен графический пользовательский интерфейс (GUI), информация о событиях в работе программы отображается в отчетах программы (см. раздел "Просмотр отчетов" на стр. 373).

kaspersky

Управление программой с помощью Консоли администрирования Kaspersky Security Center

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

Описание приведено для версии Kaspersky Security Center 12.

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

Консоль администрирования позволяет удаленно устанавливать и удалять, запускать и останавливать программу Kaspersky Endpoint Security, настраивать параметры работы программы и запускать задачи на управляемых устройствах.

Управление программой через Консоль администрирования осуществляется с помощью mmc-плагина управления Kaspersky Endpoint Security.

Чтобы управлять через Консоль администрирования работой программы Kaspersky Endpoint Security, установленной на компьютерах, вам нужно поместить эти компьютеры в группы администрирования. Вы можете создать группы администрирования в Kaspersky Security Center перед началом установки программы Kaspersky Endpoint Security и настроить правила автоматического перемещения компьютеров в группы администрирования. Или вы можете вручную переместить компьютеры из папки **Нераспределенные устройства** в группы администрирования после установки программы Kaspersky Endpoint Security (см. подробнее в документации Kaspersky Security Center).

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

- просматривать состояние защиты устройств (см. раздел "Просмотр состояния защиты компьютера" на стр. 212);
- просматривать общие параметры программы;
- обновлять базы и модули программы;
- управлять политиками (см. раздел "Управление политиками в Консоли администрирования Kaspersky Security Center" на стр. 214);
- управлять задачами программы (см. раздел "Управление задачами в Консоли администрирования Kaspersky Security Center" на стр. 259).

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

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.

В этом разделе

Запуск и остановка программы на клиентском компьютере

► *Чтобы запустить или остановить программу на клиентском компьютере:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке управляемых устройств выберите компьютер, на котором вы хотите запустить или остановить программу.
5. Правой клавишей мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.
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 11.3.0 для Linux.
8. Если вы хотите запустить программу, нажмите на кнопку  справа от списка программ "Лаборатории Касперского" или выполните следующие действия:

   a. По правой клавише мыши откройте контекстное меню программы Kaspersky Endpoint Security 11.3.0 для Linux и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ.

      Откроется окно **Параметры Kaspersky Endpoint Security 11.3.0 для Linux** на закладке **Общие**.

   b. Нажмите на кнопку **Запустить**.

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

   a. По правой клавише мыши откройте контекстное меню программы Kaspersky Endpoint Security 11.3.0 для Linux и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ.

      Откроется окно **Параметры Kaspersky Endpoint Security 11.3.0 для Linux** на закладке **Общие**.

   b. Нажмите на кнопку **Остановить**.

Просмотр состояния защиты компьютера

► *Чтобы просмотреть состояние защиты компьютера:*

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** – статус клиентского устройства, присвоенный на основе критерия, заданного администратором для статусов антивирусной защиты устройства и активности устройства в сети.
- **Все проблемы** –список проблем, обнаруженных управляемыми программами, установленными на клиентских устройствах. Каждая проблема дополняется статусом, который программа предлагает назначить устройству, имеющему эту проблему.
- **Статус постоянной защиты** – статус задачи Защита от файловых угроз, например, *Выполняется* или *Остановлена*. При изменении статуса устройства новый статус отображается в окне свойств устройства только после синхронизации клиентского устройства с Сервером администрирования.
- **Последняя проверка по требованию** – дата и время выполнения последней антивирусной проверки на клиентском устройстве.
- **Всего обнаружено угроз** – общее количество угроз, обнаруженных на клиентском устройстве с момента установки антивирусной программы (первой проверки) или с момента последнего сброса счетчика угроз.

  Чтобы сбросить счетчик, нажмите на кнопку **Обнулить**.
- **Активные угрозы** – количество угроз, которые программе Kaspersky Endpoint Security не удалось вылечить на данный момент.
- **Статус шифрования диска** – текущий статус шифрования файлов на локальных дисках устройства.

kaspersky

Просмотр параметров программы

► *Чтобы просмотреть параметры программы:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый компьютер.
2. В рабочей области выберите закладку **Устройства**.
3. Правой клавишей мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.
4. В окне **Свойства: <Имя компьютера>** выберите раздел **Программы**.
5. В разделе **Программы** выберите программу Kaspersky Endpoint Security 11.3.0 для Linux в списке установленных программ и в контекстном меню программы выберите пункт **Свойства**.

   В результате откроется окно **Параметры Kaspersky Endpoint Security 11.3.0 для Linux** на разделе **Общие**.

В окне **Параметры Kaspersky Endpoint Security 11.3.0 для Linux** отображается следующая информация о Kaspersky Endpoint Security:

- В разделе **Общие** содержится общая информация об установленной программе:
  - **Номер версии** – номер версии программы.
  - **Установлено** – дата и время установки программы 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 создания и последнего обновления баз программы, а также количество записей в базах.
- В разделе **Компоненты** содержится список стандартных задач. Для каждой задачи отображается ее статус (например, *Запущена* или *Остановлена*) и версия.
- В разделе **Лицензионные ключи** приведена информация об активном и резервном ключах:
  - Уникальная буквенно-цифровая последовательность.
  - **Тип лицензии** – тип лицензии: коммерческая или пробная.
  - **Дата активации** (поле доступно только для активного ключа) – дата добавления активного ключа.
  - **Дата окончания срока действия лицензии** (поле доступно только для активного ключа) – дата окончания срока действия активного ключа.
  - **Срок действия лицензии** – количество дней, в течение которых действует ключ.
  - **Максимальное количество устройств** – количество компьютеров, на которых вы можете использовать ключ.
- В разделе **Настройка событий** содержатся события, которые программы сохраняет в хранилище событий.
- В разделе **Дополнительно** содержится информация о плагине управления программой.

kaspersky

Управление политиками в Консоли администрирования Kaspersky Security Center

Политика – это набор параметров работы программы, определенный для группы администрирования. С помощью политик вы можете установить одинаковые значения параметров работы программы Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования. В политике задаются не все параметры программы.

Для одной программы вы можете настроить несколько политик с различными значениями параметров. Однако одновременно для программы может быть активна только одна политика в пределах группы администрирования. При создании новой политики все остальные политики в группе администрирования становятся неактивными. Вы можете изменить статус политики позже.

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

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

Каждый параметр политики имеет атрибут "замок"  , который показывает, наложен ли запрет на изменение параметров в дочерних политиках и локальных параметрах программы. 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. Для всех клиентских компьютеров группы администрирования используется значение параметра, заданное политикой.
- Если параметр не закрыт "замком" (), это означает, что вы можете изменить значение параметра. Для всех клиентских компьютеров группы администрирования используются значения параметра, установленные локально. Значение параметра, установленное в политике, не применяется.

Для дочерней политики атрибут "замок"  работает, только если в дочерней политике включено наследование параметров из родительской политики.

Параметры программы изменяются в соответствии с параметрами политики после первого применения политики.

Вы можете выполнять следующие действия над политикой:

- Создавать политику (см. раздел "Создание политики" на стр. 215).
- Изменять параметры политики (см. раздел "Изменение параметров политики" на стр. 216).

  Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения. Кроме того, некоторые параметры могут быть недоступны для настройки и использования в сертифицированной версии программы.

- Удалять политику.

- Изменять состояние политики.
- Сравнивать версии политик в окне свойств политики в разделе **История ревизий**.

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

Общая информация о работе с политиками и профилями политик приведена в документации Kaspersky Security Center.

В этом разделе

Создание политики

► *Чтобы создать политику:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** 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. Запустите мастер создания политики одним из следующих способов:
   - Нажмите на кнопку **Новая политика**.
   - По правой клавише мыши вызовите контекстное меню в списке политик и выберите пункт **Создать → Политику**.
5. Выберите в списке **Kaspersky Endpoint Security 11.3.0 для Linux**.

   Перейдите к следующему шагу мастера.
6. Введите имя создаваемой политики.

   Перейдите к следующему шагу мастера.
7. Если вы хотите перенести в создаваемую политику параметры из политики предыдущей версии программы Kaspersky Endpoint Security, установите флажок **Использовать параметры политики для предыдущей версии программы**.

   Перейдите к следующему шагу мастера.
8. Примите решение об участии в Kaspersky Security Network (см. стр. 233). Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

- Если вы согласны со всеми пунктами Положения и хотите использовать Kaspersky Security Network в работе программы, выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.
- Если вы не хотите принимать участие в Kaspersky Security Network, выберите вариант **Я не принимаю условия настоящего Положения о Kaspersky Security Network** и подтвердите свое решение в открывшемся окне.

При необходимости вы сможете изменить решение об участии в Kaspersky Security Network позже (см. стр. 233).

Перейдите к следующему шагу мастера.

9. Если требуется, настройте параметры Защиты от файловых угроз (см. раздел "Защита от файловых угроз" на стр. 219).

   Перейдите к следующему шагу мастера.

10. Если требуется, измените настроенные по умолчанию параметры проверки (см. раздел "Окно Параметры проверки" на стр. 222).

    Перейдите к следующему шагу мастера.

11. Если требуется, настройте области исключения (см стр. 225).

    Перейдите к следующему шагу мастера.

12. Если требуется, измените настроенные по умолчанию действия над зараженными объектами (см. раздел "Окно Действия над зараженными объектами" на стр. 224).

    Перейдите к следующему шагу мастера.

13. Завершите работу 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. Выберите нужную политику.
5. Выберите нужную политику и откройте окно свойств политики одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название политики>**.
6. Измените параметры политики.
7. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**, чтобы сохранить изменения.

Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения. Кроме того, некоторые параметры могут быть недоступны для настройки и использования в сертифицированной версии программы.

Параметры политики

Вы можете использовать политику для настройки параметров работы программы Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования.

Набор параметров и значения по умолчанию для параметров политики могут отличаться в зависимости от типа лицензии на программу (https://support.kaspersky.ru/15471). Кроме того, некоторые параметры могут быть недоступны для настройки и использования в сертифицированной версии программы.

С помощью политики вы можете настраивать параметры работы программы в разделах окна свойств политики, приведенных в таблице ниже. О настройке общих параметров политики и параметрах событий см. в документации Kaspersky Security Center.

Таблица 29. Разделы окна свойств политики

Раздел	Описание
Базовая защита	**Защита от файловых угроз** (см. стр. 219) **Области исключения** (см. стр. 225) **Исключения по процессам** (см. стр. 227) **Управление сетевым экраном** (см. стр. 229) **Защита от веб-угроз** (см. стр. 230) **Защита от сетевых угроз** (см. стр. 233)
Продвинутая защита	**Kaspersky Security Network** (см. стр. 233) **Контроль программ** (см. стр. 236) **Защита от шифрования** (см. стр. 239) **Контроль целостности системы** (см. стр. 244) **Контроль устройств** (см. стр. 247) **Анализ поведения** (см. стр. 248)
Локальные задачи	**Управление задачами** (см. стр. 249) **Проверка съемных дисков** (см. стр. 249)

Раздел	Описание
Общие параметры	**Параметры прокси-сервера** (см. стр. 250) **Параметры программы** (см. стр. 251) **Параметры проверки контейнеров** (см. стр. 252) **Managed Detection and Response** (см. стр. 254) **Параметры сети** (см. стр. 254) **Глобальные исключения** (см. стр. 257) **Исключение памяти процессов** (см. стр. 258) **Параметры Хранилища** (см. стр. 258)

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.

kaspersky

В этом разделе

Защита от файловых угроз

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

Таблица 30. Параметры Защиты от файловых угроз

Параметр	Описание
Включить Защиту от файловых угроз	Флажок включает или выключает Защиту от файловых угроз на всех управляемых устройствах. По умолчанию флажок установлен.

Параметр	Описание
Режим Защиты от файловых угроз	В раскрывающемся списке вы можете выбрать режим работы Защиты от файловых угроз: • **Интеллектуальный режим** (значение по умолчанию) – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс в течение определенного времени многократно обращается к файлу и изменяет его, программа повторно проверяет файл только при последнем закрытии файла этим процессом. • **При открытии** – проверять файл при попытке открытия на чтение, исполнение или изменение. • **При открытии и изменении** – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки (см. раздел "Окно Области проверки" на стр. 220) и параметры проверки (см. раздел "Окно Параметры проверки" на стр. 222).
Действия над зараженными объектами	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действия над зараженными объектами** (см. раздел "Окно Действия над зараженными объектами" на стр. 224), в котором вы можете настроить действия, которые программа Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Окно Области проверки

Таблица содержит области проверки. Программа проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Таблица 31. Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли программа эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно <Название области проверки>

В этом окне вы можете добавить или настроить область проверки.

Таблица 32. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки** (см. раздел "Окно Области проверки" на стр. 220). Поле ввода не должно быть пустым.

Параметр	Описание
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область проверки во время работы. Если флажок снят, программа не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. • **Смонтированная** – смонтированные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все смонтированные** – все смонтированные директории. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательская** – ресурсы файловой системы компьютера, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. По умолчанию указан путь **/** – программа проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, программа проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы Защиты от файловых угроз.

Таблица 33. Параметры Защиты от файловых угроз

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, Kaspersky Endpoint Security проверяет архивы. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, включив и настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, Kaspersky Endpoint Security не проверяет архивы. По умолчанию флажок снят.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, Kaspersky Endpoint Security проверяет самораспаковывающиеся архивы. Если флажок снят, Kaspersky Endpoint Security не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок снят.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз программ Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, Kaspersky Endpoint Security проверяет файлы почтовых баз. Если флажок снят, Kaspersky Endpoint Security не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, Kaspersky Endpoint Security проверяет сообщения в текстовом формате. Если флажок снят, Kaspersky Endpoint Security не проверяет сообщения в текстовом формате. По умолчанию флажок снят.

Параметр	Описание
Пропускать текстовые файлы	Временное исключение из проверки файлов в текстовом формате. Если флажок установлен, Kaspersky Endpoint Security не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течении 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов работы программ. Если флажок снят, Kaspersky Endpoint Security проверяет текстовые файлы. По умолчанию флажок снят.
Прервать проверку, если она длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки объекта в секундах. После истечения указанного времени Kaspersky Endpoint Security прекращает проверку объекта. Доступные значения: `0–9999`. Если указано значение `0`, время проверки не ограничено. Значение по умолчанию: `60`.
Пропускать объекты размером более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0–999999`. Если установлено значение `0`, Kaspersky Endpoint Security проверяет объекты любого размера. Значение по умолчанию: `0`.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, Kaspersky Endpoint Security записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, Kaspersky Endpoint Security не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, Kaspersky Endpoint Security записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, Kaspersky Endpoint Security не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, Kaspersky Endpoint Security записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, Kaspersky Endpoint Security не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.

Параметр	Описание
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, Kaspersky Endpoint Security проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, Kaspersky Endpoint Security проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.

Окно Действия над зараженными объектами

В этом окне вы можете настроить действия, которые программа Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Таблица 34. Параметры Защиты от файловых угроз

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое Kaspersky Endpoint Security выполняет над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Блокировать** доступ к объекту.

Параметр	Описание
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое Kaspersky Endpoint Security выполняет над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Блокировать** доступ к объекту (значение по умолчанию).

Области исключения

Исключение из проверки – это совокупность условий, при выполнении которых программа Kaspersky Endpoint Security не проверяет объект на вирусы и другие угрозы. Вы можете также исключать объекты из проверки по маскам и названиям угроз.

Таблица 35. Параметры исключений из проверки

Блок параметров	Описание
Исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске** (см. раздел "**Окно Исключения по маске**" на стр. 227). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по названию угрозы** (см. раздел "**Окно Исключения по названию угрозы**" на стр. 227). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Окно Области исключения

Таблица содержит области исключения из проверки. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 36. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, применяется ли это исключение в работе программы.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Название области исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Таблица 37. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы программы. Если флажок установлен, программа исключает эту область во время работы. Если флажок снят, программа включает эту область во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все смонтированные** – все смонтированные директории.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательский** – ресурсы файловой системы компьютера, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. По умолчанию указан путь **/** – программа исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые программа исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Программа не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска.

Примеры:

Маска `*.txt` – все текстовые файлы.

Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Программа не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную угрозу из списка исключений. Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

Исключения по процессам

Вы можете настроить исключение активности процессов из проверки. Программа не будет проверять активность указанных процессов. Вы также можете исключать из проверки файлы, изменяемые указанными процессами.

Блок параметров **Исключения по процессам** содержит кнопку **Настроить**, по которой открывается окно **Исключения по процессам** (см. раздел "Окно Исключения по процессам" на стр. 228). В этом окне вы можете задать список областей исключений по процессам.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса и файлов, изменяемых указанным процессом. По умолчанию таблица пуста.

Таблица 38. Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, применяется ли это исключение в работе программы.

Элементы в таблице можно добавлять (см. раздел "Окно Доверенный процесс" на стр. 228), изменять (см. раздел "Окно Доверенный процесс" на стр. 228) и удалять.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Таблица 39. Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Исключения по процессам** (см. раздел "Окно Исключения по процессам" на стр. 228). Поле ввода не должно быть пустым.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром **Путь к исключаемому процессу**. По умолчанию флажок снят.
Использовать эту область	Флажок включает или выключает исключение этой области из проверки во время работы программы. Если флажок установлен, программа исключает эту область во время работы. Если флажок снят, программа включает эту область во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Путь к изменяемым файлам	Блок параметров позволяет задать исключения из проверки для файлов, которые изменяет процесс. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все смонтированные** – все смонтированные директории. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная** или **Общая**, то в раскрывающемся списке протоколов доступа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательский** – ресурсы файловой системы компьютера, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые программа исключает из проверки. Маски применяются к объектам только внутри директории, указанной в блоке **Путь к изменяемым файлам**. Вы можете добавлять, изменять и удалять маски.

Управление сетевым экраном

Сетевой экран операционной системы защищает персональные данные, которые хранятся на компьютере пользователя. Сетевой экран блокирует большую часть угроз для операционной системы, когда компьютер подключен к интернету или локальной сети. Управление сетевым экраном позволяет обнаружить все сетевые соединения на компьютере пользователя и предоставить список их IP-адресов с указанием статуса сетевого соединения по умолчанию.

Компонент Управление сетевым экраном фильтрует всю сетевую активность в соответствии с сетевыми пакетными правилами. Настройка сетевых пакетных правил позволяет вам задать нужный уровень защиты компьютера, от полной блокировки доступа в интернет для всех программ до разрешения неограниченного доступа.

Таблица 40. Параметры компонента Управление сетевым экраном

Параметр	Описание
Включить Управление сетевым экраном	Флажок включает или выключает компонент Управление сетевым экраном. По умолчанию флажок установлен.
Сетевые пакетные правила	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Сетевые пакетные правила**. В этом окне вы можете настроить сетевые пакетные правила, которые будет применять компонент Управление сетевым экраном при обнаружении попытки установления сетевого соединения.
Доступные сети	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Список доступных сетей**. В этом окне вы можете настроить список сетей, которые будет контролировать компонент Управление сетевым экраном.
Входящие соединения	В раскрывающемся списке вы можете выбрать действие для входящих сетевых соединений: • **Разрешать** сетевые соединения (значение по умолчанию). • **Блокировать** сетевые соединения.
Входящие пакеты	В раскрывающемся списке вы можете выбрать действие для входящих пакетов: • **Разрешать** входящие пакеты (значение по умолчанию). • **Блокировать** входящие пакеты.
Всегда добавлять разрешающие правила для портов Агента администрирования	Флажок включает или выключает автоматическое добавление разрешающих правил для портов Агента администрирования. По умолчанию флажок установлен.

Защита от веб-угроз

Во время работы компонента Защита от веб-угроз программа Kaspersky Endpoint Security проверяет входящий трафик, не допускает загрузку вредоносных файлов из интернета, а также блокирует фишинговые, рекламные и прочие опасные веб-сайты. Защита от веб-угроз запускается по умолчанию при запуске программы.

Программа проверяет трафик, передаваемый по протоколам HTTP, HTTPS и FTP. Также выполняется проверка веб-сайтов и IP-адресов. Вы можете указать определенные сетевые порты или диапазоны сетевых портов для проверки.

Для проверки HTTPS-трафика требуется включить проверку зашифрованных соединений (см. раздел "Параметры сети" на стр. 254). Для проверки FTP-трафика требуется установить флажок **Отслеживать все сетевые порты** (см. раздел "Параметры сети" на стр. 254).

Таблица 41. Параметры Защиты от веб-угроз

Параметр	Описание
Включить Защиту от веб-угроз	Флажок включает или выключает компонент Защита от веб-угроз. По умолчанию флажок снят.
Доверенные веб-адреса	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные веб-адреса** (см. раздел "Окно Доверенные веб-адреса" на стр. 231), в котором вы можете указать список доверенных веб-адресов. Программа Kaspersky Endpoint Security не будет проверять содержание веб-сайтов, веб-адреса которых указаны в этом списке.
Действие при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое Kaspersky Endpoint Security будет выполнять над веб-ресурсом, на котором обнаружен опасный объект: • **Информировать** пользователя при обнаружении опасного объекта в веб-трафике. Защита от веб-угроз позволяет выполнить загрузку объекта на компьютер. Kaspersky Endpoint Security записывает в журнал и добавляет в список активных угроз информацию об опасном объекте. • **Блокировать** доступ ко всем опасным объектам, обнаруженным в веб-трафике, показывать уведомление о заблокированных попытках доступа и записывать в журнал информацию об опасных объектах (значение по умолчанию).
Параметры проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Параметры проверки** (см. раздел "Окно Параметры проверки" на стр. 232), в котором вы можете настроить параметры проверки входящего трафика.

Окно Доверенные веб-адреса

В этом окне вы можете добавить веб-адреса и веб-страницы, содержимое которых вы считаете доверенным.

В список доверенных веб-адресов вы можете добавлять только веб-адреса HTTP / HTTPS. Использование масок для указания IP-адресов не поддерживается. По умолчанию список пустой.

Вы можете добавлять, изменять и удалять веб-адреса в списке.

Окно Веб-адрес

В этом окне вы можете добавить веб-адреса или маски веб-адресов в список доверенных веб-адресов.

Таблица 42. Доверенные веб-адреса

Параметр	Описание
Введите адрес или маску адреса веб-сайта	Поле ввода веб-адресов и веб-страниц, содержимое которых вы считаете доверенным. При создании маски адреса используйте символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html).

В список доверенных веб-адресов можно добавлять только веб-адреса HTTP / HTTPS. Использование масок для указания IP-адресов не поддерживается.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки входящего трафика во время работы компонента Защита от веб-угроз.

Таблица 43. Параметры Защиты от веб-угроз

Параметр	Описание
Обнаруживать вредоносные объекты	Флажок включает или выключает проверку ссылок по базе вредоносных веб-адресов. По умолчанию флажок установлен.
Обнаруживать фишинговые ссылки	Флажок включает или выключает проверку ссылок по базе фишинговых веб-адресов. По умолчанию флажок установлен.
Использовать эвристический анализ для обнаружения фишинговых ссылок	Флажок включает или выключает использование эвристического анализа для обнаружения фишинговых ссылок. Флажок доступен и установлен по умолчанию, если установлен флажок **Обнаруживать фишинговые ссылки**.
Обнаруживать рекламные программы	Флажок включает или выключает проверку ссылок по базе рекламных веб-адресов. По умолчанию флажок снят.
Обнаруживать легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройствам или данным	Флажок включает или выключает проверку ссылок по базе легальных программ, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. По умолчанию флажок снят.

kaspersky

Защита от сетевых угроз

Во время работы компонента Защита от сетевых угроз программа проверяет входящий сетевой трафик на действия, характерные для сетевых атак. Защита от сетевых угроз запускается по умолчанию при запуске программы.

Программа проверяет входящий трафик для TCP-портов, номера которых получает из актуальных баз программы. При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, программа блокирует сетевую активность со стороны атакующего компьютера и записывает в журнал соответствующее событие.

Для проверки сетевого трафика задача Защита от сетевых угроз принимает подключения по всем портам, номера которых получает из баз программы. При проверке сети это может выглядеть как открытый порт на устройстве, даже если никакое приложение в системе его не прослушивает. Неиспользуемые порты рекомендуется закрывать средствами сетевого экрана.

Таблица 44. Параметры Защиты от сетевых угроз

Параметр	Описание
Включить Защиту от сетевых угроз	Флажок включает или выключает компонент Защита от сетевых угроз. По умолчанию флажок установлен.
Действие при обнаружении угрозы	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак: • **Информировать** пользователя. Программа разрешает сетевую активность и записывает в журнал информацию об обнаруженной сетевой активности. • **Блокировать** сетевую активность со стороны атакующего компьютера и записывать в журнал информацию об обнаруженной сетевой активности.
Блокировать атакующие устройства	Флажок включает или выключает блокировку сетевой активности при обнаружении попытки сетевой атаки. По умолчанию флажок установлен.
Блокировать атакующее устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки атакующего устройства в минутах. По истечении указанного времени программа Kaspersky Endpoint Security разрешает сетевую активность со стороны этого устройства. Доступные значения: целые числа от `1` до `32768`. Значение по умолчанию: `60`.
Исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения**, в котором вы можете указать список IP-адресов, сетевые атаки с которых не будут заблокированы.

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 различные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

В зависимости от расположения инфраструктуры существуют:

- **Глобальный KSN** – инфраструктура расположена на серверах "Лаборатории Касперского".
- **Локальный KSN** – инфраструктура расположена на сторонних серверах, например внутри сети интернет-провайдера.

В сертифицированной версии программы Kaspersky Endpoint Security используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается, так как 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.

После изменения лицензии для использования Локального KSN требуется предоставить поставщику услуг информацию о новом ключе. В противном случае обмен информацией с Локальным KSN будет невозможен из-за ошибки аутентификации.

Участие пользователей в Kaspersky Security Network позволяет "Лаборатории Касперского" разрабатывать решения для нейтрализации угроз и уменьшать количество ложных срабатываний компонентов программы. Участие в Kaspersky Security Network является добровольным. Программа предлагает участвовать в Kaspersky Security Network во время установки.

В программе предусмотрено два варианта участия в Kaspersky Security Network:

- **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.

Вы можете начать или прекратить использование Kaspersky Security Network в любой момент, а также выбрать другой вариант участия в Kaspersky Security Network, нажав на кнопку **Изменить**.

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 https://www.kaspersky.ru/products-and-services-privacy-policy.

Текст Положения о Kaspersky Security Network вы можете прочитать в окне **Положение о Kaspersky Security Network**, которое можно открыть по ссылке **Текст Положения о Kaspersky Security Network**.

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy. Вы можете настроить параметры

KSN Proxy в свойствах Сервера администрирования Kaspersky Security Center. Подробнее о службе KSN Proxy вы можете см. в документации Kaspersky Security Center.

Параметры Kaspersky Security Network

В этом окне вы можете настроить параметры участия в Kaspersky Security Network.

Таблица 45. Параметры Kaspersky Security Network

Параметр	Описание
Подробнее	По ссылке открывается веб-сайт "Лаборатории Касперского".
Не участвовать в Kaspersky Security Network	Выбирая этот вариант, вы отказываетесь от участия в Kaspersky Security Network.
Kaspersky Security Network без отправки статистических данных	Выбирая этот вариант, вы принимаете условия участия в Kaspersky Security Network. Вы сможете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения.
Kaspersky Security Network с отправкой статистических данных	Выбирая этот вариант, вы принимаете условия участия в Kaspersky Security Network. Вы сможете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Кроме того, для улучшения работы Kaspersky Security Network будет отправляться анонимная статистика и данные о типах и источник различных угроз.
Положение о Kaspersky Security Network	По ссылке открывается окно **Положение о Kaspersky Security Network** (см стр. 235). В этом окне вы можете прочитать текст Положения о Kaspersky Security Network.

Положение о Kaspersky Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Security Network и принять его условия.

Таблица 46. Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите участвовать в Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Security Network. Вариант доступен, если в окне **Параметры Kaspersky Security Network** (см стр. 235) вы выбрали вариант **Kaspersky Security Network без отправки статистических данных** или **Kaspersky Security Network с отправкой статистических данных**.
Я не принимаю условия настоящего Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите участвовать в Kaspersky Security Network. Вариант доступен, если в окне **Параметры Kaspersky Security Network** (см. стр. 235) вы выбрали вариант **Kaspersky Security Network без отправки статистических данных** или **Kaspersky Security Network с отправкой статистических данных**.

Положение о Kaspersky Private Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Private Security Network и принять его условия.

Таблица 47. Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите участвовать в Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Private Security Network.
Я не принимаю условия настоящего Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите участвовать в Kaspersky Security Network.

Контроль программ

Во время работы компонента Контроль программ Kaspersky Endpoint Security управляет запуском программ на компьютерах пользователей. Это позволяет снизить риск заражения компьютера, ограничивая доступ к программам. Запуск программ регулируется с помощью *правил контроля программ* (см. раздел "*О правилах контроля программ*" на стр. 193).

Для использования компонента требуется лицензия, которая включает эту функцию.

Контроль программ может работать в двух режимах:

- *Список запрещенных*. Режим, при котором программа Kaspersky Endpoint Security разрешает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ. Этот режим работы задачи Контроль программ настроен по умолчанию.
- *Список разрешенных*. Режим, при котором программа Kaspersky Endpoint Security запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ.

Таким образом, если правила контроля программ сформированы максимально полно, программа Kaspersky Endpoint Security запрещает запуск всех новых, не проверенных администратором локальной сети организации программ, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

Для каждого режима работы Контроля программ вы можете создать отдельные правила, а также выбрать действие, которое программа Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска программы: *применять правила* или *тестировать правила*.

Параметры Контроля программ описаны в таблице ниже.

Таблица 48. Параметры Контроля программ

Параметр	Описание
Включить Контроль программ	Флажок включает компонент Контроль программ. По умолчанию флажок снят.

Параметр	Описание
Действие при попытке запуска программы	Вы можете выбрать действие, которое программа Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска программы, удовлетворяющей настроенным правилам: • **Тестировать правила**. При выборе этого варианта программа Kaspersky Endpoint Security тестирует правила и формирует событие об обнаружении программ, удовлетворяющих правилам. • **Применять правила** (значение по умолчанию). При выборе этого варианта программа Kaspersky Endpoint Security применяет правила контроля программ и выполняет заданное в правилах действие.
Режим Контроля программ	Вы можете выбрать режим работы компонента Контроль программ: • **Список разрешенных**. При выборе этого варианта программа Kaspersky Endpoint Security запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ. • **Список запрещенных** (значение по умолчанию). При выборе этого варианта программа Kaspersky Endpoint Security разрешает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ.
Правила Контроля программ	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Правила Контроля программ** (см. раздел "Окно Правила Контроля программ" на стр. 237).

Окно Правила Контроля программ

Таблица **Правила Контроля программ** содержит правила, используемые компонентом Контроль программ. По умолчанию таблица правил контроля программ пустая.

Таблица 49. Параметры правил контроля программ

Параметр	Описание
Название категории	Название категории программ, которая используется в работе правила.
Статус	Статус работы правила контроля программ: • *Включено* – правило включено, Контроль программ применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля программ. • *Тест* – Контроль программ разрешает запуск программ, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих программ в отчете. Вы можете изменить статус правила в окне **Добавление правила** (см. раздел "Окно Добавление правила" на стр. 237).

Вы можете добавлять (см. раздел "Окно Добавление правила" на стр. 237), изменять и удалять правила контроля программ.

Окно Добавление правила

В этом окне вы можете настроить параметры создаваемого правила Контроля программ.

Таблица 50. Добавление правила Контроля программ

Параметр	Описание
Описание	Описание правила Контроля программ.
Статус правила	В раскрывающемся списке вы можете выбрать статус работы правила контроля программ: • *Включено* – правило включено, Контроль программ применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля программ. • *Тест* – Контроль программ разрешает запуск программ, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих программ в отчете.
Категория	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Категории Контроля программ** (см. раздел "Окно Категории Контроля программ" на стр. 238).
Список управления доступом	Таблица содержит список пользователей или групп пользователей, на которых распространяется правило контроля программ, и назначенные им типы доступа, и состоит из следующих граф: • **Имя оператора доступа** – пользователи или группы пользователей, на которых распространяется правило контроля программ. • **Доступ** – тип доступа: **Разрешать** доступ или **Блокировать** доступ. Вы можете добавлять, изменять и удалять операторов доступа (см. раздел "Окно Имя оператора доступа" на стр. 238).

Окно Категории Контроля программ

В этом окне вы можете добавить новую категорию или настроить параметры категории для правила Контроля программ.

Использование KL-категорий Kaspersky Security Center не поддерживается.

Таблица 51. Категории Контроля программ

Параметр	Описание
Название категории	Список добавленных категорий Контроля программ.
Добавить	При нажатии на кнопку запускается Мастер создания категорий Kaspersky Security Center. Следуйте указаниям мастера.
Изменить	При нажатии на кнопку открывается окно свойств категории, в котором вы можете изменить параметры категории.

Окно Имя оператора доступа

В этом окне вы можете настроить параметры создаваемого правила Контроля программ.

Таблица 52. Добавление правила Контроля программ

Параметр	Описание
Тип оператора доступа	Тип оператора доступа, на которого распространяется правило: **Пользователь** или **Группа**.
Имя пользователя или группы	Имя пользователя или название группы пользователей, на которых распространяется правило контроля программ.
Доступ	Тип доступа: **Разрешать** доступ или **Блокировать** доступ.

Защита от шифрования

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

Во время работы компонента Защита от шифрования программа Kaspersky Endpoint Security проверяет обращения удаленных компьютеров сети к файлам, расположенным в общих сетевых директориях защищаемого устройства. Если программа расценивает действия удаленного компьютера, получающего доступ к общим сетевым ресурсам, как вредоносное шифрование, она добавляет этот компьютер в список недоверенных устройств и запрещает ему доступ к общим сетевым директориям. Программа не расценивает действия как вредоносное шифрование, если активность обнаружена в директориях, которые не входят в область защиты компонента Защита от шифрования.

Для использования компонента требуется лицензия, которая включает эту функцию.

Для корректной работы компонента Защита от шифрования требуется, чтобы в операционной системе была установлена хотя бы одна из служб: Samba или NFS. Для службы NFS требуется, чтобы был установлен пакет rpcbind.

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

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

Таблица 53. Параметры Защиты от шифрования

Параметр	Описание
Включить Защиту от шифрования	Флажок включает или выключает защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования. По умолчанию флажок установлен.
Области защиты	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки (см. раздел "Окно Области проверки" на стр. 220) и параметры защиты (см. раздел "Окно Параметры защиты" на стр. 241).

Параметр	Описание
Исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске** (см. раздел "Окно Исключения по маске" на стр. 227). В этом окне вы можете настроить исключение объектов из проверки по маске имени.

Окно Области проверки

Таблица содержит области проверки. Программа проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Таблица 54. Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли программа эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно <Название области проверки>

В этом окне можно добавить или настроить область защиты компонента Защита от шифрования.

Таблица 55. Параметры области защиты

Параметр	Описание
Название области	Поле ввода названия области защиты. Это название будет отображаться в таблице окна **Области проверки** (см. раздел "Окно Области проверки" на стр. 220). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область защиты во время работы компонента. Если флажок снят, программа не обрабатывает эту область защиты во время работы компонента. В дальнейшем вы можете включить эту область в параметры работы компонента, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область защиты. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы компонента Защита от шифрования. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Параметры защиты

Таблица 56. Параметры защиты

Параметр	Описание
Включить блокирование недоверенных устройств	Флажок включает или выключает блокировку недоверенных устройств. По умолчанию флажок установлен.
Блокировать недоверенное устройство на (мин)	Поле, в котором вы можете указать длительность блокировки недоверенного устройства в минутах. По истечении указанного времени Kaspersky Endpoint Security удаляет недоверенные устройства из списка заблокированных. Доступ устройства к сетевым файловым ресурсам восстанавливается автоматически после его удаления из списка недоверенных устройств. Изменение параметра не влияет на длительность блокировки ранее заблокированных скомпрометированных устройств. Длительность блокировки не является динамическим значением и рассчитывается в момент блокировки. Доступные значения: целые числа от `1` до `4294967295`. Значение по умолчанию: `30`.

Окно Области исключения

Таблица содержит области исключения из проверки. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 57. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, применяется ли это исключение в работе программы.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Название области исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Таблица 58. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы программы. Если флажок установлен, программа исключает эту область во время работы. Если флажок снят, программа включает эту область во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все смонтированные** – все смонтированные директории.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательский** – ресурсы файловой системы компьютера, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. По умолчанию указан путь **/** – программа исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые программа исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

kaspersky

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Программа не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска.

Примеры:

Маска `*.txt` – все текстовые файлы.

Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Контроль целостности системы

Контроль целостности системы предназначен для отслеживания действий, выполняемых с файлами и директориями в области мониторинга, указанной в параметрах работы компонента. Вы можете использовать Контроль целостности системы, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом сервере.

Для использования компонента требуется лицензия, которая включает эту функцию.

Таблица 59. Параметры Контроля целостности системы

Параметр	Описание
Включить Контроль целостности системы	Флажок включает или выключает Контроль целостности системы. По умолчанию флажок снят.
Области мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки** (см. раздел "Окно области проверки" на стр. 246).
Исключения из мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения** (см. раздел "Окно Области исключения" на стр. 246)
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске** (см. раздел "Окно Исключения по маске" на стр. 247).

Окно Области проверки

Таблица содержит области мониторинга для задачи Контроль целостности системы. Программа контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/).

Таблица 60. Параметры области мониторинга Контроля целостности системы

Параметр	Описание
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли программа эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно <Название области проверки>

В этом окне вы можете добавить или настроить области мониторинга для компонента Контроль целостности системы.

Таблица 61. Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна **Области проверки** (см. раздел "Области мониторинга" на стр. 322). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область мониторинга во время работы. Если флажок снят, программа не обрабатывает эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Поле не должно быть пустым. По умолчанию указан путь `/opt/kaspersky/kesl`.
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Области исключения

Таблица содержит области исключения из мониторинга для компонента Контроль целостности системы. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 62. Параметры области исключения из мониторинга Контроля целостности системы

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли программа эту область из мониторинга при работе компонента.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Название области исключения>

В этом окне вы можете добавить или настроить область исключения из мониторинга для компонента Контроль целостности системы.

Таблица 63. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения** (см. раздел "Окно Области исключения" на стр. 246). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы программы. Если флажок установлен, программа исключает эту область из мониторинга во время работы компонента. Если флажок снят, программа отслеживает эту область во время работы компонента. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Поле не должно быть пустым. По умолчанию указан путь */* – программа исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые программа исключает из мониторинга. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Программа не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент.

Контроль устройств

Во время работы компонента Контроль устройств программа Kaspersky Endpoint Security управляет доступом пользователей к устройствам, установленным на компьютере или подключенным к нему (например, к жестким дискам, устройствам чтения смарт-карт, модулям Wi-Fi). Это позволяет защитить компьютер от заражения при подключении таких устройств, а также предотвратить потерю и утечку данных. Контроль устройств управляет доступом пользователей к устройствам с помощью правил доступа.

Если устройство, заблокированное Контролем устройств, подключено к компьютеру, программа запрещает пользователям доступ к этому устройству и выводит уведомление.

Таблица 64. Параметры Контроля устройств

Параметр	Описание
Включить Контроль устройств	Флажок включает или выключает компонент Контроль устройств. По умолчанию флажок установлен.
Доверенные устройства	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные устройства**. В этом окне вы можете добавлять устройства в список доверенных устройств по идентификатору устройства или выбрав их из списка существующих на компьютере устройств.
Действие Контроля устройств	Действие, выполняемое программой при попытке доступа к устройству, к которому запрещен доступ в соответствии с правилами Контроля устройств: • **Применять правила**. При выборе этого варианта программа Kaspersky Endpoint Security применяет правила доступа и выполняет заданное в правилах действие. • **Тестировать правила**. При выборе этого варианта программа Kaspersky Endpoint Security тестирует правила доступа и формирует событие об обнаружении попытки доступа к устройству.
Параметры Контроля устройств	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить правила доступа для различных типов устройств и правила доступа к шинам подключения.

kaspersky

Анализ поведения

По умолчанию компонент Анализ поведения запускается при старте программы Kaspersky Endpoint Security и контролирует вредоносную активность в операционной системе. При обнаружении вредоносной активности программа Kaspersky Endpoint Security может завершать процесс программы, осуществляющей вредоносную активность.

Таблица 65. Параметры компонента Анализ поведения

Параметр	Описание
Включить Анализ поведения	Флажок включает или выключает компонент Анализ поведения. По умолчанию флажок установлен.
Режим работы компонента Анализ поведения	Вы можете выбрать действие, которое программа будет выполнять при обнаружении вредоносной активности в операционной системе: • **Блокировать** программу, осуществляющую вредоносную активность (значение по умолчанию). Kaspersky Endpoint Security завершает процесс программы и записывает в журнал информацию об обнаруженной вредоносной активности. • **Информировать** пользователя. Kaspersky Endpoint Security не завершает процесс, осуществляющий вредоносную активность, только регистрирует обнаружение вредоносной активности в журнале событий.
Использовать исключения по процессам	Включает или выключает использование исключений по процессам в работе компонента Анализ поведения. По умолчанию флажок снят. По кнопке **Настроить** открывается окно **Исключения по процессам** (см. раздел "Окно Исключения по процессам" на стр. 248). В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса из проверки. По умолчанию таблица пуста.

Таблица 66. Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, применяется ли это исключение в работе программы.

Элементы в таблице можно добавлять, изменять и удалять (см. раздел "Окно Доверенный процесс" на стр. 248).

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Таблица 67. Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Исключения по процессам** (см. раздел "Окно Исключения по процессам" на стр. 248).
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки. Поле ввода не должно быть пустым.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром **Путь к исключаемому процессу**. По умолчанию флажок снят.
Использовать эту область	Флажок включает или выключает исключение этой области из проверки во время работы программы. Если флажок установлен, программа исключает эту область во время работы. Если флажок снят, программа включает эту область во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.

Управление задачами

Вы можете настроить возможность просмотра и управления задачами программы Kaspersky Endpoint Security на управляемых устройствах.

Таблица 68. Параметры управления задачами

Параметр	Описание
Разрешить пользователям просмотр и управление локальными задачами	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в Kaspersky Endpoint Security, и управление этими задачами на управляемых устройствах. По умолчанию флажок снят.
Разрешить пользователям просмотр и управление задачами, созданными через KSC	Флажок разрешает или запрещает пользователям просмотр задач, созданных через Kaspersky Security Center, и управление этими задачами на управляемых устройствах. По умолчанию флажок снят.

Проверка съемных дисков

Во время выполнения задачи Проверка съемных дисков программа проверяет подключенное устройство и его загрузочные секторы на вирусы и другие вредоносные программы. Выполняется проверка следующих съемных дисков: CD/DVD-приводов, Blu-ray дисков, флеш-накопителей (включая USB-модемы), внешних жестких дисков и дискет.

Таблица 69. Параметры задачи Проверка съемных дисков

Параметр	Описание
Включить проверку съемных дисков при подключении к устройству	Флажок включает или выключает проверку съемных дисков при подключении их к устройству. По умолчанию флажок снят.
Действие при подключении съемного диска	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять программа при подключении к компьютеру съемных дисков: • **Не проверять** съемные диски при подключении (значение по умолчанию). • **Быстрая проверка** – проверять на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков) только файлы определенных типов и не распаковывать составные объекты. При быстрой проверке используются параметры, заданные по умолчанию для компонента Защита от файловых угроз (см. стр. 219). • **Подробная проверка** – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При подробной проверке используются параметры, заданные по умолчанию для задачи Антивирусная проверка (см. стр. 265).
Действие при подключении CD/DVD-привода	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять программа при подключении к компьютеру CD/DVD-приводов и Blu-ray дисков: • **Не проверять** CD/DVD-приводы и Blu-ray диски при подключении (значение по умолчанию). • **Быстрая проверка** – проверять только файлы определенных типов на CD/DVD-приводах и Blu-ray дисках. При быстрой проверке используются параметры, заданные по умолчанию для компонента Защита от файловых угроз (см. стр. 219). • **Подробная проверка** – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. При подробной проверке используются параметры, заданные по умолчанию для задачи Антивирусная проверка (см. стр. 265).
Блокировать доступ к съемному диску во время проверки	Флажок включает или выключает блокировку файлов на подключенном диске во время выполнения задачи Проверка съемных дисков. По умолчанию флажок снят.

Параметры прокси-сервера

Вы можете настроить параметры прокси-сервера, если доступ пользователей клиентских компьютеров в интернет осуществляется через прокси-сервер. Программа Kaspersky Endpoint Security может использовать прокси-сервер для подключения к серверам "Лаборатории Касперского", например, при обновлении баз и модулей программы или при взаимодействии с Kaspersky Security Network.

Таблица 70. Параметры прокси-сервера

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, прокси-сервер не используется в работе программы Kaspersky Endpoint Security.
Использовать параметры указанного прокси-сервера	Если выбран этот вариант, программа Kaspersky Endpoint Security использует указанные параметры прокси-сервера.
Адрес и порт	Поля для ввода IP-адреса или доменного имени прокси-сервера и порта прокси-сервера. Порт по умолчанию: `3128`. Поля доступны, если выбран вариант **Использовать параметры указанного прокси-сервера**.
Использовать имя пользователя и пароль	Флажок включает или выключает аутентификацию с помощью имени пользователя и пароля при доступе к прокси-серверу. Флажок доступен, если выбран вариант **Использовать параметры указанного прокси-сервера**. По умолчанию флажок снят. Для подключения через HTTP-прокси-сервер рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.
Имя пользователя	Поле ввода имени пользователя для его аутентификации на прокси-сервере. Поле ввода доступно, если установлен флажок **Использовать имя пользователя и пароль**.
Пароль	Поле для ввода пароля пользователя для авторизации на прокси-сервере. При нажатии на кнопку **Показать** пароль пользователя отображается в поле **Пароль** в открытом виде. По умолчанию пароль пользователя скрыт и отображается в виде точек. Поле ввода и кнопка доступны, если установлен флажок **Использовать имя пользователя и пароль**.
Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы	Флажок включает или выключает использование Kaspersky Security Center в качестве прокси-сервера при активации программы. Если флажок установлен, программа Kaspersky Endpoint Security использует Kaspersky Security Center в качестве прокси-сервера при активации программы. По умолчанию флажок снят.

Параметры программы

Вы можете настроить общие параметры программы Kaspersky Endpoint Security.

Таблица 71. Общие параметры программы

Параметр	Описание
Обнаруживать легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройствам или данным	Флажок включает или выключает обнаружение легальных программ, через которые злоумышленники могут навредить компьютеру или данным пользователя. По умолчанию флажок снят.
Уведомления о событиях	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Параметры уведомлений**. В этом окне вы можете выбрать события, для которых программа будет записывать уведомления в журнал операционной системы (syslog). Установите флажок около каждого типа события, для которого вы хотите отправлять уведомления. Также вы можете установить флажок около уровня важности событий (*Критические события*, *Информационные сообщения*, *Отказы функционирования*, *Предупреждения*). В этом случае флажки будут установлены автоматически около каждого типа событий, входящего в группу выбранного уровня важности. По умолчанию все флажки сняты.
Блокировать файлы во время проверки	Флажок включает или выключает блокировку файлов, в которых обнаружены угрозы во время проверки компонентом Защита от файловых угроз. Этот параметр также влияет на работу компонентов Защита от шифрования, Контроль устройств и задачи Проверка съемных дисков. По умолчанию флажок установлен.

Параметры проверки контейнеров

Вы можете настроить параметры проверки пространств имен и контейнеров программой Kaspersky Endpoint Security.

Таблица 72. Параметры проверки контейнеров

Параметр	Описание
Включить проверку пространств имен и контейнеров	Флажок включает или выключает проверку пространств имен и контейнеров. По умолчанию флажок установлен.

Параметр	Описание
Действие с контейнером при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое программа будет выполнять над контейнером при обнаружении зараженного объекта: • **Пропустить контейнер** – при обнаружении зараженного объекта программа не выполняет никаких действий над контейнером. • **Остановить контейнер** – при обнаружении зараженного объекта программа останавливает контейнер. • **Остановить, если не удалось вылечить** (значение по умолчанию) – если не удалось вылечить зараженный объект, программа останавливает контейнер.
Параметры проверки контейнеров	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Параметры проверки контейнеров** (см. раздел "**Окно Параметры проверки контейнеров**" на стр. 253), в котором вы можете настроить параметры проверки контейнеров.

Окно Параметры проверки контейнеров

В этом окне вы можете настроить параметры проверки контейнеров программой Kaspersky Endpoint Security.

Таблица 73. Параметры проверки контейнеров

Параметр	Описание
Использовать Docker	Флажок включает или выключает использование среды Docker. По умолчанию флажок установлен.
Путь Docker-сокета	Поле ввода пути или URI (универсальный идентификатор ресурса) Docker-сокета. Значение по умолчанию – /var/run/docker.sock.
Использовать CRI-O	Флажок включает или выключает использование среды CRI-O. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к конфигурационному файлу CRI-O. Значение по умолчанию: /etc/crio/crio.conf.
Использовать Podman	Флажок включает или выключает использование утилиты Podman. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты Podman. Значение по умолчанию: /usr/bin/podman
Корневая директория	Поле ввода пути к корневой директории хранилища контейнеров.
Использовать runc	Флажок включает или выключает использование утилиты runc. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты runc. Значение по умолчанию: /usr/bin/runc

Параметр	Описание
Корневая директория	Поле ввода пути к корневой директории хранилища состояний контейнеров. Значение по умолчанию: /run/runc-ctrs.

Проверка съемных дисков

Интеграция программы Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response (MDR) обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.

Таблица 74. Параметры Managed Detection and Response

Параметр	Описание
Включить Managed Detection and Response	Флажок включает интеграцию программы Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response. По умолчанию флажок снят.
Загрузить	По нажатию на кнопку открывается стандартное окно Microsoft Windows, в котором вы можете выбрать конфигурационный файл BLOB.

Параметры сети

Вы можете настроить параметры проверки зашифрованных соединений. Эти параметры используются в работе компонента Защита от веб-угроз (см. стр. 230).

При изменении параметров проверки зашифрованных соединений программа формирует событие *Параметры сети изменены (Network settings changed)*.

Таблица 75. Параметры сети

Параметр	Описание
Включить проверку зашифрованных соединений	Флажок включает или выключает проверку зашифрованных соединений. По умолчанию флажок установлен.
Действие при обнаружении недоверенного сертификата	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять программа при обнаружении недоверенного сертификата: • **Разрешить** подключение к домену с недоверенным сертификатом (значение по умолчанию). • **Блокировать** подключение к домену с недоверенным сертификатом.

Параметр	Описание
Действие при обнаружении ошибки проверки зашифрованного соединения	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять программа при возникновении ошибки во время проверки зашифрованных соединений: • **Добавить в исключения** (значение по умолчанию) – добавить домен, вызвавший ошибку, в список доменов с ошибками при проверке и не проверять зашифрованный сетевой трафик при посещении этого домена. • **Отключить** – заблокировать сетевое подключение.
Политика проверки сертификатов	В раскрывающемся списке вы можете выбрать способ проверки сертификатов программой: • **Локальная проверка** – программа не использует интернет для проверки сертификата. • **Полная проверка** (значение по умолчанию) – программа использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.
Доверенные домены	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные домены** (см. раздел "Окно Доверенные домены" на стр. 255). В этом окне вы можете настроить список имен доверенных доменов.
Доверенные сертификаты	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные сертификаты** (см. раздел "Окно Доверенные сертификаты" на стр. 255). В этом окне вы можете настроить список доверенных сертификатов, который используется при проверке зашифрованных соединений.
Параметры сетевых портов	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Сетевые порты** (см. раздел "Окно Сетевые порты" на стр. 256).

Окно Доверенные домены

Список содержит доменные имена и маски доменных имен, которые будут исключены из проверки зашифрованных соединений. По умолчанию список пуст.

Вы можете добавлять, изменять и удалять домены в списке доверенных доменов.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно Доверенные сертификаты

Вы можете настроить список сертификатов, которые программа Kaspersky Endpoint Security будет считать доверенными. Список доверенных сертификатов используется при проверке зашифрованных соединений.

Для каждого сертификата отображаются следующие сведения:

- субъект сертификата;
- серийный номер;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- отпечаток сертификата SHA-256.

По умолчанию список сертификатов пуст. Вы можете добавлять (см. раздел "Окно Добавление доверенного сертификата" на стр. 256) и удалять сертификаты.

Окно Добавление доверенного сертификата

В этом окне вы можете добавить сертификат в список доверенных сертификатов одним из следующих способов:

- Указать путь к файлу сертификата. По кнопке **Обзор** открывается стандартное окно для выбора файла. Укажите путь к файлу формата DER или PEM, содержащему сертификат.
- Скопировать содержимое файла сертификата в поле **Ввести данные сертификата**.

Окно Сетевые порты

Таблица 76. Параметры сетевых портов

Параметр	Описание
Отслеживать все сетевые порты	Если выбран этот вариант, программа проверяет все сетевые порты.
Отслеживать только указанные порты	Если выбран этот вариант, программа проверяет только сетевые порты, указанные в таблице. Этот вариант выбран по умолчанию.
Параметры сетевых портов	Таблица содержит сетевые порты, которые будет проверять программа, если выбран вариант **Отслеживать только указанные порты**. Таблица содержит две графы: • **Порт** – контролируемый порт. • **Описание** – описание контролируемого порта. По умолчанию в таблице отображается список сетевых портов, обычно используемых для передачи почтового и сетевого трафика. Список сетевых портов входит в пакет программы. Элементы в таблице можно добавлять, изменять и удалять.

kaspersky

Глобальные исключения

Глобальные исключения позволяют задать точки монтирования, которые будут исключены из проверки компонентами программы, использующими перехватчик файловых операций (Защита от файловых угроз и Защита от шифрования).

Таблица 77. Параметры глобальных исключений

Параметр	Описание
Исключенные точки монтирования	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключенные точки монтирования** (см. стр. 257).

Исключенные точки монтирования

Список содержит пути к исключенным точкам монтирования. По умолчанию список пуст.

Элементы в списке можно добавлять, изменять и удалять (см. раздел "Путь к точке монтирования" на стр. 257).

Путь к точке монтирования

Таблица 78. Параметры точки монтирования

Параметр	Описание
Файловая система, протокол доступа и путь	Блок параметров позволяет задать расположение точки монтирования. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные директории. • **Смонтированная** – удаленные директории, смонтированные на компьютере по протоколу Samba или NFS. • **Все смонтированные** – все удаленные директории, смонтированные на компьютере по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательская** – все ресурсы файловой системы компьютера, указанной в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в исключения из проверки. Для указания пути можно использовать маски.

Параметр	Описание
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.

Исключение памяти процессов

Вы можете настраивать исключения из проверки памяти процессов. Программа не будет проверять память указанных процессов.

Вы можете сформировать список исключений в окне (см. раздел "Окно Исключение памяти процессов из проверки" на стр. 258), которое открывается по кнопке **Настроить** в блоке **Исключение памяти процессов из проверки**.

Окно Исключение памяти процессов из проверки

Список содержит пути к процессам, которые Kaspersky Endpoint Security исключает из проверки памяти процессов. По умолчанию список пуст.

Элементы в списке можно добавлять, изменять и удалять.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете ввести полный путь к процессу. Kaspersky Endpoint Security исключает из проверки память указанного процесса.

При нажатии на кнопку **Изменить** открывается окно, в котором вы можете изменить путь к процессу. Kaspersky Endpoint Security исключает из проверки память указанного процесса.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранный путь к процессу из списка. Кнопка доступна, если в списке выбран хотя бы один путь к процессу.

Параметры Хранилища

Хранилище – это список резервных копий файлов, которые были удалены или изменены в процессе лечения. Резервная копия – копия файла, которая создается при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности. По умолчанию Хранилище расположено в директории /var/opt/kaspersky/kesl/common/objects-backup/. Файлы в Хранилище могут содержать персональные данные. Для доступа к файлам в Хранилище требуются root-права.

Таблица 79. Параметры Хранилища

Параметр	Описание
Информировать о необработанных файлах	Флажок включает или выключает отправку уведомлений о необработанных во время проверки файлах на Сервер администрирования. По умолчанию флажок установлен.
Информировать об установленных устройствах	Флажок включает или выключает передачу на Сервер администрирования информации об устройствах, установленных на вашем компьютере. По умолчанию флажок установлен.
Информировать о файлах в Хранилище	Переключатель включает или выключает отправку уведомлений о файлах в Хранилище на Сервер администрирования. По умолчанию флажок установлен.
Хранить объекты не более (дней)	Поле ввода для указания периода хранения объектов в Хранилище. Доступные значения: `0–3653`. Значение по умолчанию: `90`. Если задано значение `0`, период хранения объектов в Хранилище не ограничен.
Максимальный размер Хранилища (МБ)	Поле ввода для указания максимального размера Хранилища (в мегабайтах). Доступные значения: `0–999999`. Значение по умолчанию: `0` (размер Хранилища не ограничен).

Управление задачами в Консоли администрирования Kaspersky Security Center

Для работы с программой Kaspersky Endpoint Security через Консоль администрирования Kaspersky Security Center вы можете создавать следующие задачи:

- локальные задачи, определенные для отдельного компьютера;
- групповые задачи, определенные для компьютеров, входящих в группы администрирования;
- задачи для набора компьютеров, не входящих в группы администрирования.

Задачи для наборов компьютеров выполняются только на компьютерах, указанных в параметрах задачи. Если в выборку компьютеров, для которой 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 задачи следующих типов:

- **Антивирусная проверка** (см. стр. 265). Во время выполнения задачи программа проверяет области компьютера, указанные в параметрах задачи, на вирусы и другие вредоносные программы.
- **Добавление ключа** (см. стр. 271). Во время выполнения задачи программа добавляет ключ, в том числе резервный, для активации программы.
- **Инвентаризация** (см. стр. 272). Во время выполнения задачи программа получает информацию обо всех исполняемых файлах программ, хранящихся на компьютерах.

- **Обновление** (см. стр. 275). Во время выполнения задачи программа обновляет базы в соответствии с настроенными параметрами обновления.
- **Откат обновления баз** (см. стр. 277). Во время выполнения задачи программа откатывает последнее обновление баз.
- **Проверка важных областей** (см. стр. 277). Во время выполнения задачи программа проверяет загрузочные секторы, объекты автозапуска, память процессов и память ядра.
- **Проверка контейнеров** (см. стр. 283). Во время выполнения задачи программа проверяет контейнеры и образы на вирусы и другие вредоносные объекты.
- **Проверка целостности системы** (см. стр. 288). Во время выполнения задачи программа определяет изменение каждого объекта путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.

Вы можете выполнять следующие действия над задачами:

- Запускать, останавливать, приостанавливать и возобновлять (см. раздел "Запуск, остановка, приостановка и возобновление выполнения задачи вручную" на стр. 262) выполнение задач.

  Задачу **Обновление** невозможно приостановить и возобновить, ее можно только запустить или остановить.
- Создавать новые задачи.
- Изменять параметры задач.

  Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения. Кроме того, некоторые параметры могут быть недоступны для настройки и использования в сертифицированной версии программы.
- Сравнивать версии задач в окне свойств задачи в разделе **История ревизий**.

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

В этом разделе

Создание локальной задачи

► *Чтобы создать локальную задачу:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите создать локальную задачу.
5. Правой клавишей мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.

   Откроется окно свойств компьютера.
6. Выберите раздел **Задачи**.
7. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания задачи.
8. Следуйте указаниям Мастера создания задачи.

Создание групповой задачи

► *Чтобы создать групповую задачу:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** в дереве Консоли администрирования.
3. Нажмите на кнопку **Новая задача**.

   Запустится Мастер создания задачи.
4. Следуйте указаниям Мастера создания задачи.

Создание задачи для набора устройств

► *Чтобы создать задачу для набора устройств:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** в дереве Консоли администрирования.
3. Нажмите на кнопку **Новая задача**.

   Запустится Мастер создания задачи.
4. Следуйте указаниям Мастера создания задачи.
5. В окне мастера **Выбор устройств, которым будет назначена задача** нажмите на кнопку **Назначить задачу выборке устройств**.
6. В следующем окне мастера нажмите на кнопку **Обзор**.

   Откроется окно **Выборка устройств**.

7. Выберите нужное устройство и нажмите на кнопку **ОК** в окне **Выборка устройств**.
8. Следуйте указаниям Мастера создания задачи.

Запуск, остановка, приостановка и возобновление выполнения задачи вручную

Если на клиентском компьютере запущена программа (см. раздел "Запуск и остановка программы на клиентском компьютере" на стр. 211) Kaspersky Endpoint Security, вы можете запустить / остановить / приостановить / возобновить выполнение задачи на этом клиентском компьютере через Kaspersky Security Center. Если программа Kaspersky Endpoint Security остановлена, выполнение запущенных задач прекращается, а управлять запуском, остановкой, приостановкой и возобновлением задач через Kaspersky Security Center становится невозможно.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение локальной задачи:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, на котором вы хотите запустить / остановить / приостановить / возобновить выполнение локальной задачи.
5. Выберите пункт **Свойства** в контекстном меню компьютера.

   Откроется окно свойств компьютера.
6. Выберите раздел **Задачи**.

   В правой части окна отобразится список локальных задач.
7. Выберите локальную задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
8. Выполните одно из следующих действий:
   - Правой клавишей мыши откройте контекстное меню локальной задачи. Выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.
   - Нажмите на кнопку / справа от списка локальных задач, чтобы запустить или остановить локальную задачу.
   - Нажмите на кнопку **Свойства** под списком локальных задач. Откроется окно **Свойства: <Название локальной задачи>**. В окне **Свойства: <Название локальной задачи>** на закладке **Общие** нажмите на кнопку **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение групповой задачи:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите запустить / остановить / приостановить / возобновить выполнение групповой задачи.
3. В рабочей области выберите закладку **Задачи**.

   В правой части окна отобразится список групповых задач.
4. В списке групповых задач выберите групповую задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
5. Правой клавишей мыши откройте контекстное меню групповой задачи. Выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

Изменение параметров локальной задачи

► *Чтобы изменить параметры локальной задачи:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите настроить параметры программы.
5. Правой клавишей мыши откройте контекстное меню компьютера и выберите пункт **Свойства**.

   Откроется окно свойств компьютера.
6. Выберите раздел **Задачи**.

   В правой части окна отобразится список локальных задач.
7. Выберите в списке локальных задач нужную локальную задачу.
8. Выполните одно из следующих действий:
   - Правой клавишей мыши откройте контекстное меню задачи и выберите пункт **Свойства**.
   - Нажмите на кнопку **Свойства**.

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

Количество и содержимое разделов зависит от типа выбранной задачи. Содержимое разделов **Общие**, **Уведомления**, **Расписание** и **История ревизий** одинаковое для всех задач. Более подробное описание этих разделов приведено в документации к Kaspersky Security Center.

Изменение параметров групповой задачи

► *Чтобы изменить параметры групповой задачи:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием нужной группы администрирования.
3. В рабочей области выберите закладку **Задачи**.
4. В нижней части панели задач отобразится список групповых задач.
5. Выберите в списке групповых задач нужную групповую задачу.
6. Правой клавишей мыши откройте контекстное меню задачи и выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название групповой задачи>**.
7. Измените параметры групповой задачи.
8. В окне **Свойства: <Название групповой задачи>** нажмите на кнопку **ОК**, чтобы сохранить изменения.

Количество и содержимое разделов зависит от типа выбранной задачи. Содержимое разделов **Общие**, **Уведомления**, **Расписание** и **История ревизий** одинаковое для всех задач. Более подробное описание этих разделов приведено в документации к Kaspersky Security Center.

Изменение параметров задачи для набора устройств

► *Чтобы изменить параметры задачи для набора устройств:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Задачи** дерева Консоли администрирования выберите задачу для набора устройств, параметры которой вы хотите изменить.
3. В контекстном меню задачи выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название задачи>**.
4. Измените параметры задачи для набора устройств.
5. Нажмите на кнопку **ОК** в окне **Свойства: <Название задачи>**.

Количество и содержимое разделов зависит от типа выбранной задачи. Содержимое разделов **Общие**, **Уведомления**, **Расписание** и **История ревизий** одинаковое для всех задач. Более подробное описание этих разделов приведено в документации к Kaspersky Security Center.

Параметры задач

Вы можете создавать любое количество групповых задач, задач для набора компьютеров и локальных задач.

Набор параметров и значения по умолчанию для параметров задачи могут отличаться в зависимости от типа лицензии на программу (https://support.kaspersky.ru/15471). Кроме того, некоторые параметры могут быть недоступны для настройки и использования в сертифицированной версии программы.

kaspersky

В этом разделе

Антивирусная проверка

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

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

Во время полной проверки диска процессор компьютера будет занят. Рекомендуется запускать задачу полной проверки в нерабочее время.

Вы также можете создавать пользовательские задачи антивирусной проверки.

Таблица 80. Параметры задачи Антивирусная проверка

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки (см. раздел "Окно Области проверки" на стр. 220), параметры области проверки (см. раздел "Окно Параметры области проверки" на стр. 267) и параметры проверки (см. раздел "Окно Параметры проверки" на стр. 222).
Приоритет задачи	В этом блоке параметров вы можете выбрать приоритет задачи проверки: • **Низкий** – задача выполняется с низким приоритетом: не более 10% потребления ресурсов процессора. Выполнение задачи занимает больше времени, но программа выделяет ресурсы на выполнение других задач. • **Нормальный** (значение по умолчанию) – задача выполняется со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. • **Высокий** – задача выполняется с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.

Параметр	Описание
Действия над зараженными объектами	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действия над зараженными объектами** (см. раздел "Окно Действия над зараженными объектами" на стр. 271), в котором вы можете настроить действия, которые программа будет выполнять над обнаруженным зараженным объектом.

В разделе **Исключения** для задачи Антивирусная проверка вы также можете настроить области исключения (см. раздел "Окно Области исключения" на стр. 225), исключения по маске (см. раздел "Окно Исключения по маске" на стр. 227) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 227).

Окно Области проверки

Таблица содержит области проверки. Программа проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Таблица 81. Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли программа эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно <Название области проверки>

В этом окне вы можете добавить или настроить область проверки.

Таблица 82. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки** (см. раздел "Окно Области проверки" на стр. 220). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область проверки во время работы. Если флажок снят, программа не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. • **Смонтированная** – смонтированные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все смонтированные** – все смонтированные директории. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательская** – ресурсы файловой системы компьютера, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. По умолчанию указан путь **/** – программа проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, программа проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Параметры области проверки

В этом окне вы можете настроить параметры проверки во время работы задачи Антивирусная проверка. Программа позволяет проверять файлы, загрузочные секторы, память компьютера и объекты автозапуска.

Таблица 83. Параметры области проверки

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, программа проверяет файлы. Если флажок снят, программа не проверяет файлы. По умолчанию флажок установлен.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, программа проверяет загрузочные секторы. Если флажок снят, программа не проверяет загрузочные секторы. По умолчанию флажок снят.
Проверять память компьютера	Флажок включает или выключает проверку памяти компьютера. Если флажок установлен, программа проверяет память процессов и память ядра. Если флажок снят, программа не проверяет память процессов и память ядра. По умолчанию флажок снят.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, программа проверяет объекты автозапуска. Если флажок снят, программа не проверяет объекты автозапуска. По умолчанию флажок снят.
Устройства для проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки** (см. раздел "Окно Области проверки" на стр. 268), в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должна проверять программа. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки. Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Таблица 84. Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, программа проверяет архивы. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, программа не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, программа проверяет самораспаковывающиеся архивы. Если флажок снят, программа не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз программ Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, программа проверяет файлы почтовых баз. Если флажок снят, программа не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, программа проверяет сообщения в текстовом формате. Если флажок снят, программа не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Прервать проверку, если она длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки объекта в секундах. После истечения указанного времени программа прекращает проверку объекта. Доступные значения: `0–9999`. Если указано значение `0`, время проверки не ограничено. Значение по умолчанию: `0`.
Пропускать объекты размером более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0–999999`. Если установлено значение `0`, программа проверяет объекты любого размера. Значение по умолчанию: `0`.

Параметр	Описание
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, программа записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, программа не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, программа записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, программа не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, программа записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, программа не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, программа проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, программа проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.

Окно Действия над зараженными объектами

В этом окне вы можете настроить действия, которые программа Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Таблица 85. Действия над зараженными объектами

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое программа будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет сохранена в хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое программа будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет сохранена в хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).

Добавление ключа

С помощью задачи Добавление ключа вы можете добавить ключ для активации программы Kaspersky Endpoint Security.

Таблица 86. Параметры задачи Добавление ключа

Параметр	Описание
Использовать ключ в качестве резервного	Флажок включает или выключает использование ключа в качестве резервного. Если флажок установлен, программа использует ключ в качестве резервного. Если флажок снят, программа использует ключ в качестве активного. По умолчанию флажок снят. Флажок недоступен, если вы добавляете ключ для пробной лицензии или ключ по подписке. Ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве резервного ключа.
Добавить	При нажатии на кнопку открывается окно **Хранилище ключей Kaspersky Security Center** (см. раздел "Окно Хранилище ключей Kaspersky Security Center" на стр. 272). В этом окне вы можете выбрать ключ, ранее добавленный в хранилище ключей Kaspersky Security Center, а также добавить ключ в хранилище ключей Kaspersky Security Center.

Параметр	Описание
Информация о лицензии	В этом блоке приведены данные о ключе и связанной с ним лицензии: • **Ключ** – уникальная буквенно-цифровая последовательность. Вы можете использовать программу только при наличии в ней ключа. • **Тип лицензии** – пробная, коммерческая или коммерческая (подписка). • **Срок действия лицензии** – количество дней, в течение которых возможно использование программы, активированной путем добавления этого ключа (например, 365 дней). Информация не отображается, если вы используете программу по подписке. • **Действует до** – дата и время окончания срока использования программы, активированной путем добавления этого ключа, в формате UTC. Если вы используете программу по неограниченной подписке, дата окончания срока годности ключа не указывается. • **Ограничение** – максимальное количество устройств, которые программа может защищать. • **Название программы** – название программы, для активации которой вы добавляете ключ.

Окно Хранилище ключей Kaspersky Security Center

В этом окне вы можете выбрать ключ, ранее добавленный в хранилище ключей Kaspersky Security Center, а также добавить ключ в хранилище ключей Kaspersky Security Center.

Таблица 87. Параметры окна Хранилище ключей Kaspersky Security Center

Параметр	Описание
Добавить ключ	При нажатии на кнопку запускается мастер добавления лицензионного ключа. Ключ будет добавлен в хранилище ключей Kaspersky Security Center. После добавления ключа информация о нем будет отображаться в таблице ключей.
Таблица ключей	Таблица содержит ключи, добавленные в хранилище ключей Kaspersky Security Center, и состоит из следующих граф: • **Тип лицензии** – тип лицензии: пробная, коммерческая или коммерческая (подписка). • **Действует до** – дата окончания срока использования программы, активированной путем добавления этого ключа. • **Льготный период** – льготный период. • **Ограничение** – максимальное количество устройств, которые программа может защищать. • **Название программы** – название программы, для активации которой добавлен ключ. • **Ключ** – уникальная буквенно-цифровая последовательность.

Инвентаризация

Задача Инвентаризация позволяет получить информацию обо всех исполняемых файлах программ, хранящихся на компьютерах. Получение информации о программах, установленных на компьютерах, может быть полезно, например, для создания правил контроля программ (см. раздел "О правилах контроля программ" на стр. 193).

Для использования задачи требуется лицензия, которая включает эту функцию.

В базе данных Kaspersky Security Center может храниться информация о 150 000 обработанных файлов. При достижении этого количества записей новые файлы не будут обработаны. Для возобновления работы инвентаризации требуется удалить с компьютера, на котором установлена программа Kaspersky Endpoint Security, файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

Таблица 88. Параметры задачи Инвентаризация

Параметр	Описание
Создать золотой образ	Флажок включает или выключает создание категории программ "Golden Image" на основе списка программ, обнаруженных на компьютере задачей Инвентаризация. Если флажок установлен, то в правилах контроля программ (см. стр. 193) вы можете использовать категорию программ "Golden Image". По умолчанию флажок снят.
Проверять все исполняемые файлы	Флажок включает или выключает проверку исполняемых файлов. По умолчанию флажок установлен.
Проверять двоичные файлы	Флажок включает или выключает проверку двоичных файлов (с расширениями elf, java и pyc). По умолчанию флажок установлен.
Проверять скрипты	Флажок включает или выключает проверку скриптов. По умолчанию флажок установлен.
Области инвентаризации	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки** (см. раздел "Окно Области проверки" на стр. 220).
Приоритет задачи	В этом блоке параметров вы можете выбрать приоритет выполнения задачи: • **Низкий** – задача выполняется с низким приоритетом: не более 10% потребления ресурсов процессора. Выполнение задачи занимает больше времени, но программа выделяет ресурсы на выполнение других задач. • **Нормальный** (значение по умолчанию) – задача выполняется со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. • **Высокий** – задача выполняется с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.

В разделе **Области исключения** для задачи Инвентаризация вы можете также настроить области исключения из проверки (см. раздел "Окно Области исключения" на стр. 225).

Окно Области проверки

Таблица содержит области проверки. Программа проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки – /usr/bin.

Таблица 89. Параметры области проверки задачи Инвентаризация

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли программа эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно <Название области проверки>

В этом окне вы можете добавить или настроить область проверки для задачи Инвентаризация.

Таблица 90. Параметры области инвентаризации

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки** (см. раздел "Окно Области проверки" на стр. 220). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время выполнения задачи. Если флажок установлен, программа обрабатывает эту область проверки во время выполнения задачи. Если флажок снят, программа не обрабатывает эту область проверки во время выполнения задачи. В дальнейшем вы можете включить эту область в параметры задачи, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область проверки. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые программа проверяет во время выполнения задачи. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Области исключения

Таблица содержит области исключения из проверки. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 91. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, применяется ли это исключение в работе программы.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Название области исключения>

В этом окне вы можете добавить или настроить область исключения из проверки для задачи Инвентаризация.

Таблица 92. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения** (см. раздел "Окно Области исключения" на стр. 225). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время выполнения задачи. Если флажок установлен, Kaspersky Endpoint Security исключает эту область во время выполнения задачи. Если флажок снят, Kaspersky Endpoint Security включает эту область во время выполнения задачи. В дальнейшем вы можете исключить эту область из проверки, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения из инвентаризации. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые Kaspersky Endpoint Security исключает из проверки. Вы можете добавлять, изменять и удалять маски.

Обновление

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 программы. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули программы.

Источник обновлений – это ресурс, содержащий обновления баз и модулей программы Kaspersky Endpoint Security. Источником обновлений могут быть FTP-, HTTP- или HTTPS-серверы (например, серверы

обновлений Kaspersky Security Center и "Лаборатории Касперского") и локальные или сетевые директории, смонтированные пользователем.

Таблица 93. Параметры источников обновлений задачи Обновление

Параметр	Описание
Источник обновлений баз	Вы можете выбрать источник обновлений: • **Серверы обновлений "Лаборатории Касперского"**, на которых публикуются обновления баз для программ "Лаборатории Касперского" (значение по умолчанию). • **Сервер администрирования Kaspersky Security Center**. • **Другие источники в локальной или глобальной сети** – HTTP-, HTTPS- или FTP-серверы или директории на серверах локальной сети.
Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны	Флажок включает или выключает использование серверов обновлений "Лаборатории Касперского" в качестве источника обновлений, если выбранные источники обновлений недоступны. Флажок доступен, если выбран вариант **Другие источники в локальной или глобальной сети** или **Сервер администрирования Kaspersky Security Center**. По умолчанию флажок установлен.
Пользовательские источники обновлений	Таблица содержит список пользовательских источников обновлений баз. В процессе обновления программа обращается к источникам обновлений в том порядке, в котором эти ресурсы указаны в таблице. Таблица содержит следующие графы: • **Адрес источника** – HTTP-, HTTPS- или FTP-серверы или директории на серверах локальной сети. • **Статус** показывает, будет ли источник использоваться в задаче (**Используется** или **Не используется**). Вы можете изменить статус, установив или сняв флажок **Использовать этот источник** в окне **Источник обновлений**, которое открывается при нажатии на кнопку **Изменить**. Таблица доступна, если выбран вариант **Другие источники в локальной или глобальной сети**. Источники обновлений в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз. По умолчанию таблица пустая.

В разделе **Параметры** вы можете указать время ожидания ответа и параметры загрузки обновлений программы.

Таблица 94. Дополнительные параметры задачи Обновление

Параметр	Описание
Максимальное время ожидания ответа от источника обновлений (сек.)	Предельный период ожидания ответа на запрос программы от выбранного источника обновлений. При отсутствии ответа по истечении этого времени в журнал выполнения задач записывается событие о нарушении связи с источником обновлений. Доступные значения: `0–120` секунд. Если указано значение `0`, период ожидания ответа на запрос программы от выбранного источника не ограничен. Значение по умолчанию: `10` секунд.
Режим загрузки обновлений программы	В раскрывающемся списке вы можете выбрать режим обновления баз программы: • **Не загружать** файлы обновлений (значение по умолчанию). Обновить программу невозможно. • **Только загружать** файлы обновлений, но не устанавливать их на компьютеры пользователей. • **Загружать и устанавливать** файлы обновлений на компьютеры пользователей. Для сохранения сертифицированной конфигурации программы требуется установить значение параметра **Не загружать**.

Откат обновления баз

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

Каждый раз, когда пользователь запускает процесс обновления, программа Kaspersky Endpoint Security создает резервную копию текущих баз программы. Это позволяет при необходимости откатить базы программы до предыдущей версии.

Откат последнего обновления баз используется, например, если новая версия баз программы содержит недопустимые сигнатуры, что приводит к блокировке безопасных программ программой Kaspersky Endpoint Security.

Задача Откат обновления баз не имеет параметров.

Проверка важных областей

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

Таблица 95. Параметры задачи Проверка важных областей

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки (см. раздел "Окно Области проверки" на стр. 220), параметры области проверки (см. раздел "Окно Параметры области проверки" на стр. 267) и параметры проверки (см. раздел "Окно Параметры проверки" на стр. 222).
Приоритет задачи	В этом блоке параметров вы можете выбрать приоритет задачи проверки: • **Низкий** – задача выполняется с низким приоритетом: не более 10% потребления ресурсов процессора. Выполнение задачи занимает больше времени, но программа выделяет ресурсы на выполнение других задач. • **Нормальный** (значение по умолчанию) – задача выполняется со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. • **Высокий** – задача выполняется с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.
Действия над зараженными объектами	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действия над зараженными объектами** (см. раздел "Окно Действия над зараженными объектами" на стр. 271), в котором вы можете настроить действия, которые программа Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

В разделе **Исключения** для задачи Проверка важных областей вы также можете настроить области исключения (см. раздел "Окно Области исключения" на стр. 225), исключения по маске (см. раздел "Окно Исключения по маске" на стр. 227) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 227).

Окно Области проверки

Таблица содержит области проверки. Программа проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Таблица 96. Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли программа эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно <Название области проверки>

В этом окне вы можете добавить или настроить область проверки.

Таблица 97. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки** (см. раздел "Окно Области проверки" на стр. 220). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область проверки во время работы. Если флажок снят, программа не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. • **Смонтированная** – смонтированные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все смонтированные** – все смонтированные директории. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательская** – ресурсы файловой системы компьютера, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. По умолчанию указан путь **/** – программа проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, программа проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Параметры области проверки

В этом окне вы можете настроить параметры проверки во время работы задачи Проверка важных областей. Программа позволяет проверять файлы, загрузочные секторы, память компьютера и объекты автозапуска.

Таблица 98. Параметры области проверки

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, Kaspersky Endpoint Security проверяет файлы. Если флажок снят, Kaspersky Endpoint Security не проверяет файл. По умолчанию флажок снят.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, Kaspersky Endpoint Security проверяет загрузочные секторы. Если флажок снят, Kaspersky Endpoint Security не проверяет загрузочные секторы. По умолчанию флажок установлен.
Проверять память компьютера	Флажок включает или выключает проверку памяти компьютера. Если флажок установлен, Kaspersky Endpoint Security проверяет память процессов и память ядра. Если флажок снят, Kaspersky Endpoint Security не проверяет память процессов и память ядра. По умолчанию флажок установлен.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, Kaspersky Endpoint Security проверяет объекты автозапуска. Если флажок снят, Kaspersky Endpoint Security не проверяет объекты автозапуска. По умолчанию флажок установлен.
Устройства для проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки** (см. раздел "Окно Области проверки" на стр. 268), в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должна проверять программа. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки. Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Таблица 99. Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, программа проверяет архивы. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, программа не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, программа проверяет самораспаковывающиеся архивы. Если флажок снят, программа не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз программ Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, программа проверяет файлы почтовых баз. Если флажок снят, программа не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, программа проверяет сообщения в текстовом формате. Если флажок снят, программа не проверяет сообщения в текстовом формате. По умолчанию флажок снят.

Параметр	Описание
Прервать проверку, если она длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки объекта в секундах. После истечения указанного времени программа прекращает проверку объекта. Доступные значения: `0–9999`. Если указано значение `0`, время проверки не ограничено. Значение по умолчанию: `0`.
Пропускать объекты размером более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0–999999`. Если установлено значение `0`, программа проверяет объекты любого размера. Значение по умолчанию: `0`.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, программа записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, программа не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, программа записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, программа не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, программа записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, программа не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, программа проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, программа проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.

Параметр	Описание
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.

Окно Действия над зараженными объектами

В этом окне вы можете настроить действия, которые программа Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Таблица 100. Действия над зараженными объектами

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое программа будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет сохранена в хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое программа будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет сохранена в хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).

Проверка контейнеров

Во время работы задачи Проверка контейнеров программа проверяет контейнеры и образы на вирусы и вредоносные программы. Вы можете одновременно запустить несколько задач Проверка контейнеров.

Для использования задачи требуется лицензия, которая включает эту функцию.

Таблица 101. Параметры задачи Проверка контейнеров

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить параметры проверки контейнеров (см. раздел "Окно Параметры проверки контейнеров" на стр. 284) и общие параметры проверки (см. раздел "Окно Параметры проверки" на стр. 268).
Приоритет задачи	В этом разделе можно задать приоритет задачи проверки: • **Низкий** – задача выполняется с низким приоритетом: не более 10% потребления ресурсов процессора. Выполнение задачи занимает больше времени, но программа выделяет ресурсы на выполнение других задач. • **Нормальный** (значение по умолчанию) – задача выполняется со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. • **Высокий** – задача выполняется с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.
Действия над зараженными объектами	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действия над зараженными объектами** (см. раздел "Окно Действия над зараженными объектами" на стр. 271), в котором вы можете настроить действия, которые программа будет выполнять над обнаруженным зараженным объектом.

В разделе **Исключения** (см. стр. 288) для задачи Проверка контейнеров вы также можете настроить исключения по маске (см. раздел "Окно Исключения по маске" на стр. 227) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 227).

Окно Параметры проверки контейнеров

В этом окне вы можете настроить параметры проверки контейнеров и образов.

Таблица 102. Параметры проверки контейнеров и образов

Параметр	Описание
Проверять контейнеры	Флажок включает или выключает проверку контейнеров. Если флажок установлен, вы можете указать имя или маску имени проверяемых контейнеров. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых контейнеров. По умолчанию указана маска ***** – выполняется проверка всех контейнеров.
Действие при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое программа будет выполнять над контейнером при обнаружении зараженного объекта: • **Пропустить контейнер** – не выполнять никаких действий над контейнером при обнаружении зараженного объекта. • **Остановить контейнер** – остановить контейнер при обнаружении зараженного объекта. • **Остановить, если не удалось вылечить** (значение по умолчанию) – остановить контейнер, если не удалось вылечить зараженный объект или устранить угрозу.

Параметр	Описание
Проверять образы	Флажок включает или выключает проверку образов. Если флажок установлен, вы можете указать имя или маску имени проверяемых образов. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых образов. По умолчанию указана маска ***** – выполняется проверка всех образов.
Действие при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое программа будет выполнять над образом при обнаружении зараженного объекта: • **Пропустить образ** (значение по умолчанию) – не выполнять никаких действий над образом при обнаружении зараженного объекта. • **Удалить образ** при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.
Проверять каждый слой	Флажок включает или выключает проверку всех слоев образов и запущенных контейнеров. По умолчанию флажок снят.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Таблица 103. Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, программа проверяет архивы. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, программа не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, программа проверяет самораспаковывающиеся архивы. Если флажок снят, программа не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.

Параметр	Описание
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз программ Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, программа проверяет файлы почтовых баз. Если флажок снят, программа не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, программа проверяет сообщения в текстовом формате. Если флажок снят, программа не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Прервать проверку, если она длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки объекта в секундах. После истечения указанного времени программа прекращает проверку объекта. Доступные значения: `0–9999`. Если указано значение `0`, время проверки не ограничено. Значение по умолчанию: `0`.
Пропускать объекты размером более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0–999999`. Если установлено значение `0`, программа проверяет объекты любого размера. Значение по умолчанию: `0`.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, программа записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, программа не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, программа записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, программа не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.

Параметр	Описание
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, программа записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, программа не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, программа проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, программа проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.

Окно Действия над зараженными объектами

В этом окне вы можете настроить действия, которые программа Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Таблица 104. Действия над зараженными объектами

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое программа будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет сохранена в хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое программа будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет сохранена в хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).

Раздел Исключения

Таблица 105. Параметры исключений из проверки

Блок параметров	Описание
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске** (см. раздел "Окно Исключения по маске" на стр. 227). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по названию угрозы** (см. раздел "Окно Исключения по названию угрозы" на стр. 227). В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Проверка целостности системы

В процессе выполнения задачи Проверка целостности системы (ODFIM) изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве *снимка состояния системы*.

Снимок состояния системы определяется во время первого выполнения задачи ODFIM на компьютере. Вы можете создать несколько задач ODFIM. Для каждой задачи ODFIM создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы относится к области мониторинга.

Если снимок состояния системы не соответствует области мониторинга, программа Kaspersky Endpoint Security создает событие о нарушении целостности системы.

Снимок состояния системы создается заново после завершения задачи ODFIM. Вы можете заново создать снимок состояния системы для задачи с помощью соответствующего параметра. Снимок состояния системы также создается при изменении параметров задачи, например, при добавлении новой области мониторинга. При следующем выполнении задачи снимок состояния системы формируется заново. Вы можете удалить снимок состояния системы, удалив соответствующую задачу ODFIM.

Задача ODFIM создает хранилище для снимков состояния системы на компьютере с установленным компонентом Контроль целостности системы.

Таблица 106. Параметры задачи Проверка целостности системы

Параметр	Описание
Обновлять снимок состояния системы при каждом запуске задачи	Флажок включает или выключает обновление снимка состояния системы при каждом запуске задачи Проверка целостности системы. По умолчанию флажок снят.
Использовать хеш (SHA-256) для проверки	Флажок включает или выключает использование хеша SHA-256 для задачи Проверка целостности системы. SHA-256 – это криптографическая хеш-функция, которая формирует 256-разрядное хеш-значение. 256-разрядное хеш-значение представляет собой последовательность из 64 шестнадцатеричных цифр. По умолчанию флажок снят.
Следить за директориями в областях мониторинга	Флажок включает или выключает проверку указанных директорий во время выполнения задачи Проверка целостности системы. По умолчанию флажок снят.
Следить за временем последнего доступа к файлу	Флажок включает или выключает отслеживание времени доступа к файлу во время выполнения задачи Проверка целостности системы. По умолчанию флажок снят.
Области мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки** (см. раздел "Окно Области проверки" на стр. 245).

В разделе **Области исключения** (см. стр. 292) для задачи Проверка целостности системы вы также можете настроить области исключения из мониторинга (см. раздел "Окно Области исключения" на стр. 246) и исключения по маске (см. раздел "Окно Исключения по маске" на стр. 247).

Окно Области проверки

Таблица содержит области мониторинга для задачи Контроль целостности системы. Программа контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/).

Таблица 107. Параметры области мониторинга Контроля целостности системы

Параметр	Описание
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли программа эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно <Название области проверки>

В этом окне вы можете добавить или настроить области мониторинга для компонента Контроль целостности системы.

Таблица 108. Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна **Области проверки** (см. раздел "Области мониторинга" на стр. 322). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область мониторинга во время работы. Если флажок снят, программа не обрабатывает эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Поле не должно быть пустым. По умолчанию указан путь `/opt/kaspersky/kesl`.
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Области исключения

Таблица содержит области исключения из мониторинга для компонента Контроль целостности системы. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 109. Параметры области исключения из мониторинга Контроля целостности системы

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли программа эту область из мониторинга при работе компонента.

Элементы в таблице можно добавлять, изменять и удалять.

Окно <Название области исключения>

В этом окне вы можете добавить или настроить область исключения из мониторинга для компонента Контроль целостности системы.

Таблица 110. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения** (см. раздел "Окно Области исключения" на стр. 246). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы программы. Если флажок установлен, программа исключает эту область из мониторинга во время работы компонента. Если флажок снят, программа отслеживает эту область во время работы компонента. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Поле не должно быть пустым. По умолчанию указан путь **/** – программа исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые программа исключает из мониторинга. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Раздел Области исключения

Таблица 111. Параметры исключений из проверки

Блок параметров	Описание
Исключения из мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения** (см. раздел "Окно Области исключения" на стр. 246). В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске** (см. раздел "Окно Исключения по маске" на стр. 247). В этом окне вы можете настроить исключение объектов из проверки по маске имени.

Проверка соединения с Сервером администрирования вручную. Утилита klnagchk

В комплект поставки Агента администрирования входит утилита klnagchk, предназначенная для проверки подключения к Серверу администрирования.

После установки Агента администрирования утилита сохраняется в директории /opt/kaspersky/klnagent/bin в 32-битной операционной системе и в директории /opt/kaspersky/klnagent64/bin в 64-битной операционной системе. В зависимости от используемых ключей Агент администрирования выполняет следующие действия при запуске:

- 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 администрирования и результаты работы утилиты в файл журнала. Если этот ключ не используется, параметры, результаты и сообщения об ошибках отображаются на экране.
- `-sp` – показать пароль аутентификации пользователя на прокси-сервере. Этот параметр используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.

- `-savecert <имя файла>` – сохранить сертификат, используемый для проверки доступа к Серверу администрирования, в указанном файле.
- `-restart` – перезапустить Агент администрирования.

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 сохраняется в директории /opt/kaspersky/klnagent/bin в 32-битной операционной системе и в директории /opt/kaspersky/klnagent64/bin в 64-битной операционной системе. В зависимости от используемых ключей Агент администрирования выполняет следующие действия при запуске:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает 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 работы утилиты в указанный файл. Если этот ключ не используется, результаты и сообщения об ошибках отправляются в stdout.
- `-address <адрес сервера>` – адрес Сервера администрирования, используемого для подключения. Это может быть IP-адрес, NetBIOS или DNS-имя компьютера.
- `-pn <номер порта>` – номер порта, по которому устанавливается незашифрованное соединение с Сервером администрирования. По умолчанию используется порт 14000.
- `-ps <номер SSL- порта>` – номер SSL-порта, по которому устанавливается зашифрованное соединение с Сервером администрирования по протоколу SSL. По умолчанию используется порт 13000.
- `-nossl` – использовать незашифрованное соединение с Сервером администрирования. Если этот ключ не указан, Агент соединяется с Сервером администрирования через зашифрованный протокол SSL.
- `-cert <путь к файлу сертификата>` – использовать указанный файл сертификата для аутентификации доступа к новому Серверу администрирования. Если ключ не используется, Агент администрирования получит сертификат при первом подключении к Серверу администрирования.
- `-silent` – запустить утилиту в неинтерактивном режиме. Использование ключа может быть полезно, например, при запуске утилиты из сценария запуска при регистрации пользователя.
- `-dupfix` – этот файл ключа используется, если способ установки Агента администрирования отличается от способа установки в составе комплекте поставки, например, восстановление с диска.
- `-cloningmode 1` – перейти в режим клонирования.
- `-cloningmode 0` – выйти из режима клонирования.

kaspersky

Управление программой с помощью Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console

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

Описание приведено для версии Kaspersky Security Center 13.

Kaspersky Security Center Cloud Console – это облачная версия Kaspersky Security Center. То есть Сервер администрирования и другие компоненты Kaspersky Security Center установлены в облачной инфраструктуре "Лаборатории Касперского". Вы управляете Kaspersky Security Center Cloud Console с помощью облачной Консоли администрирования, которая называется Kaspersky Security Center Cloud Console. Эта консоль имеет интерфейс, аналогичный интерфейсу Kaspersky Security Center Web Console. Подробная информация о Kaspersky Security Center Cloud Console приведена в документации Kaspersky Security Center Cloud Console (https://support.kaspersky.com/KSC/CloudConsole/ru-RU/5022.htm).

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

С помощью Kaspersky Security Center Web Console можно выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- устанавливать программы "Лаборатории Касперского" на устройства вашей сети;
- управлять установленными программами;
- просматривать отчеты о состоянии системы безопасности.

Управление программой Kaspersky Endpoint Security через Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console осуществляется с помощью веб-плагина управления Kaspersky Endpoint Security (см. раздел "О веб-плагине управления Kaspersky Endpoint Security" на стр. 36).

Чтобы управлять через Kaspersky Security Center Cloud Console или Kaspersky Security Center Web Console работой программы Kaspersky Endpoint Security, установленной на компьютерах, вам нужно поместить эти компьютеры в группы администрирования. Вы можете создать группы администрирования в Kaspersky Security Center перед началом установки программы Kaspersky Endpoint Security и настроить правила автоматического перемещения компьютеров в группы администрирования. Или вы можете вручную переместить компьютеры в группы администрирования после установки программы Kaspersky Endpoint Security (см. подробнее в документации Kaspersky Security Center).

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

В этом разделе

Вход и выход из Web Console и Cloud Console

Kaspersky Security Center Web Console

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

► *Чтобы войти в Web Console:*

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

   Откроется страница входа.
2. Введите имя пользователя и пароль вашей учетной записи.
3. Нажмите на кнопку **Войти**.

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

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

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

► *Чтобы выйти из Web Console:*

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

Web Console закроется и отобразится страница входа.

Kaspersky Security Center Cloud Console

Для Kaspersky Security Center Cloud Console используйте веб-токен для входа в учетную запись на портале Cloud Console.

Подробная информация о Kaspersky Security Center Cloud Console приведена в документации Kaspersky Security Center Cloud Console (https://support.kaspersky.com/KSC/CloudConsole/ru-RU/5022.htm).

Запуск и остановка программы

После установки программы Kaspersky Endpoint Security на компьютер пользователя запуск программы выполняется автоматически. Далее по умолчанию запуск программы выполняется сразу после запуска операционной системы. Вы можете контролировать статус работы программы с помощью веб-виджета **Состояние защиты** в окне **Мониторинг и отчеты / Панель мониторинга**.

► *Чтобы запустить или остановить программу дистанционно*

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите запустить или остановить программу.

   Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Установите флажок напротив программы **Kaspersky Endpoint Security 11.3.0 для Linux**.
5. Нажмите на кнопку **Запустить** или **Остановить**.

Просмотр состояния защиты устройства

► *Чтобы просмотреть состояние защиты устройства:*

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.

   Откроется список управляемых устройств.

   В списке выберите устройство, подробную информацию о котором вы хотите просмотреть, и по ссылке с названием устройства откройте окно, содержащее общую информацию о выбранном устройстве.
2. На закладке **Общие** выберите раздел **Защита**.

В разделе **Защита** отображается следующая информация о выбранном устройстве:

- **Видимо в сети** – видимость выбранного устройства в сети.
- **Статус устройства** – текущий статус выбранного устройства: *OK*, *Критический* или *Предупреждение*.
- **Описание статуса** – причины смены выбранного статуса устройства на *Критический* или *Предупреждение*.
- **Состояние защиты** – статус задачи Защита от файловых угроз, например: *Выполняется*, *Остановлена*, *Приостановлена*.
- **Последняя полная проверка** – дата и время выполнения последней полной проверки на выбранном устройстве.
- **Обнаружено вирусов** – общее количество вредоносных объектов, обнаруженных на выбранном устройстве (счетчик обнаруженных угроз) с момента установки Kaspersky Endpoint Security.

- **Объекты, которые не удалось вылечить** – количество зараженных объектов, которые программе Kaspersky Endpoint Security не удалось вылечить.
- **Статус шифрования диска** – текущий статус шифрования файлов на локальных дисках устройства.

Управление политиками в Web Console

Политика – это набор параметров работы программы, определенный для группы администрирования. С помощью политик вы можете установить одинаковые значения параметров работы программы Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования. В политике задаются не все параметры программы.

Для одной программы вы можете настроить несколько политик с различными значениями параметров. Однако одновременно для программы может быть активна только одна политика в пределах группы администрирования. При создании новой политики (см. раздел "Создание политики" на стр. 298) все остальные политики в группе администрирования становятся неактивными. Вы можете изменить статус политики (см. раздел "Изменение статуса политики" на стр. 299) позже.

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

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

Каждый параметр политики имеет атрибут «замок», который показывает, наложен ли запрет на изменение параметров в дочерних политиках и локальных параметрах программы. 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.

Для дочерней политики атрибут "замок" работает, только если в дочерней политике включено наследование параметров из родительской политики.

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

Вы можете выполнять следующие действия над политикой:

- Создавать политику (см. раздел "Создание политики" на стр. 298).
- Изменять параметры политики (см. раздел "Изменение параметров политики" на стр. 299).

Если учетная запись пользователя, под которой вы осуществили доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения. Кроме того, некоторые параметры могут быть недоступны для настройки и использования в сертифицированной версии программы.

- Удалять политику (см. раздел "Удаление политики" на стр. 300).
- Изменять состояние политики (см. раздел "Изменение статуса политики" на стр. 299).

Дополнительная информация о политиках приведена в документации Kaspersky Security Center.

В этом разделе

Создание политики

► *Чтобы создать политику:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.

   Откроется список политик.

2. Нажмите на кнопку **Добавить**.

   Откроется окно **Выбор программы**.

3. Выберите **Kaspersky Endpoint Security 11.3.0 для Linux** и нажмите на кнопку **Далее**.

4. Примите решение об участии в Kaspersky Security Network. Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

   - Если вы согласны со всеми пунктами Положения и хотите использовать Kaspersky Security Network в работе программы, выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.
   - Если вы не хотите принимать участие в Kaspersky Security Network, выберите вариант **Я не принимаю условия настоящего Положения о Kaspersky Security Network** и подтвердите свое решение в открывшемся окне.

   Отказ от участия в Kaspersky Security Network не прерывает процесс создания политики. Вы в любой момент можете включить, выключить или изменить режим Kaspersky Security Network (см. стр. 315) для управляемых компьютеров в параметрах политики (см. раздел "Параметры политики" на стр. 300).

5. Нажмите на кнопку **Далее**.

   Откроется окно параметров созданной политики на закладке **Общие**.

6. На закладке **Общие** вы можете настроить следующие параметры политики:
   - Название политики.
   - Статус политики:
     - **Активна**. При следующей синхронизации компьютера с Сервером администрирования, политика будет использоваться в качестве активной на компьютере.
     - **Неактивна**. Дополнительная политика, не используемая в настоящий момент. При необходимости можно активировать неактивную политику.
     - **Для автономных пользователей**. Политика, которая становится активной, когда компьютер покидает сеть организации.

     По умолчанию выбран вариант **Активна**.
   - Параметры наследования политики:
     - **Наследовать параметры родительской политики**. Если выбран этот вариант, значения параметров политики наследуются из групповой политики верхнего уровня и, следовательно, недоступны для изменения. Этот вариант выбран по умолчанию.
     - **Обеспечить принудительное наследование параметров для дочерних политик**. Если выбран этот вариант, параметры дочерних политик недоступны для изменения.

   Дополнительная информация о параметрах политик приведена в документации Kaspersky Security Center.
7. На закладке **Параметры программы** вы можете изменить параметры политики (см. стр. 300).
8. Нажмите на кнопку **Сохранить**.

Созданная политика появится в списке политик. Вы можете изменить параметры политики позже (см. раздел "Изменение параметров политики" на стр. 299). Дополнительная информация об управлении политиками приведена в документации Kaspersky Security Center.

Изменение параметров политики

► *Чтобы изменить параметры политики:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.

   Откроется список политик.
2. В списке политик выберите политику, параметры которой вы хотите изменить.
3. Измените параметры политики (см. стр. 300).
4. Нажмите на кнопку **ОК**.
5. Нажмите на кнопку **Сохранить**.

Политика будет сохранена с обновленными параметрами.

Изменение статуса политики

► *Чтобы изменить статус политики:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили**.

Откроется список политик.

2. В списке политик выберите политику, статус которой вы хотите изменить.
3. На закладке **Общие** в разделе **Статус политики** выберите нужный статус:
   - **Активна**. При следующей синхронизации компьютера с Сервером администрирования, политика будет использоваться в качестве активной на компьютере.
   - **Неактивна**. Дополнительная политика, не используемая в настоящий момент. При необходимости можно активировать неактивную политику.
   - **Для автономных пользователей**. Политика, которая становится активной, когда компьютер покидает сеть организации.
4. Нажмите на кнопку **Сохранить**.

Статус политики будет изменен.

Удаление политики

► *Чтобы удалить политику:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили**.

   Откроется список политик.
2. В списке политик установите флажок рядом с названием политики, которую вы хотите удалить.

   Вы можете одновременно выбрать несколько политик для удаления.
3. Нажмите на кнопку **Удалить**.
4. Нажмите на кнопку **ОК**.

Политика будет удалена.

Параметры политики

Вы можете использовать политику для настройки параметров работы программы Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования.

Набор и значения по умолчанию для параметров политики могут отличаться в зависимости от типа лицензии на программу (https://support.kaspersky.ru/15471). Кроме того, некоторые параметры могут быть недоступны для настройки и использования в сертифицированной версии программы.

kaspersky

В этом разделе

Закладка Параметры программы

На закладке **Параметры программы** вы можете выбрать раздел, содержащий набор параметров, которые вы хотите настроить.

Таблица 112. Разделы

Раздел	Описание
Базовая защита	**Защита от файловых угроз** (см. стр. 302) **Исключения из проверки** (см. стр. 307) **Управление сетевым экраном** (см. стр. 312) **Защита от веб-угроз** (см. стр. 313) **Защита от сетевых угроз** (см. стр. 315)

Раздел	Описание
Продвинутая защита	**Kaspersky Security Network** (см. стр. 315) **Защита от шифрования** (см. стр. 317) **Контроль целостности системы** (см. стр. 322) **Контроль программ** (см. стр. 325) **Контроль устройств** (см. стр. 328) **Анализ поведения** (см. стр. 328)
Локальные задачи	**Управление задачами** (см. стр. 330) **Проверка съемных дисков** (см. стр. 330)
Общие параметры	**Параметры прокси-сервера** (см. стр. 331) **Параметры программы** (см. стр. 332) **Параметры проверки контейнеров** (см. стр. 334) **Managed Detection and Response** (см. стр. 335) **Параметры сети** (см. стр. 335) **Глобальные исключения** (см. стр. 337) **Параметры Хранилища** (см. стр. 338)

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

Защита от файловых угроз

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

Таблица 113. Параметры Защиты от файловых угроз

Параметр	Описание
Защита от файловых угроз включена / выключена	Переключатель включает или выключает Защиту от файловых угроз на всех управляемых устройствах. По умолчанию переключатель включен.

Параметр	Описание
Режим Защиты от файловых угроз	В раскрывающемся списке вы можете выбрать режим работы Защиты от файловых угроз: • **Интеллектуальный режим** (значение по умолчанию) – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс в течение определенного времени многократно обращается к файлу и изменяет его, программа повторно проверяет файл только при последнем закрытии файла этим процессом. • **При открытии** – проверять файл при попытке открытия на чтение, исполнение или изменение. • **При открытии и изменении** – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое программа будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет помещена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Блокировать** доступ к объекту.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое программа будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет помещена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Блокировать** доступ к объекту (значение по умолчанию).
Области проверки	По ссылке **Настроить области проверки** открывается окно **Области проверки** (см. раздел "Окно Области проверки**" на** стр. 220).
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, программа проверяет архивы. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, включив и настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)**. Если флажок снят, программа не проверяет архивы. По умолчанию флажок снят.

Параметр	Описание
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, программа проверяет самораспаковывающиеся архивы. Если флажок снят, программа не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок снят.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз программ Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, программа проверяет файлы почтовых баз. Если флажок снят, программа не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, программа проверяет сообщения в текстовом формате. Если флажок снят, программа не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать текстовые файлы	Временное исключение из проверки файлов в текстовом формате. Если флажок установлен, Kaspersky Endpoint Security не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течении 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов работы программ. Если флажок снят, Kaspersky Endpoint Security проверяет текстовые файлы. По умолчанию флажок снят.
Прервать проверку, если она длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки объекта в секундах. После истечения указанного времени программа прекращает проверку объекта. Доступные значения: `0–9999`. Если указано значение `0`, время проверки не ограничено. Значение по умолчанию: `60`.
Пропускать объекты размером более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0–999999`. Если установлено значение `0`, программа проверяет объекты любого размера. Значение по умолчанию: `0`.

Параметр	Описание
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал события *ObjectProcessed*. Если флажок установлен, программа записывает в журнал событие *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, программа не записывает событие в журнал. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал события *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, программа записывает в журнал событие *ObjectNotProcessed*. Если флажок снят, программа не записывает событие в журнал. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал события *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, программа записывает в журнал событие *PackedObjectDetected*. Если флажок снят, программа не записывает событие в журнал. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, программа проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, программа проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке объектов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.

Окно Области проверки

Таблица содержит области проверки. Программа проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Таблица 114. Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли программа эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Таблица 115. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки** (см. раздел "Окно Области проверки" на стр. 220). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область проверки во время работы. Если флажок снят, программа не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. • **Смонтированная** – смонтированные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все смонтированные** – все смонтированные директории. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.

Параметр	Описание
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательский** – ресурсы файловой системы компьютера, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. По умолчанию указан путь **/** – программа проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, программа проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых программа Kaspersky Endpoint Security не проверяет объект на вирусы и другие угрозы. Вы также можете исключать из проверки объекты по маскам и названиям угроз и настраивать исключения для процессов.

Таблица 116. Параметры исключений из проверки

Параметр	Описание
Области исключения	По ссылке **Настроить исключения** открывается окно **Области исключения**. В этом окне вы можете задать список исключений из проверки.
Исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске** (см. раздел "Окно Исключения по маске" на стр. 309). В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	По ссылке **Настроить исключения по названию угрозы** открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Параметр	Описание
Исключения по процессам	По ссылке **Настроить исключения по процессам** открывается окно **Исключения по процессам** (см. раздел "Окно Исключения по процессам" на стр. 310). В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Области исключения

Таблица содержит области исключения из проверки. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 117. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, применяется ли это исключение в работе программы.

Элементы в таблице можно добавлять, изменять и удалять.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

Таблица 118. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время работы программы. Если флажок установлен, программа исключает эту область из проверки или защиты во время своей работы. Если флажок снят, программа включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные директории. • **Смонтированная** – удаленные директории, смонтированные на компьютере. • **Все смонтированные** – все удаленные директории, смонтированные на компьютере.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательский** – ресурсы файловой системы компьютера, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. По умолчанию указан путь **/** – программа исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые программа исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле **Путь**. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Программа не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска.

Примеры:

Маска `*.txt` – все текстовые файлы.

Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Программа не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную угрозу из списка исключений. Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение из проверки активности указанного процесса и файлов, изменяемых указанным процессом. По умолчанию таблица пуста.

Таблица 119. Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, применяется ли это исключение в работе программы.

Элементы в таблице можно добавлять, изменять и удалять (см. раздел "Окно Доверенный процесс" на стр. 310).

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Таблица 120. Параметры области исключения

Параметр	Описание
Название области исключения по процессам	Поле ввода названия области исключения по процессам. Это название будет отображаться в таблице окна **Исключения по процессам** (см. раздел "Окно Исключения по процессам" на стр. 310). Поле ввода не должно быть пустым.
Использовать / Не использовать это исключение	Переключатель включает или выключает исключение этой области во время работы программы. По умолчанию переключатель включен.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром **Путь к исключаемому процессу**. По умолчанию флажок снят.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать исключения из проверки для файлов, которые изменяет процесс. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все смонтированные** – все смонтированные директории. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательский** – ресурсы файловой системы компьютера, указанные в поле ниже. Раскрывающийся список **Протокол доступа** доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** или **Общая**.
Путь	В поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые программа исключает из проверки. Маски применяются к объектам только внутри директории, указанной в блоке **Файловая система, протокол доступа и путь**. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Управление сетевым экраном

Сетевой экран операционной системы защищает персональные данные, которые хранятся на компьютере пользователя. Сетевой экран блокирует большую часть угроз для операционной системы, когда компьютер подключен к интернету или локальной сети. Управление сетевым экраном позволяет обнаружить все сетевые соединения на компьютере пользователя и предоставить список их IP-адресов с указанием статуса сетевого соединения по умолчанию.

Компонент Управление сетевым экраном фильтрует всю сетевую активность в соответствии с сетевыми пакетными правилами. Настройка сетевых пакетных правил позволяет вам задать нужный уровень защиты компьютера, от полной блокировки доступа в интернет для всех программ до разрешения неограниченного доступа.

Перед включением компонента Управление сетевым экраном рекомендуется выключить другие средства управления сетевым экраном операционной системы.

Таблица 121. Параметры компонента Управление сетевым экраном

Параметр	Описание
Управление сетевым экраном включено / выключено	Переключатель включает или выключает Управление сетевым экраном. По умолчанию переключатель выключен.
Сетевые пакетные правила	По ссылке **Настроить сетевые пакетные правила** открывается окно **Сетевые пакетные правила**. В этом окне вы можете настроить список сетевых пакетных правил, которые будет применять компонент Управление сетевым экраном при обнаружении попытки установления сетевого соединения.
Доступные сети	По ссылке **Настроить доступные сети** открывается окно **Доступные сети**. В этом окне вы можете настроить список сетей, которые будет контролировать компонент Управление сетевым экраном.
Входящие соединения	В раскрывающемся списке вы можете выбрать действие для входящих сетевых соединений: • **Разрешать** сетевые соединения (значение по умолчанию). • **Блокировать** сетевые соединения.
Входящие пакеты	В раскрывающемся списке вы можете выбрать действие для входящих пакетов: • **Разрешать** входящие пакеты (значение по умолчанию). • **Блокировать** входящие пакеты.

Параметр	Описание
Всегда добавлять разрешающие правила для портов Агента администрирования	Флажок включает или выключает автоматическое добавление разрешающих правил для портов Агента администрирования. По умолчанию флажок установлен.

Защита от веб-угроз

Во время работы компонента Защита от веб-угроз программа Kaspersky Endpoint Security проверяет входящий трафик, не допускает загрузку вредоносных файлов из интернета, а также блокирует фишинговые, рекламные и прочие опасные веб-сайты. Защита от веб-угроз запускается по умолчанию при запуске программы.

Программа проверяет трафик, передаваемый по протоколам HTTP, HTTPS и FTP. Также выполняется проверка веб-сайтов и IP-адресов. Вы можете указать определенные сетевые порты или диапазоны сетевых портов для проверки.

Для проверки HTTPS-трафика требуется включить проверку зашифрованных соединений (см. раздел "Параметры сети" на стр. 335). Для проверки FTP-трафика требуется установить флажок **Отслеживать все сетевые порты** (см. раздел "Параметры сети" на стр. 335).

Таблица 122. Параметры Защиты от веб-угроз

Параметр	Описание
Защита от веб-угроз включена / выключена	Переключатель включает или выключает компонент Защита от веб-угроз. По умолчанию переключатель выключен.
Действие при обнаружении угрозы	В этом разделе вы можете указать действие, которое программа будет выполнять над веб-ресурсом, на котором обнаружен опасный объект: • **Информировать** пользователя при обнаружении опасного объекта в веб-трафике. Программа позволяет выполнить загрузку объекта на компьютер, записывает в журнал и добавляет в список активных угроз информацию об опасном объекте. • **Блокировать** доступ ко всем опасным объектам, обнаруженным в веб-трафике, показывать уведомление о заблокированных попытках доступа и записывать в журнал информацию об опасных объектах (значение по умолчанию).
Обнаруживать вредоносные объекты	Флажок включает или выключает проверку ссылок по базе вредоносных веб-адресов. По умолчанию флажок установлен.
Обнаруживать фишинговые ссылки	Флажок включает или выключает проверку ссылок по базе фишинговых веб-адресов. По умолчанию флажок установлен.

Параметр	Описание
Использовать эвристический анализ для обнаружения фишинговых ссылок	Флажок включает или выключает использование эвристического анализа для обнаружения фишинговых ссылок. Флажок доступен и установлен по умолчанию, если установлен флажок **Обнаруживать фишинговые ссылки**.
Обнаруживать рекламные программы	Флажок включает или выключает проверку ссылок по базе рекламных веб-адресов. По умолчанию флажок снят.
Обнаруживать легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройствам или данным	Флажок включает или выключает проверку ссылок по базе легальных программ, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. По умолчанию флажок снят.
Доверенные веб-адреса	Таблица содержит веб-адреса и веб-страницы, содержимое которых вы считаете доверенным. В список доверенных веб-адресов вы можете добавлять только веб-адреса HTTP / HTTPS. Использование масок для указания IP-адресов не поддерживается. По умолчанию таблица пуста. Вы можете добавлять, изменять и удалять веб-адреса в таблице.

Окно Веб-адрес

В этом окне вы можете добавить веб-адреса или маски веб-адресов в список доверенных веб-адресов.

Таблица 123. Доверенные веб-адреса

Параметр	Описание
Введите адрес или маску адреса веб-сайта	Поле ввода веб-адресов и веб-страниц, содержимое которых вы считаете доверенным. При создании маски адреса используйте символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html).

В список доверенных веб-адресов можно добавлять только веб-адреса HTTP / HTTPS. Использование масок для указания IP-адресов не поддерживается.

kaspersky

Защита от сетевых угроз

Во время работы компонента Защита от сетевых угроз программа проверяет входящий сетевой трафик на действия, характерные для сетевых атак. Защита от сетевых угроз запускается по умолчанию при запуске программы.

Программа проверяет входящий трафик для TCP-портов, номера которых получает из актуальных баз программы. При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, программа блокирует сетевую активность со стороны атакующего компьютера и записывает в журнал соответствующее событие.

Для проверки сетевого трафика задача Защита от сетевых угроз принимает подключения по всем портам, номера которых получает из баз программы. При проверке сети это может выглядеть как открытый порт на устройстве, даже если никакое приложение в системе его не прослушивает. Неиспользуемые порты рекомендуется закрывать средствами сетевого экрана.

Таблица 124. Параметры Защиты от сетевых угроз

Параметр	Описание
Защита от сетевых угроз включена / выключена	Переключатель включает или выключает компонент Защита от сетевых угроз. По умолчанию переключатель включен.
Действие при обнаружении угрозы	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак: • **Информировать** пользователя. Программа разрешает сетевую активность и записывает в журнал информацию об обнаруженной сетевой активности. • **Блокировать** сетевую активность со стороны атакующего компьютера и записывать в журнал информацию об обнаруженной сетевой активности.
Блокировка атакующих устройств включена / выключена	Переключатель включает или выключает блокировку сетевой активности при обнаружении попытки сетевой атаки. По умолчанию переключатель включен.
Блокировать атакующее устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки атакующего устройства в минутах. По истечении указанного времени программа Kaspersky Endpoint Security разрешает сетевую активность со стороны этого устройства. Доступные значения: целые числа от `1` до `32768`. Значение по умолчанию: `60`.
Доверенные IP-адреса	Таблица содержит список IP-адресов, сетевые атаки с которых не будут заблокированы. По умолчанию список пуст. Вы можете добавлять, настраивать и удалять IP-адреса в таблице.

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 различные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

В зависимости от расположения инфраструктуры существуют:

- **Глобальный KSN** – инфраструктура расположена на серверах "Лаборатории Касперского".
- **Локальный KSN** – инфраструктура расположена на сторонних серверах, например внутри сети интернет-провайдера.

В сертифицированной версии программы Kaspersky Endpoint Security используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается, так как 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.

После изменения лицензии для использования Локального KSN требуется предоставить поставщику услуг информацию о новом ключе. В противном случае обмен информацией с Локальным KSN будет невозможен из-за ошибки аутентификации.

Участие пользователей в Kaspersky Security Network позволяет "Лаборатории Касперского" разрабатывать решения для нейтрализации угроз и уменьшать количество ложных срабатываний компонентов программы. Участие в Kaspersky Security Network является добровольным. Программа предлагает участвовать в Kaspersky Security Network во время установки.

В программе предусмотрено два варианта участия в Kaspersky Security Network:

- **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.

Вы можете начать или прекратить использование Kaspersky Security Network в любой момент, а также выбрать другой вариант участия в Kaspersky Security Network.

Сбор, обработка и хранение персональных данных пользователя не производится. Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте https://www.kaspersky.ru/products-and-services-privacy-policy.

Текст Положения о Kaspersky Security Network вы можете прочитать в окне **Положение о Kaspersky Security Network**, которое можно открыть по ссылке **Текст Положения о Kaspersky Security Network**.

Таблица 125. Параметры Kaspersky Security Network

Параметр	Описание
Не участвовать в Kaspersky Security Network	Выбирая этот вариант, вы отказываетесь от участия в Kaspersky Security Network.
Kaspersky Security Network со статистикой	Выбирая этот вариант, вы принимаете условия участия в Kaspersky Security Network. Вы сможете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Кроме того, для улучшения работы Kaspersky Security Network будет отправляться анонимная статистика и данные о типах и источниках различных угроз.
Kaspersky Security Network без статистики	Выбирая этот вариант, вы принимаете условия участия в Kaspersky Security Network. Вы сможете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения.
Текст Положения о Kaspersky Security Network	По ссылке открывается окно **Положение о Kaspersky Security Network**. В этом окне вы можете просмотреть текст Положения о Kaspersky Security Network.

Положение о Kaspersky Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Security Network и принять его условия.

Таблица 126. Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите участвовать в Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Security Network.
Я не принимаю условия настоящего Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите участвовать в Kaspersky Security Network.

Защита от шифрования

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

Во время работы компонента Защита от шифрования программа Kaspersky Endpoint Security проверяет обращения удаленных компьютеров сети к файлам, расположенным в общих сетевых директориях защищаемого устройства. Если программа расценивает действия удаленного компьютера, получающего доступ к общим сетевым ресурсам, как вредоносное шифрование, она добавляет этот компьютер в список недоверенных устройств и запрещает ему доступ к общим сетевым директориям. Программа не расценивает действия как вредоносное шифрование, если активность обнаружена в директориях, которые не входят в область защиты компонента Защита от шифрования.

Для использования компонента требуется лицензия, которая включает эту функцию.

Для корректной работы компонента Защита от шифрования требуется, чтобы в операционной системе была установлена хотя бы одна из служб: Samba или NFS. Для службы NFS требуется, чтобы был установлен пакет rpcbind.

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

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

Таблица 127. Параметры Защиты от шифрования

Параметр	Описание
Защита от шифрования включена / выключена	Переключатель включает или выключает защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования. По умолчанию переключатель выключен.
Области защиты	По ссылке **Настроить область защиты** открывается окно **Области защиты** (см. раздел "Окно Области защиты" на стр. 319).
Блокировка недоверенных устройств включена / выключена	Переключатель включает или выключает блокировку недоверенных устройств. По умолчанию переключатель включен.
Блокировать недоверенное устройство на (мин)	Поле, в котором вы можете указать длительность блокировки недоверенного устройства в минутах. По истечении указанного времени Kaspersky Endpoint Security удаляет недоверенные устройства из списка заблокированных. Доступ устройства к сетевым файловым ресурсам восстанавливается автоматически после его удаления из списка недоверенных устройств. Изменение параметра не влияет на длительность блокировки ранее заблокированных скомпрометированных устройств. Длительность блокировки не является динамическим значением и рассчитывается в момент блокировки. Доступные значения: целые числа от `1` до `4294967295`. Значение по умолчанию: `30`.
Исключения	По ссылке **Настроить исключения** открывается окно **Исключения**.
Исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске** (см. раздел "Окно Исключения по маске" на стр. 309).

Окно Области защиты

Таблица содержит области защиты компонента Защита от шифрования. Программа проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область защиты, включающую все общие директории.

Таблица 128. Параметры области защиты

Параметр	Описание
Название области	Название области защиты.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли программа эту область при работе. Вы можете включить или выключить переключатель в таблице для изменения статуса области защиты.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно добавления области проверки

В этом окне можно добавить или настроить область защиты компонента Защита от шифрования.

Таблица 129. Параметры области защиты

Параметр	Описание
Название области проверки	Поле ввода названия области защиты. Это название будет отображаться в таблице окна **Области защиты** (см. раздел "Окно Области защиты" на стр. 319). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область защиты во время работы. Если флажок снят, программа не обрабатывает эту область защиты во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран элемент **Общие**.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите включить в область защиты. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**. Поле не должно быть пустым. По умолчанию указан путь **/** (корневая директория).
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы компонента Защита от шифрования. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Области исключения

Таблица содержит области исключения из проверки. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 130. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, применяется ли это исключение в работе программы.

Элементы в таблице можно добавлять, изменять и удалять.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

Таблица 131. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время работы программы. Если флажок установлен, программа исключает эту область из проверки или защиты во время своей работы. Если флажок снят, программа включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные директории. • **Смонтированная** – удаленные директории, смонтированные на компьютере. • **Все смонтированные** – все удаленные директории, смонтированные на компьютере.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательский** – ресурсы файловой системы компьютера, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. По умолчанию указан путь **/** – программа исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые программа исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле **Путь**. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Программа не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска.

Примеры:

Маска `*.txt` – все текстовые файлы.

Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Контроль целостности системы

Контроль целостности системы предназначен для отслеживания действий, выполняемых с файлами и директориями в области мониторинга, указанной в параметрах работы компонента. Вы можете использовать Контроль целостности системы, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом сервере.

Для использования компонента требуется лицензия, которая включает эту функцию.

Таблица 132. Параметры Контроля целостности системы

Параметр	Описание
Контроль целостности системы включен / выключен	Переключатель включает или выключает Контроль целостности системы. По умолчанию переключатель выключен.
Области мониторинга	По ссылке **Настроить области мониторинга** открывается окно **Области мониторинга** (см. стр. 322).
Исключения из мониторинга	По ссылке **Настроить области исключения из мониторинга** открывается окно **Исключения из мониторинга** (см. раздел "Окно Области исключения" на стр. 246).
Исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске** (см. раздел "Окно Исключения по маске" на стр. 247).

Окно Области мониторинга

Таблица содержит области мониторинга компонента Контроль целостности системы. Программа контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/).

Таблица 133. Параметры области мониторинга Контроля целостности системы

Параметр	Описание
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли программа эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область мониторинга для компонента Контроля целостности системы.

Таблица 134. Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна **Области мониторинга** (см. стр. 322). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область мониторинга во время работы. Если флажок снят, программа не обрабатывает эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Поле не должно быть пустым. По умолчанию указан путь */* – программа проверяет все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Области исключения

Таблица содержит области исключения из мониторинга для компонента Контроль целостности системы. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 135. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли программа эту область из мониторинга при работе компонента.

Элементы в таблице можно добавлять, изменять и удалять.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения из мониторинга для компонента Контроль целостности системы.

Таблица 136. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения** (см. раздел "Окно Области исключения" на стр. 246). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы программы. Если флажок установлен, программа исключает эту область из мониторинга во время работы компонента. Если флажок снят, программа отслеживает эту область во время работы компонента. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Поле не должно быть пустым. По умолчанию указан путь **/** – программа исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые программа исключает из мониторинга. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Программа не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент.

Контроль программ

Во время работы компонента Контроль программ Kaspersky Endpoint Security управляет запуском программ на компьютерах пользователей. Это позволяет снизить риск заражения компьютера, ограничивая доступ к программам. Запуск программ регулируется с помощью *правил контроля программ* (см. раздел "*О правилах контроля программ*" на стр. 193).

Для использования компонента требуется лицензия, которая включает эту функцию.

Контроль программ может работать в двух режимах:

- *Список запрещенных*. Режим, при котором программа Kaspersky Endpoint Security разрешает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ. Этот режим работы задачи Контроль программ настроен по умолчанию.
- *Список разрешенных*. Режим, при котором программа Kaspersky Endpoint Security запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ.

Таким образом, если правила контроля программ сформированы максимально полно, программа Kaspersky Endpoint Security запрещает запуск всех новых, не проверенных администратором локальной сети организации программ, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

Для каждого режима работы Контроля программ вы можете создать отдельные правила, а также выбрать действие, которое программа Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска программы: *применять правила* или *тестировать правила*.

Параметры Контроля программ описаны в таблице ниже.

Таблица 137. Параметры Контроля программ

Параметр	Описание
Контроль программ включен / выключен	Переключатель включает или выключает Контроль программ. По умолчанию переключатель выключен.
Действие Контроля программ	Вы можете выбрать действие, которое Контроль программ будет выполнять при обнаружении попытки запуска программы, удовлетворяющей настроенным правилам: • **Тестировать правила**. При выборе этого варианта Контроль программ проверяет правила контроля программ и формирует событие об обнаружении программ, удовлетворяющих правилам. • **Применять правила** (значение по умолчанию). При выборе этого варианта Контроль программ применяет правила контроля программ и выполняет заданное в правилах действие.

Параметр	Описание
Режим Контроля программ	Вы можете выбрать режим работы компонента Контроль программ: • **Список разрешенных**. При выборе этого варианта Контроль программ запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ. • **Список запрещенных** (значение по умолчанию). При выборе этого варианта Контроль программ разрешает всем пользователям запуск любых программ, кроме тех, которые указаны в правилах контроля программ.
Правила Контроля программ	По ссылке **Настроить правила** открывается окно **Правила Контроля программ** (см. раздел "Окно Правила Контроля программ" на стр. 326).

Окно Правила Контроля программ

Таблица **Правила Контроля программ** содержит закладки с правилами для каждого режима работы Контроля программ: **Список запрещенных (активен)** и **Список разрешенных**. По умолчанию таблица правил контроля программ на обеих закладках пустая.

Таблица 138. Параметры правил контроля программ

Параметр	Описание
Категория	Название категории программ, которая используется в работе правила.
Статус	Статус работы правила контроля программ: • *Включено* – правило включено, Контроль программ применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля программ. • *Тест* – Контроль программ разрешает запуск программ, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих программ в отчете.

Вы можете добавлять, изменять и удалять правила контроля программ (см. раздел "Окно Правило Контроля программ" на стр. 326).

Окно Правило Контроля программ

В этом окне вы можете настроить параметры правила Контроля программ.

Таблица 139. Настройка правила Контроля программ

Параметр	Описание
Описание правила	Описание правила Контроля программ.
Статус	Вы можете выбрать статус работы правила контроля программ: • *Включено* – правило включено, Контроль программ применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля программ. • *Тест* – Контроль программ разрешает запуск программ, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих программ в отчете.
Категория	По ссылке **Настроить категорию** открывается окно **Категории Контроля программ** (см. раздел "Окно Категории Контроля программ" на стр. 327).
Список управления доступом	Таблица содержит список пользователей или групп пользователей, на которых распространяется правило контроля программ, и назначенный им тип доступа, и состоит из следующих граф: • **Имя оператора доступа** – пользователи или группы пользователей, на которых распространяется правило контроля программ. • **Доступ** – тип доступа (разрешение или запрет на запуск программ). Переключатель включает или выключает тип доступа: **Разрешать** запуск программ или **Блокировать** запуск программ. Вы можете добавлять, изменять и удалять пользователей или группы пользователей (см. раздел "Окно Выбор пользователя или группы" на стр. 327).

Окно Категории Контроля программ

В этом окне вы можете добавить новую категорию или настроить параметры категории для правила Контроля программ.

Использование KL-категорий Kaspersky Security Center не поддерживается.

Таблица 140. Категории Контроля программ

Параметр	Описание
Название категории	Строка поиска добавленных категорий Контроля программ.
Добавить	При нажатии на кнопку запускается Мастер создания категорий Kaspersky Security Center. Следуйте указаниям мастера.
Изменить	При нажатии на кнопку открывается окно свойств категории, в котором вы можете изменить параметры категории.

Окно Выбор пользователя или группы

В этом окне вы можете указать пользователя или группу пользователей, для которых вы хотите настроить правило.

Вы можете использовать поле поиска, чтобы ввести критерии поиска.

Контроль устройств

Во время работы компонента Контроль устройств программа Kaspersky Endpoint Security управляет доступом пользователей к устройствам, установленным на компьютере или подключенным к нему (например, к жестким дискам, устройствам чтения смарт-карт, модулям Wi-Fi). Это позволяет защитить компьютер от заражения при подключении таких устройств, а также предотвратить потерю и утечку данных. Контроль устройств управляет доступом пользователей к устройствам с помощью правил доступа.

Если устройство, заблокированное Контролем устройств, подключено к компьютеру, программа запрещает пользователям доступ к этому устройству и выводит уведомление.

Таблица 141. Параметры Контроля устройств

Параметр	Описание
Контроль устройств включен / выключен	Переключатель включает или выключает компонент Контроль устройств. По умолчанию переключатель включен.
Настроить доверенные устройства	По ссылке открывается окно **Доверенные устройства**. В этом окне вы можете добавлять устройства в список доверенных по идентификатору устройства или выбрав их из списка существующих устройств.
Действие Контроля устройств	Действие, выполняемое программой при попытке доступа к устройству, к которому запрещен доступ в соответствии с правилами Контроля устройств: • **Тестировать правила**. При выборе этого варианта программа Kaspersky Endpoint Security тестирует правила доступа и формирует событие об обнаружении попытки доступа к устройству. • **Применять правила** (значение по умолчанию). При выборе этого варианта программа Kaspersky Endpoint Security применяет правила контроля доступа и выполняет заданное в правилах действие.
Настроить параметры для типов устройств	По ссылке открывается окно **Типы устройств**. В этом окне вы можете настроить правила доступа для различных типов устройств.
Настроить параметры для шин подключения	По ссылке открывается окно **Шины подключения**. В этом окне вы можете настроить правила доступа к шинам подключения.

Анализ поведения

По умолчанию компонент Анализ поведения запускается при старте программы Kaspersky Endpoint Security и контролирует вредоносную активность в операционной системе. При обнаружении вредоносной активности программа Kaspersky Endpoint Security завершает этот процесс.

Таблица 142. Параметры компонента Анализ поведения

Параметр	Описание
Анализ поведения включен / выключен	Переключатель включает или выключает компонент Анализ поведения. По умолчанию переключатель включен.

Параметр	Описание
Режим работы компонента Анализ поведения	Действия, выполняемые при обнаружении вредоносной активности в операционной системе: • **Блокировать** программу, осуществляющую вредоносную активность (значение по умолчанию). Kaspersky Endpoint Security завершает процесс программы и записывает в журнал информацию об обнаруженной вредоносной активности. • **Информировать** пользователя. Kaspersky Endpoint Security не завершает процесс, осуществляющий вредоносную активность, только регистрирует обнаружение вредоносной активности в журнале событий.
Исключения по процессам	По ссылке **Настроить исключения по процессам** открывается окно **Исключения по процессам** (см. раздел "Окно Исключения по процессам" на стр. 329). В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса и файлов, изменяемых указанным процессом. По умолчанию таблица пуста.

Таблица 143. Параметры области исключения по процессам

Параметр	Описание
Исключать / Не исключать из проверки доверенные процессы	Переключатель включает или выключает использование настроенных исключений по процессам в работе компонента Анализ поведения. По умолчанию переключатель выключен.
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, применяется ли это исключение в работе программы.

Элементы в таблице можно добавлять, изменять и удалять (см. раздел "Окно добавления области исключения по процессам" на стр. 329).

Окно добавления области исключения по процессам

В этом окне вы можете добавить или настроить область исключения по процессам.

Таблица 144. Параметры области исключения

Параметр	Описание
Название области исключения по процессам	Поле ввода названия области исключения по процессам. Это название будет отображаться в таблице окна **Исключения по процессам** (см. раздел "Окно Исключения по процессам" на стр. 329). Поле ввода не должно быть пустым.

Параметр	Описание
Использовать это исключение	Флажок включает или выключает исключение этой области во время работы программы. По умолчанию флажок установлен.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки. Поле ввода не должно быть пустым.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром **Путь к исключаемому процессу**. По умолчанию флажок снят.

Управление задачами

Вы можете настроить возможность просмотра и управления задачами программы Kaspersky Endpoint Security на управляемых устройствах.

Таблица 145. Параметры управления задачами

Параметр	Описание
Разрешить пользователям просмотр и управление локальными задачами	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в Kaspersky Endpoint Security, и управление этими задачами на управляемых устройствах. По умолчанию флажок снят.
Разрешить пользователям просмотр и управление задачами, созданными через KSC	Флажок разрешает или запрещает пользователям просмотр задач, созданных через Kaspersky Security Center Web Console, и управление этими задачами на управляемых устройствах. По умолчанию флажок снят.

Проверка съемных дисков

Во время выполнения задачи Проверка съемных дисков программа проверяет подключенное устройство и его загрузочные секторы на вирусы и другие вредоносные программы. Выполняется проверка следующих съемных дисков: CD/DVD-приводов, Blu-ray дисков, флеш-накопителей (включая USB-модемы), внешних жестких дисков и дискет.

Таблица 146. Параметры задачи Проверка съемных дисков

Параметр	Описание
Проверка съемных дисков включена / выключена	Переключатель включает или выключает проверку съемных дисков при подключении их к устройству. По умолчанию переключатель выключен.

Параметр	Описание
Действие при подключении съемного диска	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять программа при подключении к компьютеру съемных дисков: • **Не проверять** съемные диски при подключении (значение по умолчанию). • **Быстрая проверка** – проверять на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков) только файлы определенных типов и не распаковывать составные объекты. При быстрой проверке используются параметры, заданные по умолчанию для компонента Защита от файловых угроз (см. стр. 302). • **Подробная проверка** – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При подробной проверке используются параметры, заданные по умолчанию для задачи Антивирусная проверка (см. раздел "Антивирусная проверка. Раздел Параметры проверки" на стр. 343).
Действие при подключении CD/DVD-привода	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять программа при подключении к компьютеру CD/DVD-приводов и Blu-ray дисков: • **Не проверять** CD/DVD-приводы и Blu-ray диски при подключении (значение по умолчанию). • **Быстрая проверка** – проверять только файлы определенных типов на CD/DVD-приводах и Blu-ray дисках. При быстрой проверке используются параметры, заданные по умолчанию для компонента Защита от файловых угроз (см. стр. 302). • **Подробная проверка** – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. При подробной проверке используются параметры, заданные по умолчанию для задачи Антивирусная проверка (см. раздел "Антивирусная проверка. Раздел Параметры проверки" на стр. 343).
Блокировать доступ к съемному диску во время проверки	Флажок включает или выключает блокировку файлов на подключенном диске во время выполнения задачи Проверка съемных дисков. По умолчанию флажок снят.

Параметры прокси-сервера

Вы можете настроить параметры прокси-сервера, если доступ пользователей клиентских компьютеров в интернет осуществляется через прокси-сервер. Программа Kaspersky Endpoint Security может использовать прокси-сервер для подключения к серверам "Лаборатории Касперского", например, при обновлении баз и модулей программы или при взаимодействии с Kaspersky Security Network.

Таблица 147. Параметры прокси-сервера

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, прокси-сервер не используется в работе программ Kaspersky Endpoint Security.
Использовать параметры указанного прокси-сервера	Если выбран этот вариант, программа Kaspersky Endpoint Security использует указанные параметры прокси-сервера.
Адрес и порт	Поля для ввода IP-адреса или доменного имени прокси-сервера и порта прокси-сервера. Порт по умолчанию: `3128`. Поля доступны, если выбран вариант **Использовать параметры указанного прокси-сервера**.
Использовать имя пользователя и пароль	Флажок включает или выключает аутентификацию с помощью имени пользователя и пароля при доступе к прокси-серверу. Флажок доступен, если выбран вариант **Использовать параметры указанного прокси-сервера**. По умолчанию флажок снят. Для подключения через HTTP-прокси-сервер рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.
Имя пользователя	Поле ввода имени пользователя для его аутентификации на прокси-сервере. Поле ввода доступно, если установлен флажок **Использовать имя пользователя и пароль**.
Пароль	Поле для ввода пароля пользователя для авторизации на прокси-сервере. При нажатии на кнопку **Показать** пароль пользователя отображается в поле **Пароль** в открытом виде. По умолчанию пароль пользователя скрыт и отображается в виде точек. Поле ввода и кнопка доступны, если установлен флажок **Использовать имя пользователя и пароль**.
Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы	Флажок включает или выключает использование Kaspersky Security Center в качестве прокси-сервера при активации программы. Если флажок установлен, программа Kaspersky Endpoint Security использует Kaspersky Security Center в качестве прокси-сервера при активации программы. По умолчанию флажок снят.

Параметры программы

Вы можете настроить общие параметры программы Kaspersky Endpoint Security.

Таблица 148. Общие параметры программы

Параметр	Описание
Обнаруживать легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройствам или данным	Флажок включает или выключает обнаружение легальных программ, через которые злоумышленники могут навредить компьютеру или данным пользователя. По умолчанию флажок снят.
Уведомления о событиях	По ссылке **Настроить уведомления о событиях** открывается окно **Уведомления о событиях**. В этом окне вы можете выбрать события, для которых программа будет записывать уведомления в журнал операционной системы (syslog). Установите флажок около каждого типа события, для которого вы хотите отправлять уведомления. Также вы можете установить флажок около уровня важности событий (*Критические события*, *Информационные сообщения*, *Отказ функционирования*, *Предупреждения*). В этом случае флажки будут установлены автоматически около каждого типа событий, входящего в группу выбранного уровня важности. По умолчанию все флажки сняты.
Блокировать файлы во время проверки	Флажок включает или выключает блокировку файлов, в которых обнаружены угрозы во время проверки компонентом Защита от файловых угроз. Этот параметр также влияет на работу компонентов Защита от шифрования, Контроль устройств и задачи Проверка съемных дисков. По умолчанию флажок установлен.
Исключение памяти процессов из проверки	По ссылке **Настроить исключение памяти процессов из проверки** открывается окно **Исключение памяти процессов из проверки** (см. раздел "Окно Исключение памяти процессов из проверки" на стр. 258), в котором вы можете сформировать список процессов, исключаемых из проверки памяти процессов.

Окно Исключение памяти процессов из проверки

Список содержит пути к процессам, которые Kaspersky Endpoint Security исключает из проверки памяти процессов. По умолчанию список пуст.

Элементы в списке можно добавлять, изменять и удалять.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете ввести полный путь к процессу. Kaspersky Endpoint Security исключает из проверки память указанного процесса.

При нажатии на кнопку **Изменить** открывается окно, в котором вы можете изменить путь к процессу. Kaspersky Endpoint Security исключает из проверки память указанного процесса.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранный путь к процессу из списка. Кнопка доступна, если в списке выбран хотя бы один путь к процессу.

kaspersky

Параметры проверки контейнеров

Вы можете настроить параметры проверки пространств имен и контейнеров программой Kaspersky Endpoint Security.

Таблица 149. Параметры проверки контейнеров

Параметр	Описание
Проверка пространств имен и контейнеров включена / выключена	Переключатель включает или выключает проверку пространств имен и контейнеров. По умолчанию переключатель включен.
Действие с контейнером при обнаружении угрозы	Вы можете выбрать действие, которое программа будет выполнять над контейнером при обнаружении зараженного объекта: • **Пропустить контейнер** – при обнаружении зараженного объекта программа не выполняет никаких действий над контейнером. • **Остановить контейнер** – при обнаружении зараженного объекта программа останавливает контейнер. • **Остановить, если не удалось вылечить** (значение по умолчанию) – если не удалось вылечить зараженный объект, программа останавливает контейнер.
Использовать Docker	Флажок включает или выключает использование среды Docker. По умолчанию флажок установлен.
Путь Docker-сокета	Поле ввода пути или URI (универсальный идентификатор ресурса) Docker-сокета. Значение по умолчанию – /var/run/docker.sock.
Использовать CRI-O	Флажок включает или выключает использование среды CRI-O. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к конфигурационному файлу CRI-O. Значение по умолчанию: /etc/crio/crio.conf.
Использовать Podman	Флажок включает или выключает использование утилиты Podman. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты Podman. Значение по умолчанию: /usr/bin/podman.
Корневая директория	Поле ввода пути к корневой директории хранилища контейнеров. Значение по умолчанию: /var/lib/containers/storage.
Использовать runc	Флажок включает или выключает использование утилиты runc. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты runc. Значение по умолчанию: /usr/bin/runc.
Корневая директория	Поле ввода пути к корневой директории хранилища состояний контейнеров. Значение по умолчанию: /run/runc-ctrs.

Managed Detection and Response

Интеграция программы Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response (MDR) обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.

Таблица 150. Параметры Managed Detection and Response

Параметр	Описание
Managed Detection and Response включен / выключен	Переключатель включает или выключает интеграцию программы Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response. По умолчанию переключатель выключен.
Загрузить	По нажатию на кнопку открывается стандартное окно Microsoft Windows, в котором вы можете выбрать конфигурационный файл BLOB.

Параметры сети

Вы можете настроить параметры проверки зашифрованных соединений. Эти параметры используются в работе компонента Защита от веб-угроз (см. стр. 313).

При изменении параметров проверки зашифрованных соединений программа формирует событие *Параметры сети изменены (Network settings changed)*.

Таблица 151. Параметры сети

Параметр	Описание
Проверка зашифрованных соединений включена / выключена	Переключатель включает или выключает проверку зашифрованных соединений. По умолчанию переключатель включен.
Доверенные сертификаты	По ссылке **Настроить список доверенных сертификатов** открывается окно (см. раздел "Окно Доверенные сертификаты" на стр. 336), в котором вы можете настроить список доверенных сертификатов. Доверенные сертификаты используются при проверке зашифрованных соединений.
Действие при обнаружении недоверенного сертификата	Вы можете выбрать действие, которое будет выполнять программа при обнаружении недоверенного сертификата: • **Разрешить соединение** с доменом с недоверенным сертификатом (значение по умолчанию). • **Блокировать соединение** с доменом с недоверенным сертификатом.
Действие при ошибках во время проверки зашифрованных соединений	Вы можете выбрать действие, которое будет выполнять программа при возникновении ошибки во время проверки зашифрованных соединений: • **Добавить веб-сайт в исключения** (значение по умолчанию) – добавить домен, вызвавший ошибку, в список доменов с ошибками при проверке и не проверять зашифрованный сетевой трафик при посещении этого домена. • **Отключиться от веб-сайта** – заблокировать сетевое подключение.

Параметр	Описание
Политика проверки сертификатов	Вы можете выбрать способ проверки сертификатов программой: • **Локальная проверка** – программа не использует интернет для проверки сертификата. • **Полная проверка** (значение по умолчанию) – программа использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.
Доверенные домены	По ссылке **Настроить список доверенных доменов** открывается окно **Доверенные домены** (см. раздел "Окно Доверенные домены" на стр. 337).
Сетевые порты	По ссылке **Настроить параметры сетевых портов** открывается окно **Сетевые порты** (см. раздел "Окно Сетевые порты" на стр. 337), в котором вы можете указать, какие порты будет проверять программа.
Отслеживать все сетевые порты	Если выбран этот вариант, программа проверяет все сетевые порты.
Отслеживать только указанные порты	Если выбран этот вариант, программа проверяет только сетевые порты, указанные в окне **Сетевые порты** (см. раздел "Окно Сетевые порты" на стр. 337). Этот вариант выбран по умолчанию.

Окно Доверенные сертификаты

Вы можете настроить список сертификатов, которые программа Kaspersky Endpoint Security будет считать доверенными. Список доверенных сертификатов используется при проверке зашифрованных соединений.

Для каждого сертификата отображаются следующие сведения:

- субъект сертификата;
- серийный номер;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- отпечаток сертификата SHA-256.

По умолчанию список сертификатов пуст.

Вы можете добавлять (см. раздел "Окно добавления доверенного сертификата" на стр. 336) и удалять сертификаты.

Окно добавления доверенного сертификата

В этом окне вы можете добавить сертификат, который программа Kaspersky Endpoint Security будет считать доверенным.

По ссылке **Добавить сертификат** открывается стандартное окно для выбора файла. Укажите путь к файлу формата DER или PEM, содержащему сертификат.

После выбора файла сертификата в окне отображается информация о сертификате и путь к файлу.

Окно Доверенные домены

Список содержит доменные имена и маски доменных имен, которые будут исключены из проверки зашифрованных соединений. По умолчанию список пуст.

Вы можете добавлять, изменять и удалять домены в списке доверенных доменов.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно Сетевые порты

Таблица содержит сетевые порты, будет проверять программа, если в окне **Параметры сети** (см. стр. 335) выбран вариант **Отслеживать только указанные порты**.

Таблица содержит две графы:

- **Порт** – контролируемый порт.
- **Описание** – описание контролируемого порта.

По умолчанию в таблице отображается список сетевых портов, обычно используемых для передачи почтового и сетевого трафика. Список сетевых портов входит в пакет программы.

Элементы в таблице можно добавлять, настраивать и удалять.

Глобальные исключения

Таблица содержит точки монтирования, которые будут исключены из проверки компонентами программы, использующими перехватчик файловых операций (Защита от файловых угроз и Защита от шифрования).

В графе **Путь** отображается путь к исключенным точкам монтирования. По умолчанию таблица пустая.

Элементы в таблице можно добавлять, изменять и удалять (см. раздел "Окно добавления исключения точки монтирования" на стр. 338).

Окно добавления исключения точки монтирования

Таблица 152. Параметры точки монтирования

Параметр	Описание
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные директории. • **Смонтированная** – удаленные директории, смонтированные на компьютере по протоколу Samba или NFS. • **Все смонтированные** – все удаленные директории, смонтированные на компьютере по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательский** – ресурсы файловой системы компьютера, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите добавить в исключения из проверки. Для указания пути можно использовать маски. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.

Параметры Хранилища

Хранилище – это список резервных копий файлов, которые были удалены или изменены в процессе лечения. Резервная копия – копия файла, которая создается при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности. По умолчанию Хранилище расположено в директории /var/opt/kaspersky/kesl/common/objects-backup/. Файлы в Хранилище могут содержать персональные данные. Для доступа к файлам в Хранилище требуются root-права.

Таблица 153. Параметры Хранилища

Параметр	Описание
Информирование о необработанных файлах включено / выключено	Переключатель включает или выключает отправку уведомлений о необработанных во время проверки файлах на Сервер администрирования. По умолчанию переключатель включен.
Информирование об установленных устройствах включено / выключено	Переключатель включает или выключает передачу на Сервер администрирования информации об устройствах, установленных на вашем компьютере. По умолчанию переключатель включен.
Информирование о файлах в Хранилище включено / выключено	Переключатель включает или выключает отправку уведомлений о файлах в Хранилище на Сервер администрирования. По умолчанию переключатель включен.
Хранить объекты не более (дней)	Поле ввода для указания периода хранения объектов в Хранилище. Доступные значения: `0-3653`. Значение по умолчанию: `90`. Если задано значение `0`, период хранения объектов в Хранилище не ограничен.
Максимальный размер Хранилища (МБ)	Поле ввода для указания максимального размера Хранилища (в мегабайтах). Доступные значения: `0-999999`. Значение по умолчанию: `0` (размер Хранилища не ограничен).

Управление задачами в Web Console

Для управления программой с помощью Kaspersky Security Center Web Console вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного компьютера;
- групповые задачи, определенные для компьютеров, входящих в группы администрирования;
- задачи для наборов компьютеров, не входящих в группы администрирования.

  Задачи для наборов компьютеров выполняются только на компьютерах, указанных в параметрах задачи. Если в выборку компьютеров, для которой 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 задачи следующих типов:

- Антивирусная проверка (см. раздел "Антивирусная проверка. Раздел Параметры проверки" на стр. 343). Во время выполнения задачи программа проверяет области компьютера, указанные в параметрах задачи, на вирусы и другие вредоносные программы.
- Добавление ключа (см. стр. 365). Во время выполнения задачи программа добавляет ключ, в том числе резервный, для активации программы.
- Инвентаризация (см. раздел "Инвентаризация. Раздел Параметры проверки" на стр. 367). Во время выполнения задачи программа получает информацию обо всех исполняемых файлах программ, хранящихся на компьютерах.

- Обновление (см. раздел "Обновление. Раздел Источник обновлений баз" на стр. 365). Во время выполнения задачи программа обновляет базы в соответствии с настроенными параметрами обновления.
- Откат обновления баз. Во время выполнения задачи программа откатывает последнее обновление баз.
- Проверка важных областей (см. раздел "Проверка важных областей. Раздел Параметры проверки" на стр. 348). Во время выполнения задачи программа проверяет загрузочные секторы, объекты автозапуска, память процессов и память ядра.
- Проверка контейнеров (см. раздел "Проверка контейнеров. Раздел Параметры проверки" на стр. 357). Во время выполнения задачи программа проверяет контейнеры и образы на вирусы и другие вредоносные объекты.
- Проверка целостности системы (см. раздел "Проверка целостности системы. Раздел Параметры проверки" на стр. 354). Во время выполнения задачи программа определяет изменение каждого объекта путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.

Задачи выполняются, только если на компьютерах запущена программа Kaspersky Endpoint Security.

Вы можете выполнять следующие действия над задачами:

- Создавать новые задачи (см. раздел "Создание задачи" на стр. 340).
- Изменять параметры задач (см. раздел "Изменение параметров задачи" на стр. 341).

  Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения. Кроме того, некоторые параметры могут быть недоступны для настройки и использования в сертифицированной версии программы.

- Управлять задачами (см. раздел "Действия с задачами" на стр. 341).

Общая информация о задачах в Web Console приведена в документации для Kaspersky Security Center.

В этом разделе

Создание задачи

► *Чтобы создать задачу:*

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится **Мастер добавления задачи**.

3. Настройте параметры задачи:
   a. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Security 11.3.0 для Linux**.
   b. В раскрывающемся списке **Тип задачи** выберите задачу (см. раздел "Управление задачами в Web Console" на стр. 339), которую вы хотите запустить на компьютерах пользователей.
   c. В поле **Название задачи** введите короткое описание, например, `Обновление программы`.
   d. В разделе **Выбор устройств, которым будет назначена задача** выберите область действия задачи.
4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.
5. Завершите работу мастера по кнопке **Готово**.

В списке задач отобразится новая задача. Задача будет иметь параметры по умолчанию. Для настройки параметров задачи (см. раздел "Изменение параметров задачи" на стр. 341) вам нужно перейти в свойства задачи. Для выполнения задачи вам нужно установить флажок напротив задачи и нажать на кнопку **Запустить**.

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

Изменение параметров задачи

► *Чтобы изменить параметры задачи:*

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

   Откроется список задач.
2. В списке задач выберите задачу, параметры которой вы хотите изменить.
3. Измените параметры задачи.
4. Нажмите на кнопку **Сохранить**.

Задача будет сохранена с обновленными параметрами.

Действия с задачами

► *Чтобы запустить, приостановить, возобновить, остановить, удалить, скопировать или переместить задачу*

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

   Откроется список задач.

2. В списке задач выберите задачу, которую вы хотите запустить, приостановить, возобновить, остановить, удалить, скопировать или переместить, и нажмите на соответствующую кнопку (если она доступна).

Параметры задач

Для работы с программой Kaspersky Endpoint Security через Web Console вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного клиентского компьютера;
- групповые задачи, определенные для клиентских компьютеров, входящих в группы администрирования;
- задачи для выборки компьютеров.

Вы можете создавать любое количество групповых задач, задач для выборки компьютеров и локальных задач. Дополнительная информация о работе с группами администрирования и выборками компьютеров приведена в документации Kaspersky Security Center.

Набор и значения по умолчанию для параметров задачи могут отличаться в зависимости от типа лицензии на программу (https://support.kaspersky.ru/15471). Кроме того, некоторые параметры могут быть недоступны для настройки и использования в сертифицированной версии программы.

В этом разделе

kaspersky

Антивирусная проверка. Раздел Параметры проверки

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

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

Во время полной проверки диска процессор компьютера будет занят. Рекомендуется запускать задачу полной проверки в нерабочее время.

Вы также можете создавать пользовательские задачи антивирусной проверки.

Таблица 154. Параметры проверки задачи Антивирусная проверка

Параметр	Описание
Приоритет задачи	В этом блоке параметров вы можете выбрать приоритет выполнения задачи: • **Низкий** – задача выполняется с низким приоритетом: не более 10% потребления ресурсов процессора. Выполнение задачи занимает больше времени, но программа выделяет ресурсы на выполнение других задач. • **Нормальный** (значение по умолчанию) – задача выполняется со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. • **Высокий** – задача выполняется с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, программа проверяет архивы. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, программа не проверяет архивы. По умолчанию флажок установлен.

Параметр	Описание
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, программа проверяет самораспаковывающиеся архивы. Если флажок снят, программа не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз программ Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, программа проверяет файлы почтовых баз. Если флажок снят, программа не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, программа проверяет сообщения в текстовом формате. Если флажок снят, программа не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Прервать проверку, если она длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки объекта в секундах. После истечения указанного времени программа прекращает проверку объекта. Доступные значения: `0–9999`. Если указано значение `0`, время проверки не ограничено. Значение по умолчанию: `0`.
Пропускать объекты размером более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0–999999`. Если установлено значение `0`, программа проверяет объекты любого размера. Значение по умолчанию: `0`.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, программа записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, программа не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.

Параметр	Описание
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, программа записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, программа не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, программа записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, программа не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, программа проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, программа проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое программа будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое программа будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).
Области проверки	Таблица, содержащая области, проверяемые задачей. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы. Области проверки в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Таблица 155. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки** (см. раздел "Окно Области проверки" на стр. 220). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область проверки во время работы. Если флажок снят, программа не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. • **Смонтированная** – смонтированные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все смонтированные** – все смонтированные директории. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательский** – ресурсы файловой системы компьютера, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. По умолчанию указан путь */* – программа проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, программа проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Антивирусная проверка. Раздел Области проверки

Вы можете настроить параметры области проверки для задачи Антивирусная проверка. Программа позволяет проверять файлы, загрузочные секторы, память компьютера и объекты автозапуска.

Таблица 156. Параметры области проверки задачи Антивирусная проверка

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, программа проверяет файлы. Если флажок снят, программа не проверяет файлы. По умолчанию флажок установлен.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, программа проверяет загрузочные секторы. Если флажок снят, программа не проверяет загрузочные секторы. По умолчанию флажок снят.
Проверять память компьютера	Флажок включает или выключает проверку памяти компьютера. Если флажок установлен, программа проверяет память процессов и память ядра. Если флажок снят, программа не проверяет память процессов и память ядра. По умолчанию флажок снят.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, программа проверяет объекты автозапуска. Если флажок снят, программа не проверяет объекты автозапуска. По умолчанию флажок снят.
Устройства для проверки	По ссылке **Настроить маски устройств** открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должна проверять программа. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

Антивирусная проверка. Раздел Области исключения

В разделе **Области исключения** для задачи Антивирусная проверка вы можете настроить области исключения, исключения по маске (см. раздел "Окно Исключения по маске" на стр. 309) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 227).

Проверка важных областей. Раздел Параметры проверки

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

Таблица 157. Параметры задачи Проверка важных областей

Параметр	Описание
Приоритет задачи	В этом блоке параметров вы можете выбрать приоритет выполнения задачи: • **Низкий** – задача выполняется с низким приоритетом: не более 10% потребления ресурсов процессора. Выполнение задачи занимает больше времени, но программа выделяет ресурсы на выполнение других задач. • **Нормальный** (значение по умолчанию) – задача выполняется со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. • **Высокий** – задача выполняется с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, программа проверяет архивы. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, программа не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, программа проверяет самораспаковывающиеся архивы. Если флажок снят, программа не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз программ Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, программа проверяет файлы почтовых баз. Если флажок снят, программа не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, программа проверяет сообщения в текстовом формате. Если флажок снят, программа не проверяет сообщения в текстовом формате. По умолчанию флажок снят.

Параметр	Описание
Прервать проверку, если она длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки объекта в секундах. После истечения указанного времени программа прекращает проверку объекта. Доступные значения: `0–9999`. Если указано значение `0`, время проверки не ограничено. Значение по умолчанию: `0`.
Пропускать объекты размером более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0–999999`. Если установлено значение `0`, программа проверяет объекты любого размера. Значение по умолчанию: `0`.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, программа записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, программа не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных файлах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, программа записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, программа не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, программа записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, программа не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, программа проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, программа проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.

Параметр	Описание
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое программа будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое программа будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).
Области проверки	Таблица, содержащая области, проверяемые задачей. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы. Области проверки в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Таблица 158. Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки** (см. раздел "Окно Области проверки" на стр. 220). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область проверки во время работы. Если флажок снят, программа не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. • **Смонтированная** – смонтированные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все смонтированные** – все смонтированные директории. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на компьютере по протоколу NFS. • **Samba** – удаленные директории, смонтированные на компьютере по протоколу Samba. • **Пользовательский** – ресурсы файловой системы компьютера, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. По умолчанию указан путь */* – программа проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, программа проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.

Параметр	Описание
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Проверка важных областей. Раздел Области проверки

Вы можете настроить параметры области проверки для задачи Проверка важных областей. Программа позволяет проверять файлы, загрузочные секторы, память компьютера и объекты автозапуска.

Таблица 159. Параметры области проверки задачи Проверка важных областей

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, программа проверяет файлы. Если флажок снят, программа не проверяет файлы. По умолчанию флажок снят.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, программа проверяет загрузочные секторы. Если флажок снят, программа не проверяет загрузочные секторы. По умолчанию флажок установлен.
Проверять память компьютера	Флажок включает или выключает проверку памяти компьютера. Если флажок установлен, программа проверяет память процессов и память ядра. Если флажок снят, программа не проверяет память процессов и память ядра. По умолчанию флажок установлен.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, программа проверяет объекты автозапуска. Если флажок снят, программа не проверяет объекты автозапуска. По умолчанию флажок установлен.
Устройства для проверки	По ссылке **Настроить маски устройств** открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должна проверять программа. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

kaspersky

Проверка важных областей. Раздел Области исключения

В разделе **Области исключения** для задачи Проверка важных областей вы можете настроить области исключения, исключения по маске (см. раздел "Окно Исключения по маске" на стр. 309) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 227).

Проверка целостности системы. Раздел Параметры проверки

В процессе выполнения задачи Проверка целостности системы (ODFIM) изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве *снимка состояния системы*.

Снимок состояния системы определяется во время первого выполнения задачи ODFIM на компьютере. Вы можете создать несколько задач ODFIM. Для каждой задачи ODFIM создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы относится к области мониторинга. Если снимок состояния системы не соответствует области мониторинга, программа Kaspersky Endpoint Security создает событие о нарушении целостности системы.

Снимок состояния системы создается заново после завершения задачи ODFIM. Вы можете заново создать снимок состояния системы для задачи с помощью соответствующего параметра. Снимок состояния системы также создается при изменении параметров задачи, например, при добавлении новой области мониторинга. При следующем выполнении задачи снимок состояния системы формируется заново. Вы можете удалить снимок состояния системы, удалив соответствующую задачу ODFIM.

Задача ODFIM создает хранилище для снимков состояния системы на компьютере с установленным компонентом Контроль целостности системы.

Таблица 160. Параметры задачи Проверка целостности системы

Параметр	Описание
Обновлять снимок состояния системы при каждом запуске задачи	Флажок включает или выключает обновление снимка состояния системы при каждом запуске задачи Проверка целостности системы. По умолчанию флажок снят.
Использовать хеш (SHA-256) для проверки	Флажок включает или выключает использование хеша SHA-256 для задачи Проверка целостности системы. SHA-256 – это криптографическая хеш-функция, которая формирует 256-разрядное хеш-значение. 256-разрядное хеш-значение представляет собой последовательность из 64 шестнадцатеричных цифр. По умолчанию флажок снят.
Следить за директориями в областях мониторинга	Флажок включает или выключает проверку указанных директорий во время выполнения задачи Проверка целостности системы. По умолчанию флажок снят.
Следить за временем последнего доступа к файлу	Флажок включает или выключает отслеживание времени доступа к файлу во время выполнения задачи Проверка целостности системы. По умолчанию флажок снят.

Параметр	Описание
Области мониторинга	Таблица, содержащая области мониторинга, проверяемые задачей. По умолчанию таблица содержит область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/). Области мониторинга в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область мониторинга для задачи Проверка целостности системы.

Таблица 161. Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице раздела **Параметры проверки** (см. раздел "Проверка целостности системы. Раздел Параметры проверки" на стр. 354). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область мониторинга во время работы. Если флажок снят, программа не обрабатывает эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Поле не должно быть пустым. По умолчанию указан путь **/** – программа проверяет все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Проверка целостности системы. Раздел Области исключения

В разделе **Области исключения** для задачи Проверка целостности системы вы можете настроить исключения из мониторинга (см. раздел "Окно Области исключения" на стр. 246) и исключения по маске (см. раздел "Окно Исключения по маске" на стр. 247).

Окно Области исключения

Таблица содержит области исключения из мониторинга для компонента Контроль целостности системы. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 162. Параметры области исключения из мониторинга Контроля целостности системы

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли программа эту область из мониторинга при работе компонента.

Элементы в таблице можно добавлять, изменять и удалять.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения из мониторинга для компонента Контроль целостности системы.

Таблица 163. Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения** (см. раздел "Окно Области исключения" на стр. 246). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы программы. Если флажок установлен, программа исключает эту область из мониторинга во время работы компонента. Если флажок снят, программа отслеживает эту область во время работы компонента. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Поле не должно быть пустым. По умолчанию указан путь */* – программа исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые программа исключает из мониторинга. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

kaspersky

Проверка контейнеров. Раздел Параметры проверки

Во время работы задачи Проверка контейнеров программа проверяет контейнеры и образы на вирусы и вредоносные программы. Вы можете одновременно запустить несколько задач Проверка контейнеров.

Для использования задачи требуется лицензия, которая включает эту функцию.

Таблица 164. Параметры задачи Проверка контейнеров

Параметр	Описание
Приоритет задачи	В этом блоке параметров вы можете выбрать приоритет выполнения задачи: • **Низкий** – задача выполняется с низким приоритетом: не более 10% потребления ресурсов процессора. Выполнение задачи занимает больше времени, но программа выделяет ресурсы на выполнение других задач. • **Нормальный** (значение по умолчанию) – задача выполняется со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. • **Высокий** – задача выполняется с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, программа проверяет архивы. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, программа не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, программа проверяет самораспаковывающиеся архивы. Если флажок снят, программа не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз программ Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, программа проверяет файлы почтовых баз. Если флажок снят, программа не проверяет файлы почтовых баз. По умолчанию флажок снят.

Параметр	Описание
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, программа проверяет сообщения в текстовом формате. Если флажок снят, программа не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Прервать проверку, если она длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки объекта в секундах. После истечения указанного времени программа прекращает проверку объекта. Доступные значения: `0–9999`. Если указано значение `0`, время проверки не ограничено. Значение по умолчанию: `0`.
Пропускать объекты размером более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0–999999`. Если установлено значение `0`, программа проверяет объекты любого размера. Значение по умолчанию: `0`.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, программа записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, программа не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, программа записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, программа не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, программа записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, программа не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.

Параметр	Описание
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, программа проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, программа проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке объектов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое программа будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое программа будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Удалять** объект. Копия зараженного объекта будет сохранена в Хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).

Параметр	Описание
Проверять контейнеры	Флажок включает или выключает проверку контейнеров. Если флажок установлен, вы можете указать имя или маску имени проверяемых контейнеров. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых контейнеров. По умолчанию указана маска ***** – выполняется проверка всех контейнеров.
Действие при обнаружении угрозы	Вы можете выбрать действие, которое программа будет выполнять над контейнером при обнаружении зараженного объекта: • **Пропустить контейнер** – не выполнять никаких действий над контейнером при обнаружении зараженного объекта. • **Остановить контейнер** – остановить контейнер при обнаружении зараженного объекта. • **Остановить контейнер, если не удалось вылечить** (значение по умолчанию) – остановить контейнер, если не удалось вылечить зараженный объект или устранить угрозу.
Проверять образы	Флажок включает или выключает проверку образов. Если флажок установлен, вы можете указать имя или маску имени проверяемых образов. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых образов. По умолчанию указана маска ***** – выполняется проверка всех образов.
Действие при обнаружении угрозы	Вы можете выбрать действие, которое программа будет выполнять над образом при обнаружении зараженного объекта: • **Пропустить образ** (значение по умолчанию) – не выполнять никаких действий над образом при обнаружении зараженного объекта. • **Удалить образ** при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.
Проверять каждый слой	Флажок включает или выключает проверку всех слоев образов и запущенных контейнеров. По умолчанию флажок снят.

Проверка контейнеров. Раздел Области исключения

В разделе **Области исключения** для задачи Проверка контейнеров вы можете настроить исключения по маске (см. раздел "Окно Исключения по маске" на стр. 227) и по названию угрозы (см. раздел "Окно Исключения по названию угрозы" на стр. 227).

Инвентаризация. Раздел Параметры проверки

Задача Инвентаризация позволяет получить информацию обо всех исполняемых файлах программ, хранящихся на компьютерах. Получение информации о программах, установленных на компьютерах,

может быть полезно, например, для создания правил контроля программ (см. раздел "О правилах контроля программ" на стр. 193).

Для использования задачи требуется лицензия, которая включает эту функцию.

В базе данных Kaspersky Security Center может храниться информация о 150 000 обработанных файлов. При достижении этого количества записей новые файлы не будут обработаны. Для возобновления работы инвентаризации требуется удалить с компьютера, на котором установлена программа Kaspersky Endpoint Security, файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

Таблица 165. Параметры задачи Инвентаризация

Параметр	Описание
Приоритет задачи	В этом блоке параметров вы можете выбрать приоритет выполнения задачи: • **Низкий** – задача выполняется с низким приоритетом: не более 10% потребления ресурсов процессора. Выполнение задачи занимает больше времени, но программа выделяет ресурсы на выполнение других задач. • **Нормальный** (значение по умолчанию) – задача выполняется со стандартным приоритетом: не более 50% потребления ресурсов всех процессоров. • **Высокий** – задача выполняется с высоким приоритетом, без ограничения потребления ресурсов процессора. Выберите это значение, если вы хотите, чтобы текущая задача выполнялась быстрее.
Создать золотой образ	Флажок включает или выключает создание категории программ "Golden Image" на основе списка программ, обнаруженных на компьютере задачей Инвентаризация. Если флажок установлен, то в правилах контроля программ (см. раздел "О правилах контроля программ" на стр. 193) вы можете использовать категорию программ "Golden Image". По умолчанию флажок снят.
Проверять все исполняемые файлы	Флажок включает или выключает проверку исполняемых файлов. По умолчанию флажок установлен.
Проверять двоичные файлы	Флажок включает или выключает проверку двоичных файлов (с расширениями elf, java и pyc). По умолчанию флажок установлен.
Проверять скрипты	Флажок включает или выключает проверку скриптов. По умолчанию флажок установлен.
Области инвентаризации	Таблица, содержащая области инвентаризации, проверяемые задачей. По умолчанию таблица содержит одну область проверки – /usr/bin. Области инвентаризации в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки для задачи Инвентаризация.

Таблица 166. Параметры области инвентаризации

Параметр	Описание
Название области проверки	Поле ввода названия области инвентаризации. Это название будет отображаться в таблице раздела **Параметры проверки** (см. раздел "Инвентаризация. Раздел Параметры проверки" на стр. 367). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы программы. Если флажок установлен, программа обрабатывает эту область инвентаризации во время работы. Если флажок снят, программа не обрабатывает эту область инвентаризации во время работы. В дальнейшем вы можете включить эту область в параметры работы программы, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область инвентаризации. Поле не должно быть пустым. По умолчанию указан путь **/** – программа проверяет все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые программа проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Инвентаризация. Раздел Области исключения

В разделе **Области исключения** для задачи Инвентаризация вы можете настроить области исключения из проверки.

Окно Области исключения

Таблица содержит области исключения из проверки. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Таблица 167. Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, применяется ли это исключение в работе программы.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения из проверки для задачи Инвентаризация.

Таблица 168. Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения** (см. раздел "Окно Области исключения" на стр. 225). Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время выполнения задачи. Если флажок установлен, Kaspersky Endpoint Security исключает эту область во время выполнения задачи. Если флажок снят, Kaspersky Endpoint Security включает эту область во время выполнения задачи. В дальнейшем вы можете исключить эту область из проверки, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения из инвентаризации. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые Kaspersky Endpoint Security исключает из проверки. Вы можете добавлять, изменять и удалять маски.

Добавление ключа

С помощью задачи Добавление ключа вы можете добавить ключ для активации программы Kaspersky Endpoint Security.

Таблица 169. Параметры задачи Добавление ключа

Параметр	Описание
Использовать ключ в качестве резервного	Флажок включает или выключает использование ключа в качестве резервного. Если флажок установлен, программа использует ключ в качестве резервного. Если флажок снят, программа использует ключ в качестве активного. По умолчанию флажок снят. Флажок недоступен, если вы добавляете ключ для пробной лицензии или ключ по подписке. Ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве резервного ключа.
Информация о лицензии	В этом блоке приведены данные о ключе и связанной с ним лицензии: • **Ключ** – уникальная буквенно-цифровая последовательность. Вы можете использовать программу только при наличии в ней ключа. • **Тип лицензии** – пробная, коммерческая или коммерческая (подписка). • **Срок действия лицензии** – количество дней, в течение которых возможно использование программы, активированной путем добавления этого ключа (например, 365 дней). Информация не отображается, если вы используете программу по подписке. • **Действует до** – дата и время окончания срока использования программы, активированной путем добавления этого ключа, в формате UTC. Если вы используете программу по неограниченной подписке, дата окончания срока годности ключа не указывается. • **Ограничение** – максимальное количество устройств, которые программа может защищать. • **Название программы** – название программы, для активации которой вы добавляете ключ.
Добавить	При нажатии на кнопку открывается окно **Хранилище ключей Kaspersky Security Center** (см. раздел "Окно Хранилище ключей Kaspersky Security Center" на стр. 363). В этом окне вы можете выбрать ключ, ранее добавленный в хранилище ключей Kaspersky Security Center, а также добавить ключ в хранилище ключей Kaspersky Security Center.

Окно Хранилище ключей Kaspersky Security Center

В этом окне вы можете выбрать ключ, ранее добавленный в хранилище ключей Kaspersky Security Center, а также добавить ключ в хранилище ключей Kaspersky Security Center.

Таблица 170. Параметры окна Хранилище ключей Kaspersky Security Center

Параметр	Описание
Таблица ключей	Таблица содержит ключи, добавленные в хранилище ключей Kaspersky Security Center, и состоит из следующих граф: • **Тип лицензии** – тип лицензии: пробная, коммерческая или коммерческая (подписка). • **Действует до** – дата окончания срока использования программы, активированной путем добавления этого ключа. • **Льготный период** – льготный период. • **Ограничение** – максимальное количество устройств, которые программа может защищать. • **Название программы** – название программы, для активации которой добавлен ключ. • **Ключ** – уникальная буквенно-цифровая последовательность.
Добавить ключ	При нажатии на кнопку запускается Мастер добавления лицензионного ключа. Ключ будет добавлен в хранилище ключей Kaspersky Security Center. После добавления ключа информация о нем будет отображаться в таблице ключей.

Обновление. Раздел Источник обновлений баз

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 программы. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули программы.

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

Таблица 171. Параметры источников обновлений задачи Обновление

Параметр	Описание
Источник обновлений баз	В этом разделе вы можете выбрать источник обновлений: • **Серверы обновлений "Лаборатории Касперского"**, на которых публикуются обновления баз для программ "Лаборатории Касперского" (значение по умолчанию). • **Сервер администрирования Kaspersky Security Center** (этот вариант доступен только для Web Console). • **Точки распространения** (этот вариант доступен только для Kaspersky Security Center Cloud Console). • **Другие источники в локальной или глобальной сети** – HTTP-, HTTPS- и FTP-серверы или директории на серверах локальной сети.

Параметр	Описание
Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны	Флажок включает или выключает использование серверов обновлений "Лаборатории Касперского" в качестве источника обновлений, если выбранные источники обновлений недоступны. Флажок доступен, если выбран вариант **Другие источники в локальной или глобальной сети** или **Сервер администрирования Kaspersky Security Center**. По умолчанию флажок установлен.
Пользовательские источники обновлений	Таблица содержит список пользовательских источников обновлений баз. В процессе обновления программа обращается к источникам обновлений в том порядке, в котором эти ресурсы указаны в таблице. Таблица содержит следующие графы: • **Источник обновлений** – HTTP-, HTTPS- или FTP-серверы или директории на серверах локальной сети. • Переключатель показывает, будет ли источник использоваться в задаче (**Включено** или **Выключено**). Вы можете включить или выключить переключатель в таблице, а также установить или снять флажок **Использовать этот источник** в окне **Источник обновлений**, которое открывается по ссылке с названием источника). Таблица доступна, если выбран вариант **Другие источники в локальной или глобальной сети**. По умолчанию таблица пустая. Источники обновлений в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Обновление. Раздел Параметры

В разделе **Параметры** вы можете указать время ожидания ответа и параметры загрузки обновлений программы.

Таблица 172. Параметры задачи Обновление

Параметр	Описание
Максимальное время ожидания ответа от источника обновлений (сек.)	Предельный период ожидания ответа на запрос программы от выбранного источника обновлений. При отсутствии ответа по истечении этого времени в журнал выполнения задач записывается событие о нарушении связи с источником обновлений. Доступные значения: `0–120`. Если указано значение `0`, период ожидания ответа на запрос программы от выбранного источника не ограничен. Значение по умолчанию: `10`.
Режим загрузки обновлений программы	В раскрывающемся списке вы можете выбрать режим обновления баз программы: • **Не загружать** файлы обновлений (значение по умолчанию). Обновить программу невозможно. • **Только загружать** файлы обновлений, но не устанавливать их на компьютеры пользователей. • **Загружать и устанавливать** файлы обновлений на компьютеры пользователей. Для сохранения сертифицированной конфигурации программы требуется установить значение параметра **Не загружать**.

Откат обновления баз

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

Каждый раз, когда пользователь запускает процесс обновления, программа Kaspersky Endpoint Security создает резервную копию текущих баз программы. Это позволяет при необходимости откатить базы программы до предыдущей версии.

Откат последнего обновления баз используется, например, если новая версия баз программы содержит недопустимые сигнатуры, что приводит к блокировке безопасных программ программой Kaspersky Endpoint Security.

Задача Откат обновления баз не имеет параметров.

kaspersky

Управление программой с помощью графического пользовательского интерфейса

Вы можете управлять работой программы Kaspersky Endpoint Security с помощью графического пользовательского интерфейса.

В этом разделе

Интерфейс программы

Значок программы в области уведомлений

После установки пакета графического пользовательского интерфейса программы Kaspersky Endpoint Security значок программы появляется справа в области уведомлений панели задач.

Значок программы обеспечивает доступ к контекстному меню и главному окну программы. Вы можете открыть контекстное меню значка программы, нажав правой клавишей мыши по значку программы в области уведомлений.

Контекстное меню значка программы содержит следующие пункты:

- **Kaspersky Endpoint Security 11.3.0 для Linux**. Открывает главное окно программы, в котором отображается состояние защиты вашего компьютера и находятся элементы интерфейса, предоставляющие доступ к функциям программы.
- **Выход**. Выполняет выход из графического пользовательского интерфейса программы.

Главное окно программы

Главное окно программы разделено на несколько частей:

- В центральной части главного окна программы отображается статус защиты вашего компьютера. При нажатии клавишей мыши на этой области окна открывается окно **Центр защиты**. В этом окне отображается информация о состоянии защиты вашего компьютера и рекомендации о действиях, которые вам нужно выполнить для устранения проблем в защите (при их наличии).
- На кнопке **Проверка** отображается состояние задачи антивирусной проверки и количество обнаруженных угроз. При нажатии на эту кнопку открывается окно **Проверка**. В этом окне вы можете запустить и остановить задачи **Антивирусная проверка**, **Проверка важных областей** и

Проверка контейнеров (см. раздел "Запуск и остановка задач проверки" на стр. 371). Вы также можете просмотреть отчеты для этих задач.

- На кнопке **Обновление** отображается состояние задачи **Обновление**. При нажатии на эту кнопку открывается окно **Обновление**. В этом окне вы можете запустить задачи (см. раздел "Запуск и остановка задач обновления" на стр. 371) **Обновление** и **Откат обновления баз**. Вы также можете просмотреть отчеты для этих задач.
- В нижней части главного окна программы находятся следующие элементы:
  - Кнопка **Отчеты**. При нажатии на эту кнопку открывается окно **Отчеты**, в котором вы можете просмотреть статистику работы задач и различные отчеты (см. раздел "Просмотр отчетов" на стр. 373).
  - Кнопка **Хранилище**. При нажатии на эту кнопку открывается окно **Хранилище**, в котором содержится информация об объектах в Хранилище (см. раздел "Просмотр объектов в Хранилище" на стр. 374).
  - Кнопка **Настройка**. При нажатии на эту кнопку открывается окно **Настройка**, в котором вы можете включить или выключить мониторинговые задачи программы, а также участие в Kaspersky Security Network.
  - Кнопка **Поддержка**. При нажатии на эту кнопку открывается окно **Поддержка**, в котором содержится информация о текущей версии программы, лицензионном ключе, состоянии баз программы, операционной системе, а также ссылки на информационные ресурсы "Лаборатории Касперского".
- В нижней части главного окна программы отображается информация о лицензии и о ключе, а также о проблемах лицензирования (при их наличии). При нажатии клавишей мыши на этой области окна открывается окно **Лицензия**. В этом окне отображается подробная информация о лицензии (см. раздел "Просмотр информации о лицензии" на стр. 375). Также вы можете открыть это окно из окна **Поддержка** по ссылке с лицензионным ключом.

Вы можете открыть главное окно программы одним из следующих способов:

- По правой клавише мыши или двойным щелчком мыши по значку программы в области уведомлений панели задач.
- Выбрав название программы в меню приложений оконного менеджера операционной системы.

Управление задачами

Графический пользовательский интерфейс программы позволяет включать и выключать следующие мониторинговые задачи программы:

- Защита от файловых угроз (см. раздел "Задача Защита от файловых угроз (File_Threat_Protection, ID:1)" на стр. 108).
- Контроль целостности системы (см. раздел "Задача Контроль целостности системы (System_Integrity_Monitoring, ID:11)" на стр. 156).
- Управление сетевым экраном.
- Защита от шифрования (см. раздел "Задача Защита от шифрования (Anti_Cryptor, ID:13)" на стр. 163).
- Защита от веб-угроз (см. раздел "Задача Защита от веб-угроз (Web_Threat_Protection, ID:14)" на стр. 169).
- Контроль устройств.

- Проверка съемных дисков (см. раздел "Задача Проверка съемных дисков (Removable_Drives_Scan, ID:16)" на стр. 172).
- Защита от сетевых угроз.
- Анализ поведения (см. раздел "Задача Анализ поведения (Behavior_Detection, ID:20)" на стр. 191).
- Контроль программ (см. раздел "Задача Контроль программ (Application_Control, ID:21)" на стр. 192).

Графический пользовательский интерфейс программы позволяет также запускать следующие задачи по требованию:

- Антивирусная проверка (см. раздел "Задача Антивирусная проверка (Scan_My_Computer, ID:2)" на стр. 120).
- Выборочная проверка (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 129) (запускается при нажатии клавишей мыши на файле или директории, которые вы хотите проверить).
- Проверка важных областей (см. раздел "Задача Проверка важных областей (Critical_Areas_Scan, ID:4)" на стр. 138).
- Проверка целостности системы (см. раздел "Контроль целостности системы по требованию (ODFIM)" на стр. 157).
- Проверка контейнеров (см. раздел "Задача Проверка контейнеров (Container_Scan, ID:18)" на стр. 174).
- Обновление (см. раздел "Задача Обновление (Update, ID:6)" на стр. 146).
- Откат обновления баз (см. раздел "Задача Откат обновления баз (Rollback, ID:7)" на стр. 150).

Кроме того, вы можете управлять своим участием в Kaspersky Security Network.

Несмотря на то, что параметры некоторых из этих функций отображаются в графическом пользовательском интерфейсе, невозможно использовать эти функции и настроить их параметры.

Включение и выключение мониторинговых задач программы

Вы можете включать и выключать мониторинговые задачи (см. раздел "Управление задачами" на стр. 369) программы. Если задача включена, доступна кнопка **Выключить**. По умолчанию включены задачи Защита от файловых угроз и Анализ поведения.

Если задача выключена, доступна кнопка **Включить**.

► *Чтобы включить или выключить мониторинговую задачу программы:*

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

   Откроется окно **Настройка**.
3. Выполните следующие действия для нужной задачи:
   - Если вы хотите включить задачу, нажмите на кнопку **Включить**.
   - Если вы хотите выключить задачу, нажмите на кнопку **Выключить**.

Запуск и остановка задач проверки

С помощью графического пользовательского интерфейса программы вы можете запускать и останавливать задачи **Антивирусная проверка**, **Проверка важных областей** и **Проверка контейнеров**.

► *Чтобы запустить или остановить задачу проверки:*

1. Откройте главное окно программы.
2. В главном окне программы нажмите на раздел **Проверка**.

   Откроется окно **Проверка**.
3. Выполните одно из следующих действий:
   - Если вы хотите запустить задачу проверки, нажмите на кнопку **Запустить**, расположенную под той задачей проверки, которую вы хотите запустить.

     Отобразится ход выполнения задачи проверки.
   - Если вы хотите остановить задачу проверки, нажмите на кнопку **Остановить**, расположенную под той задачей проверки, которую вы хотите остановить.

     Задача проверки остановится, отобразится информация о проверенных объектах и обнаруженных угрозах.
4. Если вы хотите просмотреть отчет по задаче проверки, нажмите на кнопку **Показать отчет**.

При обнаружении зараженного объекта или при завершении задачи проверки отображается всплывающее окно в области уведомлений рядом со значком программы в правой части панели задач.

Также в окне **Проверка** отображается ход выполнения и результат работы временных задач Scan_Boot_Sectors_{идентификатор} и Scan_File_{идентификатор}. Вы можете скрыть информацию о выполненных временных задачах, нажав на крестик или закрыв окно **Проверка** (при переходе в главное окно или при выходе из программы (см. раздел "Интерфейс программы" на стр. 368)).

Запуск и остановка задач обновления

С помощью графического пользовательского интерфейса программы вы можете запускать задачи **Обновление** и **Откат обновления баз**.

► *Чтобы запустить или остановить задачу обновления:*

1. Откройте главное окно программы.
2. В главном окне программы нажмите на раздел **Обновление**.

   Откроется окно **Обновление**.
3. Выполните одно из следующих действий:
   - Если вы хотите запустить задачу, нажмите на кнопку **Запустить**, расположенную под той задачей, которую вы хотите запустить.

     Отобразится ход выполнения задачи обновления.

     При успешном завершении задачи обновления становится доступна ссылка **Откатить обновление**, с помощью которой вы можете откатить последнее успешное обновление баз.

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

  Задача обновления остановится.

4. Если вы хотите просмотреть отчет по задаче, нажмите на кнопку **Показать отчет**.

► *Чтобы запустить задачу отката обновления баз:*

1. Откройте главное окно программы.
2. В главном окне программы нажмите на раздел **Обновление**.

   Откроется окно **Обновление**.
3. Запустите задачу отката обновления баз по ссылке **Откатить обновление**.

Управление участием в Kaspersky Security Network

С помощью графического пользовательского интерфейса вы можете включать или выключать использование Kaspersky Security Network.

В сертифицированной версии программы используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается, так как приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

► *Чтобы включить использование Kaspersky Security Network:*

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

   Откроется окно **Настройка**.
3. Выберите один из следующих вариантов:
   - **Kaspersky Security Network со статистикой**, если вы хотите использовать Kaspersky Security Network, получать информацию из базы знаний и отправлять анонимную статистику и данные о типах и источниках угроз.
   - **Kaspersky Security Network без статистики**, если вы хотите использовать Kaspersky Security Network, получать информацию из базы знаний, но не отправлять анонимную статистику и данные о типах и источниках угроз.
4. Нажмите на кнопку **Включить**.
5. В окне **Участие в Kaspersky Security Network** внимательно прочитайте Положение о Kaspersky Security Network и выберите один их следующих вариантов:
   - **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**, если вы хотите использовать Kaspersky Security Network.
   - **Я не принимаю условия использования Kaspersky Security Network**, если вы хотите отказаться от использования Kaspersky Security Network.
6. Нажмите **ОК**.

Кнопка **ОК** недоступна, если в окне **Участие в Kaspersky Security Network** не выбран ни один из вариантов.

► *Чтобы выключить использование Kaspersky Security Network:*

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

   Откроется окно **Настройка**.
3. Нажмите на кнопку **Выключить**.
4. В открывшемся окне выполните одно из следующих действий:
   - Нажмите на кнопку **Да**, чтобы отказаться от использования Kaspersky Security Network.
   - Нажмите на кнопку **Отмена**, чтобы продолжать участвовать в Kaspersky Security Network.

Просмотр отчетов

Информация о работе задач программы записывается в отчеты программы.

Данные в отчетах представлены в виде таблицы, которая содержит список событий. Каждая строка в таблице содержит информацию об отдельном событии. Атрибуты события отображаются в графах таблицы. События, зарегистрированные в работе разных задач, имеют разный набор атрибутов.

В отчетах предусмотрены следующие уровни важности событий:

- Критический – события критической важности, на которые нужно обратить внимание, поскольку они указывают на проблемы в работе программы или на уязвимости в защите компьютера.
- Высокий.
- Средний.
- Низкий.
- Информационный.
- Ошибка.

В программе доступны следующие отчеты, перечисленные в окне **Отчеты** слева:

- **Статистика**. Этот отчет содержит статистические данные о задаче Защита от файловых угроз и задачах проверки. Вы можете обновить отображаемый отчет, нажав на кнопку **Обновить**.
- **Системный аудит**. Этот отчет содержит информацию о событиях, которые произошли во время работы программы и во время взаимодействия пользователя с программой.
- **Защита от угроз**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы следующих мониторинговых задач программы:
  - Защита от шифрования.
  - Контроль целостности системы.
  - Управление сетевым экраном.
  - Защита от веб-угроз.
  - Контроль программ.

  - Контроль устройств.
  - Проверка съемных дисков.
  - Защита от сетевых угроз.
  - Анализ поведения.
  - Защита от файловых угроз.
- **Задачи по требованию**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы следующих задач программы:
  - Задачи проверки.
  - Обновление.
  - Проверка целостности системы.

► *Чтобы просмотреть отчет:*

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

   Откроется окно **Отчеты**.
3. В левой части окна **Отчеты** выберите нужный тип отчета.

   В правой части окна отобразится отчет, содержащий список событий.

   По умолчанию события в отчете отсортированы по возрастанию значений графы **Дата**.
4. Если вы хотите посмотреть подробную информацию о событии отчета, представленную в отдельном блоке, выберите это событие в отчете.

   В нижней части окна отобразится блок, который содержит атрибуты этого события.

Для удобства работы вы можете изменять представление данных на экране следующими способами:

- фильтровать список событий по времени возникновения;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке.

Просмотр объектов в Хранилище

► *Чтобы просмотреть объекты в Хранилище:*

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

   Откроется окно **Хранилище**.

В окне отображается следующая информация об объектах в Хранилище:

- название объекта;
- полный путь к объекту;
- дата добавления объекта в Хранилище;

- дата удаления объекта из Хранилища (это поле отображается, если задан параметр `DaysToLive` (см. раздел "Параметры задачи Управление Хранилищем" на стр. 153));
- размер объекта.

Вы можете восстановить объекты из Хранилища в их исходные директории. Вы также можете удалить объекты из Хранилища. Удаленные объекты восстановить невозможно. Информация об этих действиях записывается в журнал событий.

Просмотр информации о лицензии

► *Чтобы просмотреть информацию о лицензии:*

1. Откройте главное окно программы.
2. Выполните одно из следующих действия:
   - В нижней части главного окна программы нажмите на область окна, в которой отображается информация о лицензии и о ключе.
   - В нижней части главного окна программы нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** нажмите по ссылке с уникальной буквенно-цифровой последовательностью, которая отображается в поле **Ключ**.

   Откроется окно **Лицензия**.

В окне отображается следующая информация о лицензии:

- **Активный ключ** – уникальная буквенно-цифровая последовательность.
- **Статус ключа** – статус ключа или сообщение о каких-либо проблемах, связанных с ключом (при их наличии).
- **Действует с** – дата активации программы путем добавления этого ключа.
- **Срок действия лицензии истекает** – количество дней до истечения срока действия лицензии и дата окончания срока действия лицензии в формате UTC.
- Сводная информация о лицензии или сообщение о каких-либо проблемах, связанных с лицензированием, и рекомендации о действиях, которые вам нужно выполнить для устранения проблем (при их наличии).

По ссылке **подробнее** отображается следующая информация:

- **Название программы** – название программы, для которой предназначена лицензия, связанная с ключом.
- **Защита** – информация о доступной функциональности программы и список доступных компонентов программы. Доступность функциональности и компонентов программы зависит от лицензии, связанной с ключом (https://support.kaspersky.ru/15471).

Создание файла трассировки

► *Чтобы создать файл трассировки:*

1. Откройте главное окно программы.

2. В нижней части главного окна программы нажмите на кнопку **Поддержка**.

   Откроется окно **Поддержка**.

3. По ссылке **Трассировка** откройте окно **Трассировка**.

4. В раскрывающемся списке **Уровень** выберите уровень детализации файла трассировки.

   Рекомендуется уточнить требуемый уровень детализации у специалиста из Службы технической поддержки "Лаборатории Касперского". По умолчанию установлено значение **Диагностический (300)**.

5. Нажмите на кнопку **Включить**, чтобы запустить процесс трассировки.

6. Воспроизведите ситуацию, при которой у вас возникает проблема.

7. Нажмите на кнопку **Выключить**, чтобы остановить процесс трассировки.

Созданные файлы трассировки хранятся в директории /var/log/kaspersky/kesl/. В файлах трассировки содержится информация об операционной системе, а также могут содержаться персональные данные (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 381).

kaspersky

Обновление антивирусных баз в ручном режиме

Для обновления баз, находящихся в изолированном сегменте сети, рекомендуется использовать следующий порядок действий:

1. В программе Kaspersky Security Center, находящейся в открытом сегменте сети, настройте задачу *Загрузка обновлений в хранилище Сервера администрирования*.
2. Убедитесь в том, что под управлением Kaspersky Security Center в открытом сегменте есть управляемые компьютеры с установленными программами, базы для которых необходимо обновить.
3. Запустите задачу *Загрузка обновлений в хранилище Сервера администрирования*. В процессе загрузки обновлений с открытых серверов «Лаборатории Касперского» Kaspersky Security Center выполнит проверку целостности обновлений, прежде чем добавит их в свое хранилище.
4. Удобным вам способом перенесите содержимое хранилища Kaspersky Security Center в изолированный сегмент сети.
5. Запустите на средствах антивирусной защиты внутри изолированного сегмента сети задачу обновления баз с указанием перенесенного хранилища как источника обновлений. При загрузке обновлений из хранилища программы еще раз выполнят проверку целостности загружаемых обновлений баз.

Если вам недоступны серверы обновлений "Лаборатории Касперского" (например, нет доступа к интернету), обратитесь в Службу технической поддержки "Лаборатории Касперского" для получения обновлений баз программы на дисках.

kaspersky

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программы, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте https://support.kaspersky.ru/general/certificates и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe).

Порядок получения критических обновлений изложен в формуляре.

Лицо, ответственное за эксплуатацию программы, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в программе, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

kaspersky

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 380).

kaspersky

Обращение в Поддержку пользователей

Этот раздел содержит информацию о способах и условиях получения поддержки.

В этом разделе

Способы получения технической поддержки

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

"Лаборатория Касперского" предоставляет поддержку Kaspersky Endpoint Security в течение жизненного цикла (см. страницу жизненного цикла программ (https://support.kaspersky.com/corporate/lifecycle)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

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

- посетить сайт Службы технической поддержки (https://support.kaspersky.ru/b2b);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

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).

Содержимое файлов трассировки и их хранение

Пользователи лично отвечают за безопасность данных, хранящихся на их компьютерах, в частности, за мониторинг и ограничение доступа к данным до момента их передачи в "Лабораторию Касперского".

Файлы трассировки хранятся на компьютере в течение всего времени использования программы и удаляются без возможности восстановления при удалении программы.

По умолчанию файлы трассировки хранятся в директории /var/log/kaspersky/kesl/. Можно просматривать данные, хранящиеся в файлах трассировки. Для доступа к заданной по умолчанию директории хранения файлов трассировки требуются root-права.

Во всех файлах трассировки хранятся общие данные:

- время возникновения события;
- номер потока исполнения;
- компонент программы, инициировавший событие;
- уровень важности события (информационное событие, предупреждение, критическое событие, ошибка);
- описание события, связанного с выполнением команды компонентом программы, и результат выполнения этой команды.

Программа Kaspersky Endpoint Security сохраняет пароли пользователей в файл трассировки только в зашифрованном виде.

В файлах трассировки могут храниться следующие данные в дополнение к общим данным:

- статусы компонентов программы и их рабочие данные;

- данные о действиях пользователей в программе;
- данные об оборудовании, установленном на компьютере;
- данные обо всех объектах и событиях операционной системы, включая данные о действиях пользователей;
- данные, содержащиеся в объектах операционной системы (например, содержимое файлов, в которых могут находиться персональные данные пользователей);
- данные о сетевом трафике (например, содержимое полей ввода на веб-сайте, которые могут включать данные банковской карты или любые другие конфиденциальные данные);
- данные, полученные с серверов "Лаборатории Касперского" (например, версия баз программы).

Содержимое файлов дампа и их хранение

Файлы дампа формируются автоматически при сбое в работе программы и хранятся на компьютере в течение всего времени использования программы. При необходимости вы можете выключить создание файлов дампа. Файлы дампа хранятся в директориях /var/opt/kaspersky/kesl/common/dumps и /var/opt/kaspersky/kesl/common/dumps-user и удаляются без возможности восстановления при удалении программы.

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security на момент создания файла дампа. Для доступа к файлам дампа требуются root-права.

Сохраненные файлы дампа могут содержать персональные данные. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

► *Чтобы выключить создание файла дампа:*

1. Остановите Kaspersky Endpoint Security (см. раздел "Запуск и остановка программы" на стр. 70).
2. Откройте файл /var/opt/kaspersky/kesl/common/kesl.ini на редактирование.
3. Добавьте следующий параметр в секцию `[General]`:

   ```
   CoreDumps=no
   ```

4. Запустите Kaspersky Endpoint Security (см. раздел "Запуск и остановка программы" на стр. 70).

Соответствие терминов

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

Таблица 173. Соответствие терминов

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

kaspersky

Приложения

Этот раздел содержит информацию, которая дополняет основной текст справки.

В этом разделе

Приложение 1. Оптимизация потребления ресурсов

При проверке объектов Kaspersky Endpoint Security использует ресурсы процессора, ввод-вывод дисковой подсистемы и оперативную память.

► *Чтобы посмотреть потребление ресурсов программой, выполните следующую команду:*

```
top -bn1|grep kesl
```

Выполнять команду требуется в момент нагрузки на систему.

Вывод команды показывает количество потребляемой памяти и занимаемого процессорного времени:

```
651 root   20    0 3014172 2.302g 154360 S 120.0 30.0   0:32.80 kesl
```

В графе 6 отображается количество резидентной памяти – 2.302g.

В графе 9 отображается процент использования ядер процессора – 120.0, где каждое ядро принимается за 100 процентов. Таким образом, 120% означает, что одно ядро занято полностью, а второе – на 20%.

Если работа Kaspersky Endpoint Security при проверке объектов критически замедляет работу системы, требуется провести настройку программы для оптимизации потребления ресурсов системы.

В этом разделе

Определение задачи, которая занимает ресурсы

Для того, чтобы определить, какая задача или задачи программы (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92) занимают ресурсы системы, требуется разделить потребление ресурсов задачей Защита от файловых угроз (см. раздел "Анализ работы задачи Защита от

файловых угроз" на стр. 385) (тип OAS) и задачами проверки по требованию (см. раздел "Анализ работы задач проверки по требованию" на стр. 386) (типы ODS и ContainerScan).

Если программа находится под управлением политики Kaspersky Security Center, требуется на время проведения исследования разрешить управление локальными задачами.

В этом разделе

Анализ работы задачи Защита от файловых угроз

► *Чтобы проанализировать работу задачи Защита от файловых угроз:*

1. Остановите (см. раздел "Запуск и остановка задачи" на стр. 98) все задачи проверки и мониторинга (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92).
2. Убедитесь, что задачи проверки по требованию не будут запущены во время проверки или не имеют расписания. Вы можете это сделать через Kaspersky Security Center или локально, выполнив следующие действия:
   a. Получите список всех задач программы, выполнив следующую команду:

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

   b. Получите параметры расписания задачи антивирусной проверки, выполнив следующую команду:

      ```
      kesl-control --get-schedule <идентификатор задачи>
      ```

      Если команда выводит `RuleType=Manual`, то задача запускается только вручную.

   c. Получите параметры расписания всех ваших задач антивирусной проверки, если такие были созданы, и укажите им запуск вручную, выполнив следующую команду:

      ```
      kesl-control --set-schedule <идентификатор задачи> RuleType=Manual
      ```

3. Включите создание файлов трассировки программы с высоким уровнем детализации, выполнив команду:

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

4. Запустите задачу Защита от файловых угроз, если она не была запущена, выполнив команду:

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

5. Создайте нагрузку на систему в том же режиме, который вызвал проблемы с производительностью, достаточно нескольких часов.

   Под нагрузкой программа записывает много информации в файлы трассировки, при этом по умолчанию хранится 5 файлов по 500 МБ, поэтому старая информация будет перезаписываться. Если проблемы с производительностью и потреблением ресурсов перестали проявляться, значит, скорее всего, проблемы вызывают задачи проверки по требованию и можно перейти к анализу работы задач проверки с типами ContainerScan и ODS (см. раздел "Анализ работы задач проверки по требованию" на стр. 386).

6. Выключите создание файлов трассировки программы, выполнив команду:

   ```
   kesl-control --set-app-settings TraceLevel=None
   ```

7. Определите список объектов, которые были проверены наибольшее количество раз, выполнив команду:

   ```
   fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -r|less
   ```

   Результат загрузится в программу просмотра текста less, где в самом начале будут отображаться те объекты, которые были проверены наибольшее количество раз.

8. Теперь вам нужно самостоятельно определить, являются ли наиболее часто проверенные объекты опасными. В случае затруднения обратитесь в Службу технической поддержки (см. раздел "Обращение в Поддержку пользователей" на стр. 380).

   Например, неопасными можно признать директории и файлы журналов, если запись в них ведет доверенный процесс, файлы баз данных.

9. Запишите пути к неопасным, по вашему мнению, объектам, они потребуются в дальнейшем для настройки исключений из проверки.

10. Если в системе осуществляется частая запись файлов различными сервисами, такие файлы будут повторно проверяться в отложенной очереди. Определите список путей, которые были проверены в отложенной очереди наибольшее количество раз, выполнив команду:

    ```
    fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $9}' | sort | uniq -c | sort -k1 -n -r
    ```

    Файлы, проверенные наибольшее количество раз, будут отображаться в начале списка.

11. Если счетчик по одному файлу превышает несколько тысяч за несколько часов, вам нужно определить, можно ли доверять этому файлу, чтобы исключить его из проверки.

    Логика определения такая же, как и для предыдущего исследования (см. п. 8): файлы журналов можно признать неопасными, так как они не могут быть запущены.

12. Даже если некоторые файлы исключены из проверки постоянной защитой, они все равно могут перехватываться программой. Если исключение определенных файлов из постоянной защиты не приносит существенного прироста производительности, вы можете полностью исключить из перехвата программой точку монтирования, где расположены эти файлы. Для этого выполните следующие действия:

    a. Получите список файлов, перехваченных программой, выполнив следующую команду:

       ```
       grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $7}' | sort | uniq -c | sort -k1 -n -r
       ```

    b. С помощью полученного списка определите пути, по которым происходит большое количество перехватов файловых операций, и настройте исключения из перехвата (см. раздел "Настройка задачи Защита от файловых угроз" на стр. 387).

Анализ работы задач проверки по требованию

Также большое потребление ресурсов может быть вызвано использованием задач с типами ODS и ContainerScan (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92). Следуйте следующим рекомендациям по использованию задач с типом ODS:

- Убедитесь, что не выполняется запуск нескольких задач проверки по требованию одновременно. Программа позволяет работать в таком режиме, но потребление ресурсов может сильно увеличиться. Проверьте расписание всех задач с типами ODS и ContainerScan локально (как

описано для задачи Защита от файловых угроз (см. раздел "Анализ работы задачи Защита от файловых угроз" на стр. 385)) или через Kaspersky Security Center.

- Запускайте проверку во время наименьшей нагрузки на сервер.
- Убедитесь, что по указанному пути проверки нет примонтированных удаленных ресурсов (SMB / NFS). Если задача состоит в проверке удаленного ресурса и нет возможности выполнять ее непосредственно на сервере, предоставляющем ресурс, не выполняйте проверку на серверах с критическими сервисами, так как такая задача может выполняться достаточно долго (в зависимости от скорости соединения и количества файлов).
- Выполните оптимизацию параметров задачи проверки по требованию перед запуском.

Настройка задачи Защита от файловых угроз

Если после выполнения анализа работы задачи Защита от файловых угроз (см. раздел "Анализ работы задачи Защита от файловых угроз" на стр. 385) вы сформировали список директорий и файлов, которые можно исключить из проверки задачи, вам нужно добавить их в исключения.

Исключения из антивирусной проверки

► *Чтобы исключить директорию /tmp/logs и все поддиректории и файлы рекурсивно, выполните следующую команду:*

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

► *Чтобы исключить конкретный файл или файлы по маске в директории /tmp/logs, выполните следующую команду:*

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

► *Чтобы исключить по рекурсивной маске все файлы с расширением .log в директории /tmp/ и поддиректориях, выполните следующую команду:*

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Исключения из перехвата

Если вы хотите исключить файлы определенной директории не только из проверки, но и из перехвата, вы можете исключить точку монтирования целиком.

► *Чтобы исключить точку монтирования целиком:*

1. Если директория не является точкой монтирования, нужно создать из нее точку монтирования. Например, чтобы создать точку монтирования из директории /tmp, выполнив следующую команду:

   ```
   mount --bind /tmp/ /tmp
   ```

2. Чтобы точка монтирования сохранилась после перезагрузки сервера, добавьте в файл /etc/fstab следующую строку:

   ```
   /tmp /tmp none defaults,bind 0 0
   ```

3. Добавьте директорию /tmp в глобальные исключения, выполнив следующую команду:

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

4. Если требуется добавить несколько директорий, увеличивайте счетчик item_0000 на единицу (item_0001, item_0002 и так далее).

Исключать точки монтирования также рекомендуется, если это примонтированный удаленный ресурс с нестабильным или медленным соединением.

Изменение типа проверки

По умолчанию задача Защита от файловых угроз может проверять файлы при открытии и закрытии. Если в ходе анализа работы задачи Защита от файловых угроз (см. раздел "Анализ работы задачи Защита от файловых угроз" на стр. 385) было выявлено слишком много записываемых файлов, вы можете перевести файловый перехватчик в режим работы только при открытии файлов, выполнив следующую команду:

```
kesl-control --set-set 1 ScanByAccessType=Open
```

При таком режиме работы изменения, внесенные в файл после открытия, не будут проверяться до следующего обращения к файлу.

Настройка задачи проверки по требованию

Для задач проверки по требованию с типами ODS и ContainerScan (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92) применима настройка исключений из антивирусной проверки, описанная для задачи Защита от файловых угроз (см. раздел "Настройка задачи Защита от файловых угроз" на стр. 387), но неприменима настройка исключения точек монтирования.

Настройка приоритета

Для задач проверки по требованию предусмотрен параметр `ScanPriority`, с помощью которого можно указать, как программа распределяет ресурсы системы для запущенных задач.

Доступные значения:

- `Idle` – не более 10% загрузки одного процессора (вне зависимости от того, занят он или нет).
- `Normal` – 50% загрузки всех доступных процессоров.
- `High` – без ограничений.

Ограничение по загрузке процессоров также снижает потребление ресурсов ввода-вывода дисковой подсистемы.

► *Чтобы установить для задачи приоритет выполнения Idle, выполните следующую команду:*

```
kesl-control --set-settings <идентификатор задачи> ScanPriority=Idle
```

Ограничение использования памяти для распаковки архивов

Задача проверки по требованию при рекурсивной проверке во время проверки архивов будет распаковывать их, используя оперативную память. По умолчанию программа имеет ограничение в 40% от всей доступной оперативной памяти, но не менее 2 ГБ. Поэтому если система имеет более 5 ГБ оперативной памяти, можно установить ограничение на использование памяти вручную. Это особенно актуально для серверов, имеющих сотни гигабайт оперативной памяти.

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

1. Остановите Kaspersky Endpoint Security (см. раздел "Запуск и остановка программы" на стр. 70).
2. Откройте файл /var/opt/kaspersky/kesl/common/kesl.ini на редактирование.
3. Добавьте параметр `ScanMemoryLimit` с нужным значением (например, 8192) в секцию `[General]`:

   ```
   ScanMemoryLimit=8192
   ```

4. Запустите Kaspersky Endpoint Security (см. раздел "Запуск и остановка программы" на стр. 70).

Параметр `ScanMemoryLimit` ограничивает не общее количество памяти, которое использует программа, а количество памяти, которое используется при проверке файлов, то есть общее количество памяти может быть больше значения, заданного этим параметром.

Приложение 2. Конфигурационные файлы программы

В программе предусмотрены конфигурационные файлы, содержащие параметры программы, заданные при установке программы, а также конфигурационные файлы, содержащие параметры по умолчанию для задач программы.

Вы можете редактировать значения параметров конфигурационных файлов программы из командной строки.

В этом разделе

kaspersky

Конфигурационные файлы параметров программы

После первоначальной настройки в программе создаются следующие конфигурационные файлы:

- /var/opt/kaspersky/kesl/common/agreements.ini

  Конфигурационный файл agreements.ini содержит параметры, связанные с Лицензионным соглашением, Политикой конфиденциальности и Положением о Kaspersky Security Network.

- /var/opt/kaspersky/kesl/common/kesl.ini

  Конфигурационный файл kesl.ini содержит параметры, приведенные в таблице ниже.

При необходимости вы можете изменять значения параметров (см. раздел "Правила редактирования конфигурационных файлов задач программы" на стр. 395) в этих файлах.

Изменять значения по умолчанию в этих файлах рекомендуется под руководством специалистов Службы технической поддержки по полученным от них инструкциям.

Таблица 174. Параметры конфигурационного файла kesl.ini

Параметр	Описание	Значения
Секция **[General]** содержит следующие параметры:		
`PCID`	Уникальный идентификатор установки программы.	Заполняется автоматически во время первоначальной настройки программы.
`ExecEnvMax`	Количество переменных окружения, которые программа будет захватывать из вызова команды.	Значение по умолчанию: 50.
`UseGui`	Наличие установленного пакета графического пользовательского интерфейса (см. раздел "Установка Kaspersky Endpoint Security с помощью командной строки" на стр. 25).	`True/Yes` – пакет графического пользовательского интерфейса установлен. `False/No` – пакет графического пользовательского интерфейса не установлен. Заполняется автоматически во время первоначальной настройки программы.
`Locale`	Языковой стандарт, используемый для локализации событий программы, отправляемых в Kaspersky Security Center. Локализация графического интерфейса и командной строки программы зависит от локализации, указанной в переменной окружения LANG. Если в переменной окружения LANG указана локализация, которую не поддерживает программа, то графический интерфейс и командная строка отображаются в английской локализации.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр `Locale` не указан, устанавливается язык локализации операционной системы. Если программе не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию `en_US.utf8`.

Параметр	Описание	Значения
ScanMemoryLimit	Ограничение на использование памяти программой (см. раздел "Установка ограничения на использование памяти программой" на стр. 81) в мегабайтах.	Значение по умолчанию: 8192.
ExecArgMax	Количество аргументов, которые программа будет захватывать из вызова exec.	Значение по умолчанию: 50.
MachineId	Уникальный идентификатор устройства пользователя.	Заполняется автоматически во время первоначальной настройки программы.
StartupTraces	Включение создания файлов трассировки (см. раздел "Содержимое файлов трассировки и их хранение" на стр. 381) при запуске программы.	True/Yes – создавать файлы трассировки при запуске программы. False/No (значение по умолчанию) – не создавать файлы трассировки при запуске программы.
CoreDumps	Включение создания файла дампа (см. раздел "Содержимое файлов дампа и их хранение" на стр. 382) при сбое в работе программы.	True/Yes (значение по умолчанию) – создавать файл дампа при сбое в работе программы. False/No – не создавать файл дампа при сбое в работе программы.
UseFanotify	Использование технологии fanotify.	True/Yes – операционная система поддерживает технологию fanotify. False/No – операционная система не поддерживает технологию fanotify. Заполняется автоматически во время первоначальной настройки программы.
SocketPath	Путь к сокету для удаленного подключения, по которому подключаются, например, графический интерфейс и утилита kesl-control.	Значение по умолчанию: /var/run/bl4control.
PackageType	Формат установленного пакета программы (см. раздел "Установка Kaspersky Endpoint Security с помощью командной строки" на стр. 25).	RPM – установлен пакет формата RPM. DEB – установлен пакет формата DEB. Заполняется автоматически во время первоначальной настройки программы.

Параметр	Описание	Значения
`AdditionalDNSLookup`	Использование публичного DNS.	`True/Yes` – использовать публичный DNS для доступа к серверам "Лаборатории Касперского". `False/No` – не использовать публичный DNS для доступа к серверам "Лаборатории Касперского". При сбоях доступа к серверам через системный DNS программа будет использовать публичный DNS. Это нужно для обновления баз программы и поддержки уровня безопасности компьютера. Программа будет использовать следующие публичные DNS в порядке их обхода: • Google Public DNS™ (8.8.8.8). • Cloudflare® DNS (1.1.1.1). • Alibaba Cloud® DNS (223.6.6.6). • Quad9® DNS (9.9.9.9). • CleanBrowsing (185.228.168.168). Запросы программы могут содержать адреса доменов и внешний IP-адрес пользователя, так как программа устанавливает с DNS-сервером TCP/UDP-соединение. Эти данные нужны, например, для проверки сертификата веб-ресурса при обращении по HTTPS. Если программа использует публичный DNS-сервер, правила обработки данных регламентируются Политикой конфиденциальности этого сервиса. Если требуется запретить программе использовать публичный DNS-сервер, обратитесь в Службу технической поддержки за приватным патчем.
Секция **[Network]** содержит следующие параметры:		
`WtpFwMark`	Метка в правилах утилиты iptables для перенаправления трафика в программу для обработки задачей Защита от веб-угроз. Вам может потребоваться изменить эту метку, если на одном компьютере с установленной программой работает другое ПО, которое использует девятый бит маски TCP-пакета, и возникает конфликт.	Значение задается десятеричным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 256.

Параметр	Описание	Значения
NtpFwMark	Метка в правилах утилиты iptables для перенаправления трафика в программу для обработки задачей Защита от сетевых угроз. Вам может потребоваться изменить эту метку, если на одном компьютере с установленной программой работает другое ПО, которое использует девятый бит маски TCP-пакета, и возникает конфликт.	Значение задается десятеричным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 512.
BypassFwMark	Метка, которой маркируются пакеты, созданные или проверенные программой, чтобы они снова не попали в программу на проверку.	Значение задается десятеричным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 1024.
ProxyRouteTable	Номер таблицы маршрутизации.	Значение по умолчанию: 101.
Секция **[Watchdog]** содержит следующие параметры:		
TimeoutAfterHeadshot	Максимальное время ожидания завершения управляемого процесса от момента отправки сигнала HEADSHOT Watchdog-сервером управляемому процессу.	Значение по умолчанию: 120000 мсек.
StartupTimeout	Максимальный интервал времени от момента получения сообщения REGISTER до момента получения сообщения SUCCESSFUL_STARTUP.	Значение по умолчанию: 180000 мсек.
TimeoutAfterKill	Максимальное время ожидания завершения управляемого процесса от момента отправки Watchdog-сервером сигнала SIGKILL управляемому процессу. Если по истечении этого времени управляемый процесс не завершился, выполняется действие, заданное параметром --failed-kill.	Значение по умолчанию: 172800000 мсек.
PingInterval	Периодичность, с которой программа пытается отправить серверу сообщение PONG в ответ на принятое сообщение PING.	Значение по умолчанию: 2000 мсек.
MaxRestartCount	Максимальное количество неудачных последовательных попыток запуска программы.	Значение по умолчанию: 5.

Параметр	Описание	Значения
`ActivityTimeout`	Максимальный интервал времени, в течение которого программа должна отправить сообщение Watchdog-серверу. Если в течение этого интервала времени от программы не будет сообщения, Watchdog-сервер начнет процедуру завершения управляемого процесса.	Значение по умолчанию: 120000 мсек.
`ConnectTimeout`	Максимальный интервал времени от момента запуска управляемого процесса до момента установления программой соединения с Watchdog-сервером. Если программа не успеет создать соединение за этот интервал времени, Watchdog-сервер начнет процедуру завершения управляемого процесса.	Значение по умолчанию: 180 мсек.
`RegisterTimeout`	Максимальный интервал времени от момента соединения программы с Watchdog-сервером до получения сервером сообщения REGISTER.	Значение по умолчанию: 500 мсек.
`TimeoutAfterShutdown`	Максимальное время ожидания завершения управляемого процесса от момента отправки Watchdog-сервером сигнала SHUTDOWN управляемому процессу.	Значение по умолчанию: 120000 мсек.
`MaxVirtualMemory`	Ограничение на использование виртуальной памяти управляемого процесса. Если виртуальная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения управляемого процесса.	`Off` (значение по умолчанию) – использование виртуальной памяти не ограничено. `<значение>%` – значение от 0 до 100 в процентах от объема памяти. `<значение>MB` – значение в мегабайтах. `lowest/<значение>%/<значение>MB/` – наименьшее значение между значением в процентах и значением в мегабайтах. `highest/<значение>%/<значение>MB/` – наибольшее значение между значением в процентах и значением в мегабайтах.

Параметр	Описание	Значения
MaxSwapMemory	Ограничение на размер swap-файла управляемого процесса. Если swap-файл управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения управляемого процесса.	Off (значение по умолчанию) – размер swap-файла не ограничен. <значение>% – значение от 0 до 100 в процентах от объема памяти. <значение>MB – значение в мегабайтах. lowest/<значение>%/<значение>MB/ – наименьшее значение между значением в процентах и значением в мегабайтах. highest/<значение>%/<значение>MB/ – наибольшее значение между значением в процентах и значением в мегабайтах.
MaxMemory	Ограничение на использование резидентной памяти управляемого процесса. Если резидентная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения управляемого процесса.	Off – использование резидентной памяти не ограничено. <значение>% – значение от 0 до 100 в процентах от объема памяти. <значение>MB – значение в мегабайтах. lowest/<значение>%/<значение>MB/ – наименьшее значение между значением в процентах и значением в мегабайтах. highest/<значение>%/<значение>MB/ – наибольшее значение между значением в процентах и значением в мегабайтах. Значение по умолчанию: highest/2048MB/50%.

Правила редактирования конфигурационных файлов задач программы

При редактировании конфигурационного файла соблюдайте следующие правила:

- В конфигурационном файле укажите все обязательные параметры. Отдельные параметры задачи можно указать без файла, с помощью командной строки (см. раздел "Управление задачами программы с помощью командной строки" на стр. 92).
- Если параметр принадлежит к какой-либо секции, укажите его только в этой секции. В пределах одной секции вы можете указывать параметры в любом порядке.
- Заключайте имена секций в квадратные скобки [ ].
- Вводите значения параметров в формате <имя параметра>=<значение параметра> (пробелы между именем параметра и его значением не обрабатываются).

Пример:

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

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

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

  Пример:

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

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

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

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

  Пример:

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

Одиночная кавычка в начале или в конце строки считается ошибкой.

Конфигурационный файл задачи Защита от файловых угроз

```
ScanArchived=No
ScanSfxArchived=No
ScanMailBases=No
ScanPlainMail=No
SkipPlainTextFiles=No
TimeLimit=60
```

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

Конфигурационный файл задачи Антивирусная проверка

```
ScanFiles=Yes
ScanBootSectors=Yes
ScanComputerMemory=Yes
ScanStartupObjects=Yes
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
```

```
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
ScanPriority=Normal
DeviceNameMasks.item_0000=/**
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Выборочная проверка

```
ScanFiles=Yes
ScanBootSectors=No
ScanComputerMemory=No
ScanStartupObjects=No
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
```

```
ScanPriority=High
DeviceNameMasks.item_0000=/**
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Проверка важных областей

```
ScanFiles=No
ScanBootSectors=Yes
ScanComputerMemory=Yes
ScanStartupObjects=Yes
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
ScanPriority=Normal
DeviceNameMasks.item_0000=/**
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
```

```
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Обновление

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

Конфигурационный файл задачи Управление Хранилищем

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

Конфигурационный файл задачи Контроль целостности системы

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

Конфигурационный файл задачи Защита от шифрования

```
UseHostBlocker=Yes
BlockTime=30
UseExcludeMasks=No
[ScanScope.item_0000]
AreaDesc=All shared directories
UseScanArea=Yes
Path=AllShared
AreaMask.item_0000=*
```

Конфигурационный файл задачи Защита от веб-угроз

```
UseTrustedAddresses=Yes
ActionOnDetect=Block
CheckMalicious=Yes
CheckPhishing=Yes
UseHeuristicForPhishing=Yes
CheckAdware=No
CheckOther=No
```

Конфигурационный файл задачи Проверка съемных дисков

```
ScanRemovableDrives=NoScan
ScanOpticalDrives=NoScan
BlockDuringScan=No
```

Конфигурационный файл задачи Проверка контейнеров

```
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
ScanContainers=Yes
ContainerNameMask=*
```

```
ScanImages=Yes
ImageNameMask=*
DeepScan=No
ScanPriority=Normal
ContainerScanAction=StopContainerIfFailed
ImageAction=Skip
```

Вы можете использовать параметры этого конфигурационного файла также для задачи Выборочная проверка контейнеров (см. раздел "Задача Выборочная проверка контейнеров (Custom_Container_Scan, ID:19)" на стр. 184), за исключением параметра `ScanPriority=Normal`. Для задачи Выборочная проверка значение параметра `ScanPriority=High`.

Конфигурационный файл задачи Анализ поведения

```
UseTrustedPrograms=No
TaskMode=Block
```

Конфигурационный файл задачи Контроль программ

```
AppControlMode=DenyList
AppControlRulesAction=ApplyRules
```

Конфигурационный файл задачи Инвентаризация

```
ScanScripts=Yes
ScanBinaries=Yes
ScanAllExecutable=Yes
ScanPriority=Normal
CreateGoldenImage=No
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/usr/bin
AreaMask.item_0000=*
```

kaspersky

Приложение 3. Коды возврата командной строки

В программе Kaspersky Endpoint Security предусмотрены следующие коды возврата командной строки.

0 – команда / задача выполнена успешно;

1 – общая ошибка в аргументах команды;

2 – ошибка в переданных параметрах программы;

64 – программа Kaspersky Endpoint Security не запущена;

66 – базы программы не загружены (используется только командой `kesl-control --app-info`);

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

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

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

71 – не приняты условия Положения о Kaspersky Security Network;

72 – при выполнении задачи Выборочная проверка (см. раздел "Задача Выборочная проверка (Scan_File, ID:3)" на стр. 129) или Выборочная проверка контейнеров (см. раздел "Задача Выборочная проверка контейнеров (Custom_Container_Scan, ID:19)" на стр. 184) обнаружены угрозы;

73 – попытка задать параметры задачи Контроль программ (см. раздел "Задача Контроль программ (Application_Control, ID:21)" на стр. 192), влияющие на работу программы, без их подтверждения с помощью флага `--accept`.

74 – требуется перезапуск программы Kaspersky Endpoint Security после обновления;

75 – требуется перезагрузка компьютера;

128 – неизвестная ошибка;

65 – все остальные ошибки.

Приложение 4. Значения параметров программы в сертифицированной конфигурации

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Если вы меняете значения (диапазоны значений) перечисленных параметров с их значений в сертифицированной конфигурации на другие значения, программа выходит из безопасного состояния.

Таблица 175. Параметры и их безопасные значения для программы в сертифицированной конфигурации

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
`FirstAction`	задача Защита от файловых угроз, задача Антивирусная проверка, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Одно из следующих значений: • `Disinfect` (лечить) – программа пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), программа оставляет объект неизменным. Если первым действием выбрано `Disinfect`, рекомендуется задать второе действие в параметре `SecondAction`. • `Remove` (удалять) – программа удаляет зараженный объект, предварительно создав его резервную копию. • `Recommended` (выполнять рекомендуемое действие) – программа автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе.

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
SecondAction	задача Защита от файловых угроз, задача Антивирусная проверка, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Одно из следующих значений: • Disinfect (лечить) – программа пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), программа оставляет объект неизменным. Если первым действием выбрано Disinfect, рекомендуется задать второе действие в параметре SecondAction. • Remove (удалять) – программа удаляет зараженный объект, предварительно создав его резервную копию. • Recommended (выполнять рекомендуемое действие) – программа автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Если в качестве первого действия FirstAction выбрано Remove, то второе действие SecondAction указывать не нужно.
UseAnalyzer	задача Защита от файловых угроз, задача Антивирусная проверка, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Yes – включить эвристический анализатор.
HeuristicLevel	задача Защита от файловых угроз, задача Антивирусная проверка, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Одно из следующих значений: • Light – наименее тщательная проверка, минимальная загрузка системы. • Medium – средний уровень эвристического анализа, сбалансированная загрузка системы. • Deep – наиболее тщательная проверка, максимальная загрузка системы. • Recommended – рекомендуемое значение.

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
ScanArchived	задача Защита от файловых угроз, задача Антивирусная проверка, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Yes – проверять архивы.
ScanSfxArchived	задача Защита от файловых угроз, задача Антивирусная проверка, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Yes – проверять самораспаковывающиеся архивы.
ScanMailBases	задача Защита от файловых угроз, задача Антивирусная проверка, задача Выборочная проверка, задача Проверка важных областей, задача Проверка контейнеров, задача Выборочная проверка контейнеров	Yes – проверять файлы почтовых баз.
ScanByAccessType	задача Защита от файловых угроз	Open – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.
SourceType	задача Обновление	Одно из следующих значений: • KLServers – программа получает обновления с одного из серверов обновлений "Лаборатории Касперского". Обновления загружаются по протоколу HTTPS. • SCServer – программа загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. • Custom – программа загружает обновления из пользовательского источника, указанного в секции [CustomSources.item_#]. Вы можете указывать директории FTP-, HTTP- и HTTPS-серверов или директории на любом смонтированном устройстве защищаемого компьютера, включая директории на удаленных компьютерах, смонтированные по протоколам Samba или NFS.

Название параметра	Сущность, к которой относится параметр	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
ApplicationUpdateMode	задача Обновление	Disabled – не загружать и не устанавливать обновления программы.
UseHostBlocker	задача Защита от шифрования	Yes – включить блокировку недоверенных компьютеров.
ActionOnDetect	задача Защита от веб-угроз	Block – запретить доступ к обнаруженному объекту, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.
ScanRemovableDrives	задача Проверка съемных дисков	Одно из следующих значений: • DetailedScan – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). • QuickScan – проверять только файлы определенных типов на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков).
UseKSN	общие параметры программы	No – выключить участие в Kaspersky Security Network.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Amazon – товарный знак или зарегистрированный в США и/или других странах товарный знак, принадлежащий Amazon.com, Inc. и/или дочерним/аффилированным компаниям.

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Google Public DNS – товарный знак Google LLC.

Core – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

EulerOS является зарегистрированным товарным знаком Huawei Technologies Co., Ltd в Китае и других странах.

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

Microsoft, Active Directory, Outlook, Visual C++ и Windows являются товарными знаками группы компаний Microsoft.

Oracle и JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Red Hat и Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

CentOS – товарный знак или зарегистрированный в США и других странах товарный знак Red Hat, Inc. или дочерних компаний.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.