kaspersky

Kaspersky Endpoint Security 11.1.0 для Linux

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 11.1.0

Содержание

Уведомления о товарных знаках

Kaspersky Endpoint Security 11 для Linux

Kaspersky Endpoint Security 11 для Linux (далее также Kaspersky Endpoint Security) осуществляет защиту компьютеров под управлением операционной системы Linux от вредоносных программ. Угрозы могут проникать в систему через сетевые каналы передачи данных или со съемных дисков.

Программа позволяет:

- Проверять объекты файловой системы, расположенные на локальных дисках компьютера, а также смонтированные и разделяемые ресурсы, доступ к которым предоставляется по протоколам SMB и NFS.
- Проверять объекты файловой системы как в режиме реального времени с помощью задач Защиты от файловых угроз, так и по требованию с помощью задач антивирусной проверки.
- Проверка загрузочных секторов.
- Проверять память процессов.
- Обнаруживать зараженные объекты. Kaspersky Endpoint Security оценивает объект как зараженный, если в объекте обнаружен код известного вируса.
- Обезвреживать обнаруженные в файлах угрозы.
- Автоматически выбирать действие для нейтрализации угрозы.
- Сохранять резервные копии файлов перед лечением или удалением и восстанавливать файлы из резервных копий.
- Управлять задачами и настраивать их параметры.
- Добавлять ключи и активировать программу с помощью кодов активации.
- Уведомлять администратора о событиях, произошедших во время работы Kaspersky Endpoint Security.
- Обновлять базы Kaspersky Endpoint Security с серверов обновлений "Лаборатории Касперского", через Сервер администрирования или из указанного пользователем источника по расписанию и по требованию.
- Использовать антивирусные базы для поиска и лечения зараженных файлов. Во время процесса проверки Kaspersky Endpoint Security анализирует каждый файл на наличие

угрозы: программа сравнивает код файла с кодом конкретной угрозы и ищет возможные совпадения.

- Отслеживать целостность системы или указанных файлов и сообщать об изменениях. Контроль целостности системы может выполняться в режиме постоянного мониторинга и в режиме проверки по требованию.

- Управлять сетевым экраном операционной системы и при необходимости восстанавливать набор правил сетевого экрана, который был изменен.

- Защищать ваши файлы в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования.

- Анализировать трафик, передаваемый по протоколам HTTP/HTTPS и FTP от пользовательских компьютеров, и проверять, являются ли веб-адреса вредоносными или фишинговыми.

- Настраивать гибкие ограничения доступа к запоминающим устройствам (жестким дискам, съемным дискам, CD/DVD-приводам), оборудованию для передачи данных (модемам), устройствам преобразования данных (принтерам) и интерфейсам подключения устройств к компьютерам (USB, FireWire).

- Проверять съемные диски при подключении к компьютеру.

- Проверять входящий сетевой трафик на активность, характерную для сетевых атак.

- Проверять Docker-контейнеры и образы, а также пространства имен.

- Получать информацию о действиях программ на компьютере.

- Настраивать параметры проверки зашифрованных соединений.

- Участвовать в Kaspersky Security Network.

- Разрешать пользователям без root-прав управлять базовыми функциями программы с помощью графического пользовательского интерфейса.

- Обновлять программу с помощью пакетов обновлений.

- Проверять целостность компонентов программы с помощью инструмента проверки целостности.

Управлять программой Kaspersky Endpoint Security можно следующими способами:

- С помощью команд управления программой из командной строки.

- Через Kaspersky Security Center.

- С помощью графического пользовательского интерфейса.

- Через Kaspersky Security Center Web Console. Удаленное управление Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console поддерживается только в Kaspersky Security Center 12.

- Через Kaspersky Security Center Cloud Console. Удаленное управление Kaspersky Endpoint Security с помощью Kaspersky Security Center Cloud Console поддерживается только в Kaspersky Security Center 12.

Комплект поставки

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

- kesl-11.0.0-<номер сборки>.i386.rpm, kesl_11.0.0-<номер сборки>_i386.deb

  Содержат основные файлы Kaspersky Endpoint Security. Пакеты могут быть установлены на 32-битные операционные системы в соответствии с типом пакетного менеджера.

- kesl-11.0.0-<номер сборки>.x86_64.rpm, kesl_11.0.0-<номер сборки>_amd64.deb

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

- kesl.zip

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

- klnagent-<номер сборки>.i386.rpm, klnagent_<номер сборки>_i386.deb, klnagent64-<номер сборки>.x86_64.rpm, klnagent64_<номер сборки>_amd64.deb

  Содержит Агент администрирования (компонент Kaspersky Security Center, обеспечивающий взаимодействие между Сервером администрирования Kaspersky Security Center и Kaspersky Endpoint Security).

- klnagent-rpm.tar.gz, klnagent-deb.tar.gz

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

- ksn_license.<ID языка>

  Содержит текст Положения о Kaspersky Security Network.

- license.<ID языка>

  Содержит текст Лицензионного соглашения. В Лицензионном соглашении указано, на каких условиях вы можете пользоваться программой.

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Минимальные общие требования:

- процессор Core 2 Duo 1.86 GHz или выше;
- 1 ГБ оперативной памяти для 32-разрядной операционной системы, 2 ГБ оперативной памяти для 64-разрядной операционной системы;
- раздел подкачки не менее 1 GB;
- 1 GB свободного места на жестком диске.

Программные требования:

- Поддерживаемые 32-битные операционные системы:
  - Ubuntu 16.04 LTS и выше.
  - Red Hat Enterprise Linux 6.7 и выше.
  - CentOS 6.7 и выше.
  - Debian GNU / Linux 9.4 и выше.
  - Debian GNU / Linux 10.
  - Linux Mint 18.2 и выше.
  - Linux Mint 19 и выше.
  - Альт 8 СП Рабочая Станция.
  - Альт 8 СП Сервер.
  - Альт Рабочая Станция 8.
  - Альт Рабочая Станция K 8.
  - Альт Сервер 8.
  - Альт Образование 8.

    - Альт Рабочая Станция 9.
    - Альт Образование 9.
    - Гослинукс 6.6.
    - Mageia 4.
- Поддерживаемые 64-битные операционные системы:
    - Ubuntu 16.04 LTS и выше.
    - Ubuntu 18.04 LTS и выше.
    - Red Hat Enterprise Linux 6.7 и выше.
    - Red Hat Enterprise Linux 7.2 и выше.
    - Red Hat Enterprise Linux 8.0 и выше.
    - CentOS 6.7 и выше.
    - CentOS 7.2 и выше.
    - CentOS 8.0 и выше.
    - Debian GNU / Linux 9.4 и выше.
    - Debian GNU / Linux 10.1 и выше.
    - OracleLinux 7.3 и выше.
    - OracleLinux 8 и выше.
    - SUSE Linux Enterprise Server 15 и выше.
    - openSUSE Leap 15 и выше.
    - Альт 8 СП Рабочая Станция.
    - Альт 8 СП Сервер.
    - Альт Рабочая Станция 8.
    - Альт Рабочая Станция K 8.
    - Альт Сервер 8.

    - Альт Образование 8.
    - Альт Рабочая Станция 9.
    - Альт Сервер 9.
    - Альт Образование 9.
    - Amazon Linux AMI.
    - Linux Mint 18.2 и выше.
    - Linux Mint 19 и выше.
    - Astra Linux Special Edition, версия 1.5 (стандартное ядро и ядро PaX).
    - Astra Linux Special Edition, версия 1.5 (стандартное ядро и ядро PaX).
    - Astra Linux Common Edition, версия 2.12.
    - Гослинукс 6.6.
    - Гослинукс 7.2.
    - AlterOS 7.5 и выше.
    - Pardus OS 19.1.
- Интерпретатор языка Perl версии 5.10 или выше.
- Установленная утилита which.
- Установленные пакеты для компиляции программ и запуска задач (gcc, binutils, glibc, glibc-devel, make, ld, rpcbind).
- Исходный код ядра операционной системы – для компиляции модулей Kaspersky Endpoint Security на операционных системах, не поддерживающих технологию fanotify.

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

Kaspersky Endpoint Security 11 для Linux совместим с Kaspersky Security Center 11 и Kaspersky Security Center 12. Удаленное управление Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console поддерживается только в Kaspersky Security Center 12. Дополнительная информация будет добавлена в справку после выхода Kaspersky Security Center 12.

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

Для операционных систем Red Hat Enterprise Linux 8 и CentOS 8 необходимо установить пакет perl-Getopt-Long.

Сравнение функций программы в зависимости от инструментов управления

Набор доступных функций Kaspersky Endpoint Security зависит от инструментов управления (см. таблицу ниже).

Вы можете управлять программой с помощью следующих консолей Kaspersky Security Center:

- Консоль администрирования. Оснастка к Microsoft Management Console (MMC), которая устанавливается на рабочее место администратора.
- Web Console. Компонент Kaspersky Security Center, который устанавливается на Сервер администрирования. Вы можете работать в Web Console через браузер на любом компьютере, который имеет доступ к Серверу администрирования.

Вы также можете управлять программой с помощью Kaspersky Security Center Cloud Console. 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".

Сравнение функций Kaspersky Endpoint Security

Функция	Kaspersky Security Center Консоль администрирования	Kaspersky Security Center Web Console	Kaspersky Security Center Cloud Console
Продвинутая защита			
Kaspersky Security Network	✓	✓	✓
Защита от шифрования	✓	✓	✓
Контроль целостности системы	✓	✓	–
Контроль устройств	✓	✓	✓
Анализ поведения	✓	✓	✓
Базовая защита			
Защита от файловых угроз	✓	✓	✓

Управление сетевым экраном	✓	✓	✓
Защита от веб-угроз	✓	✓	✓
Защита от сетевых угроз	✓	✓	✓
Задачи			
Антивирусная проверка	✓	✓	✓
Проверка загрузочных секторов	✓	✓	✓
Проверка памяти процессов	✓	✓	✓
Обновление	✓	✓	✓
Откат обновлений	✓	✓	✓
Добавление ключа	✓	✓	✓
Контроль целостности системы по требованию	✓	✓	—
Проверка съемных дисков	✓	✓	✓
Задача Проверка контейнеров	✓	✓	—

Что нового

Kaspersky Endpoint Security 11 для Linux предлагает следующие возможности и улучшения:

- Защита от веб-угроз

  Реализована возможность проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым.

- Контроль устройств

  Реализована возможность управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения.

- Проверка съемных дисков

  Реализована возможность проверки съемных дисков.

- Защита от сетевых угроз

Реализована возможность отслеживания во входящем сетевом трафике активности, характерной для сетевых атак.

- Проверка контейнеров

  Реализована возможность проверки по требованию Docker-контейнеров и образов.

- Анализ поведения

  Реализована возможность получения данных о действиях программ на компьютере пользователя.

- Роли пользователей

  Изменена ролевая модель управления программой.

- Проверка пространств имен и Docker-контейнеров.

  Реализована возможность проверки пространств имен (name space) и Docker-контейнеров в режиме мониторинга (общие параметры программы), а также возможность указать действие с Docker-контейнером при обнаружении вредоносного объекта (настройки задачи File_Threat_Protection).

- Изменены названия задач:

  - File_Monitoring переименована в File_Threat_Protection;
  - Integrity_Monitoring переименована в System_Integrity_Monitoring;
  - Firewall_Manager переименована в Firewall_Management.

- Удалена задача ретрансляции (Retranslate).

  Удалена задача ретрансляции антивирусных баз (Retranslate). Воспользоваться функцией ретрансляции баз можно с помощью утилиты Kaspersky Update Utility.

- Проверка памяти ядра

  Реализована возможность проверки памяти ядра в задаче Memory_Scan.

- Управление задачами Обновления

  Удален функционал паузы (suspend-task/resume-task) для задач Update.

- Приоритет задачи

  Реализована возможность указать приоритет выполнения задач проверки по требованию и выборочной проверки, в том числе для задач Container_Scan.

- Автоматическое добавление динамических правил для Агента Администрирования

Реализована возможность автоматического добавления предзаданных (динамических) правил для Агента администрирования (nagent) в пакетные правила для задачи Firewall_Management.

- Блокировка файлов во время проверки

  Реализована возможность включения опции блокировки файлов во время проверки. При включении опции действие при обнаружении объекта для файловых перехватчиков (Removable_Drives_Scan, File_Threat_Protection, Anti_Cryptor) не будет применяться: программа только зарегистрирует событие об обнаружении объекта. В настройках Защиты от файловых угроз (File_Threat_Protection) больше недоступно действие **Пропускать**.

- Настройки файлов трассировки

  Изменены возможные значения и значения по умолчанию параметров создания файлов трассировки (максимальное количество записей в файле и максимальный размер файлов).

- Kaspersky Security Center Cloud Console

  Добавлена возможность управления устройствами, на которых установлен Kaspersky Endpoint Security 11 для Linux, с помощью Kaspersky Security Center Cloud Console.

- Процесс kesl-supervisor переименован в kesl.

- Информация об инициаторе добавлена во все события. Эта информация включена в отчеты.

- Действие **Cure** переименовано в **Disinfect**.

- Добавлена возможность указывать список масок устройств, которые будут проверены задачей Boot_Scan.

- Обновлен список поддерживаемых операционных систем.

- Реализована поддержка работы с файловой системой GlusterFS.

- Инструмент проверки целостности позволяет проверять модули программы и файлы на несанкционированное изменение или повреждения.

Установка программы

Этот раздел содержит инструкции по установке Kaspersky Endpoint Security из пакета установки (далее "пакет") и по установке Агента администрирования.

Сценарий: установка и первоначальная настройка Kaspersky Endpoint Security

Сценарий описывает установку и первоначальную настройку Kaspersky Endpoint Security, а также установку и настройку пакета Агента администрирования.

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

1. **Установка пакета Kaspersky Endpoint Security**

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

2. **Выполнение первоначальной настройки Kaspersky Endpoint Security**

   После завершения установки Kaspersky Endpoint Security запустите скрипт послеустановочной настройки. Выполнение первоначальной настройки необходимо для включения защиты вашего компьютера. Скрипт послеустановочной настройки Kaspersky Endpoint Security входит в пакет Kaspersky Endpoint Security.

   На этапе первоначальной настройки можно вручную указать значения параметров или использовать конфигурационный файл первоначальной настройки для выполнения первоначальной настройки автоматически. При необходимости можно изменить значения параметров в конфигурационном файле первоначальной настройки.

3. **Установка Агента администрирования**

   Установите Агент администрирования. Этот шаг необходим, если вы планируете управлять Kaspersky Endpoint Security с помощью Kaspersky Security Center.

4. **Первоначальная настройка Агента администрирования**

   После установки Агента администрирования настройте его параметры.

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

   Для управления Kaspersky Endpoint Security с помощью Kaspersky Security Center необходимо установить плагин управления Kaspersky Endpoint Security. Дополнительная информация приведена в документации Kaspersky Security Center.

   Плагин управления Kaspersky Endpoint Security 11 для Linux, плагин управления Kaspersky Endpoint Security Service Pack 1 для Linux и плагин управления Kaspersky Endpoint Security Service Pack 1 Maintenance Release 1 для Linux можно установить одновременно. Таким образом, можно управлять программой с помощью политик, созданных с помощью различных версий плагина управления. Можно также преобразовать политики и задачи, созданные с помощью предыдущих версий плагина управления, в новые версии.

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

Установка пакета Kaspersky Endpoint Security

Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM.

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

```
# rpm -i kesl-11.0.0-<номер сборки>.i386.rpm
```

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

```
# rpm -i kesl-11.0.0-<build number>.x86_64.rpm
```

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

```
# dpkg -i kesl-11.0.0-<номер сборки>_i386.deb
```

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

```
# dpkg -i kesl_11.0.0-<номер сборки>_amd64.deb
```

О первоначальной настройке Kaspersky Endpoint Security

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

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

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

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

Скрипт послеустановочной настройки пошагово запрашивает значения параметров Kaspersky Endpoint Security.

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

Только Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux можно обновить до Kaspersky Endpoint Security 11 для Linux.

Антивирус Касперского 8.0 для Linux File Server, Kaspersky Endpoint Security 10 для Linux и Kaspersky Endpoint Security 10 Service Pack 1 невозможно обновить до Kaspersky Endpoint Security 11 для Linux. Сначала нужно удалить предыдущую версию программы, а затем установить Kaspersky Endpoint Security 11 для Linux.

Шаг 1. Выбор языкового стандарта

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

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

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

```
# locale -a
```

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

Шаг 2. Принятие Лицензионного соглашения

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

Можно просмотреть текст с помощью утилиты `less`. Чтобы переходить по разделам текста, используйте клавиши со стрелками или клавиши **B** (чтобы перейти на один экран назад) и **F** (чтобы перейти на один экран вперед). Для получения справки нажмите на клавишу **H**. Чтобы завершить просмотр, нажмите на клавишу **Q**.

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.

Шаг 3. Принятие Политики конфиденциальности

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

Можно просмотреть текст с помощью утилиты `less`. Чтобы переходить по разделам текста, используйте клавиши со стрелками или клавиши **B** (чтобы перейти на один экран назад) и **F** (чтобы перейти на один экран вперед). Для получения справки нажмите на клавишу **H**. Чтобы завершить просмотр, нажмите на клавишу **Q**.

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`) – принять Политику конфиденциальности.
- `no` (или `n`) – не принимать Политику конфиденциальности.

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

Шаг 4. Участие в Kaspersky Security Network

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

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 не прерывает процесс установки Kaspersky Endpoint Security. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент.

Шаг 5. Настройка графического пользовательского интерфейса

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

Введите одно из следующих значений:

- `yes` (или `y`), чтобы включить использование графического пользовательского интерфейса. Kaspersky Endpoint Security проверит наличие всех нужных библиотек и при необходимости попробует установить отсутствующие.

- `no` (или `n`), чтобы не включать использование графического пользовательского интерфейса.

Вы можете включить или выключить использование графического пользовательского интерфейса в любой момент.

Шаг 6. Определение типа перехватчика файловых операций

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

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

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

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

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

Шаг 7. Настройка источника обновлений

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

Введите одно из следующих значений:

- `KLServers` – Kaspersky Endpoint Security получает обновления с одного из серверов обновлений "Лаборатории Касперского".

- `SCServer` – Kaspersky Endpoint Security загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновлений, если вы используете

программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации.

- `<Url>` – Kaspersky Endpoint Security загружает обновления из пользовательского источника. Вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.

Шаг 8. Настройка параметров прокси-сервера

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

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

По умолчанию в программе указано значение `no`.

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

Шаг 9. Загрузка антивирусных баз Kaspersky Endpoint Security

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

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

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

По умолчанию предлагается ответ `yes`.

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

Задачу обновления можно запустить без использования скрипта первоначальной настройки.

Шаг 10. Включение автоматического обновления антивирусных баз

На этом шаге вы можете включить автоматическое обновление антивирусных баз.

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

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

Вы можете включить автоматическое обновление антивирусных баз без помощи скрипта первоначальной настройки путем управления расписанием задачи обновления.

Шаг 11. Активация программы

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

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

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

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

Вы можете установить файл ключа без использования скрипта первоначальной настройки.

Автоматический режим первоначальной настройки Kaspersky Endpoint Security

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

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

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

Параметры конфигурационного файла первоначальной настройки Kaspersky Endpoint Security kesl.ini

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

Параметры конфигурационного файла первоначальной настройки Kaspersky Endpoint Security

Параметр	Описание	Возможные 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.
USE_KSN	Согласие с Положением о Kaspersky Security Network	`yes` – принять Положение о Kaspersky Security Network. `no` – не принимать Положение о Kaspersky Security Network.
LOCALE	Дополнительный параметр Языковой стандарт, используемый при работе Kaspersky Endpoint Security	Языковой стандарт в формате, определенном в RFC 3066. Если параметр `LOCALE` не указан, устанавливается языковой стандарт системы по умолчанию.

INSTALL_LICENSE	Код активации или файл ключа	None
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.
USE_GUI	Включение использования графического пользовательского интерфейса	• `yes` – включить использование графического пользовательского интерфейса. • `no` – выключить использование графического пользовательского интерфейса.

		Чтобы изменения значений параметров вступили в силу, требуется перезапустить программу.
IMPORT_SETTINGS	Использование параметров программы из конфигурационного файла	• `yes` – использовать параметры программы из конфигурационного файла. • `no` – не использовать параметры программы из конфигурационного файла.

Если вы хотите изменить параметры в конфигурационном файле первоначальной настройки Kaspersky Endpoint Security kesl.ini, вводите 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

Вы можете установить Kaspersky Endpoint Security на компьютер с помощью Kaspersky Security Center.

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

Установка Агента администрирования

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

Запускать процесс установки Агента администрирования требуется с root-правами.

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

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

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

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

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

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

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

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

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

- для 32-битных операционных систем:
  `/opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl`
- для 64-битных операционных систем:
  `/opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl`

Если вы планируете управлять Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console, для централизованного обновления баз в инфраструктуре вашей организации должен быть как минимум один компьютер с операционной системой Microsoft Windows и установленным Агентом администрирования соответствующей версии. Агенты администрирования для операционных систем на базе Linux не используются для ретрансляции баз.

Начальная настройка параметров Агента администрирования

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

Чтобы настроить параметры Агента администрирования, выполните следующие действия:

1. Выполните команду:

   - для 32-битных операционных систем:
     `# /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl`

- для 64-битных операционных систем:

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

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

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

   По умолчанию используется порт 13000.
5. Выполните одно из следующих действий:

   - Введите `yes`, чтобы использовать SSL-соединение.
   - Введите `no`, чтобы не использовать SSL-соединение.

   По умолчанию SSL-соединение включено.
6. При необходимости укажите режим шлюза соединений:

   - `0` – не использовать шлюз соединений.
   - `1` – использовать Агент администрирования в качестве шлюза соединений.
   - `2` – подключаться к Серверу администрирования с помощью шлюза соединений.

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

Обновление старой версии программы

Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux можно обновить до Kaspersky Endpoint Security 11 для Linux.

Независимо от того, была ли программа Kaspersky Endpoint Security запущена до начала процесса обновления, если обновление завершено успешно, то запустится новая версия программы. Если выполнить обновление не удалось, запустится предыдущая версия.

Вы можете обновить предыдущую версию программы следующими способами:

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

Доступно только обновление Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux до Kaspersky Endpoint Security 11 для Linux. Если у вас установлена версия Kaspersky Endpoint Security 10 Service Pack 1 для Linux, сначала необходимо обновить ее до версии Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1, а затем – до версии Kaspersky Endpoint Security 11 для Linux. Если у вас установлена программа Kaspersky Endpoint Security 10 для Linux, ее необходимо удалить, а затем установить Kaspersky Endpoint Security 11.

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

Обновление программы с помощью командной строки

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

Перед обновлением программы необходимо принять Лицензионное соглашение (/opt/kaspersky/kesl/doc/license.<ID языка>) и Политику конфиденциальности (/opt/kaspersky/kesl/doc/license.<ID языка>). Если вы не согласны с положениями Лицензионного соглашения и Политики конфиденциальности, программа не будет обновлена.

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

Чтобы обновить программу, выполните следующие действия:

1. Прочитайте текст Лицензионного соглашения (/opt/kaspersky/kesl/doc/license.<ID языка>) и Политики конфиденциальности (/opt/kaspersky/kesl/doc/license.<ID языка>).
2. Если вы планируете участвовать в Kaspersky Security Network, прочитайте текст Положения о Kaspersky Security Network (/opt/kaspersky/kesl/doc/ksn_license.<ID языка>).

Отказ от участия в Kaspersky Security Network не прерывает процесс обновления Kaspersky Endpoint Security. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент.

3. Если вы согласны с условиями Лицензионного соглашения и Политики конфиденциальности, запустите установку требуемого пакета Kaspersky Endpoint Security 11 для Linux:

   - Пакет в формате RPM:

     ```
     # KESL_EULA_AGREED=Yes KESL_PRIVACY_POLICY_AGREED=Yes
     KESL_USE_KSN=<Yes/No> rpm -U --replacefiles --replacepkgs <имя
     пакета в формате rpm>.rpm
     ```

   - Пакет в формате DEB:

     ```
     # KESL_EULA_AGREED=Yes KESL_PRIVACY_POLICY_AGREED=Yes
     KESL_USE_KSN=<Yes/No> dpkg -i <имя пакета в формате deb>.deb
     ```

   Будет выполнен экспорт параметров и журнала событий Kaspersky Endpoint Security 10 Service Pack 1 для Linux.

4. Перезапустите программу.

5. При необходимости перезагрузите операционную систему.

Если во время обновления программы произошла ошибка, программа автоматически восстанавливается до предыдущей версии. Отображается сообщение об ошибке.

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

Обновление программы с помощью Kaspersky Security Center

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

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

1. Обновите Агент администрирования до последней версии.

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

   Программа работает корректно во время обновления Агента администрирования.

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

Если для завершения установки необходимо перезапустить Kaspersky Endpoint Security и возникло событие *NeedToRestart*, дождитесь завершения задачи удаленной установки. После этого перезапустите Kaspersky Endpoint Security с помощью Kaspersky Security Center. Если пакет установлен успешно, после перезапуска откроется новая версия программы. Если установка пакета завершилась с ошибкой, программа откатывает обновления и запускается предыдущая версия. Однако в менеджере пакетов будет указана новая версия (rpm/dpkg).

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

Настройка разрешающих правил в системе SELinux

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

1. Переведите SELinux в разрешающий режим:

   - Если SELinux был активирован, выполните следующую команду:
     ```
     # setenforce Permissive
     ```
   - Если SELinux был выключен, в конфигурационном файле `/etc/selinux/config` задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.

2. Запустите следующие задачи:

   - задачу Защита от файловых угроз:
     ```
     kesl-control --start-task 1
     ```
   - задачу проверки загрузочных секторов:
     ```
     kesl-control --start-task 4 -W
     ```
   - задачу проверки памяти процессов:
     ```
     kesl-control --start-task 5 -W
     ```

   Рекомендуется запустить все задачи, которые вы планируете запускать при использовании Kaspersky Endpoint Security.

3. Создайте модуль правил на основе блокирующих записей:

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

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

4. Загрузите полученный модуль правил:

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

5. Переведите SELinux в принудительный режим:

   ```
   # setenforce Enforcing
   ```

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

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

Настройка разрешающих правил в системе AppArmor

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

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

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

2. Создайте профиль Kaspersky Endpoint Security:

   a. В первой консоли выполните команды:

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

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

   - задачу Защита от файловых угроз:

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

   - задачу проверки загрузочных секторов:

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

- задачу проверки памяти процессов:
```
kesl-control --start-task 5 -W
```

- задачу обновления:
```
kesl-control --start-task 6 -W
```

Рекомендуется запустить все задачи, которые вы планируете запускать при использовании Kaspersky Endpoint Security.

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

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

Созданные профиль можно определить вручную или с помощью команды:

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

3. Переведите созданный профиль Kaspersky Endpoint Security в режим показа сообщений:
```
aa-complain <имя файла профиля Kaspersky Endpoint Security>
```

4. Через несколько дней работы программы обновите профиль, запустив команду:
```
aa-logprof
```

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

5. Переведите профиль Kaspersky Endpoint Security в блокирующий режим:
```
aa-enforce <имя файла профиля Kaspersky Endpoint Security>
```

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

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

Удаление программы

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

Локальное удаление Kaspersky Endpoint Security

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

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

```
# rpm -e kesl
```

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

```
# dpkg -r kesl
```

Чтобы удалить Агент администрирования, который был установлен на 32-битную операционную систему из пакета формата RPM, выполните следующую команду:

```
# rpm -e klnagent
```

Чтобы удалить Агент администрирования, который был установлен на 64-битную операционную систему из пакета формата RPM, выполните следующую команду:

```
# rpm -e klnagent64
```

Чтобы удалить Агент администрирования, который был установлен на 32-битную операционную систему из пакета формата DEB, выполните следующую команду:

```
# dpkg -r klnagent
```

Чтобы удалить Агент администрирования, который был установлен на 64-битную операционную систему из пакета формата DEB, выполните следующую команду:

```
# dpkg -r klnagent64
```

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

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

Удаление Kaspersky Endpoint Security через Kaspersky Security Center

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

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

Лицензирование программы

В этом разделе описаны основные аспекты лицензирования программы.

О лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

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

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

О лицензии

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

Лицензия включает в себя право на получение следующих видов услуг:

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

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

Предусмотрены следующие типы лицензий:

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

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

  Вы можете активировать программу по пробной лицензии только один раз.

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

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

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

О лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

О лицензионном ключе

Лицензионный ключ – последовательность битов, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Лицензионные ключи формируются "Лабораторией Касперского".

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

Лицензионный ключ может быть заблокирован "Лабораторией Касперского" в случае нарушения условий Лицензионного соглашения. Если лицензионный ключ был заблокирован, необходимо добавить другой ключ, чтобы использовать программу.

Лицензионный ключ может быть активным и дополнительным.

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы программы. Активный лицензионный ключ можно добавить для пробной и коммерческой лицензии. В программе не может быть несколько активных лицензионных ключей.

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

Лицензионный ключ для пробной лицензии можно добавить в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии невозможно добавить в качестве дополнительного лицензионного ключа.

О коде активации

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

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

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

О файле ключа

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

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

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

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

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

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" с помощью имеющегося у вас кода активации.

О подписке

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

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

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

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

В зависимости от поставщика услуг, набор возможных действий для управления подпиской может различаться. Поставщик услуг может не предоставлять льготный период для продления подписки, в течение которого функциональность программы сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Endpoint Security.

О предоставлении данных

Если программа была активирована с использованием кода активации, с целью проверки законности использования программы и получения статистической информации о распространении и использовании продуктов держателя лицензии, вы соглашаетесь передавать в автоматическом режиме следующую информацию: код активации, уникальный идентификатор активации текущей лицензии, время активации лицензии, параметры упаковки подтверждения статуса лицензионного ключа, дату и время создания ключа программы, тип, версию и языковые настройки установленной программы, версию установленных обновлений, идентификатор компьютера и идентификатор установки программы на компьютер, статус защиты от файловых угроз.

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 продуктов держателя лицензии, вы соглашаетесь в автоматическом режиме предоставлять следующую информацию: версию и языковые настройки установленной программы, идентификаторы компонентов программы, подлежащие обновлению, идентификатор установки программы на компьютер, тип, версию и разрядность операционной системы.

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

- идентификаторы выполненных команд;
- идентификатор операции, выполняемой сторонним ПО;
- идентификатор обновления стороннего ПО;
- идентификатор регионального центра активации;
- имя отправителя маркетинговых рассылок, определенное эвристически;

- содержимое фрагментов обрабатываемого объекта;
- уникальный идентификатор журнала действий обрабатываемого объекта;
- дата и время истечения срока действия сертификата;
- дата и время выпуска сертификата;
- версия списка отозванных решений служб программы;
- уникальный идентификатор события;
- дата и время возникновения события;
- идентификатор базы, по которой выполняется категоризация программ;
- идентификатор записи в базе программы;
- тип сработавшей записи в антивирусной базе программы;
- версия записи в базе программы;
- идентификатор сработавшей записи в антивирусной базе программы;
- отметка времени сработавшей записи в антивирусной базе программы;
- тип сработавшей записи в антивирусной базе программы;
- дата и время выпуска баз программы;
- отметка времени выпуска баз программы;
- бинарная маска вариантов запроса DNS;
- тип DNS-запроса;
- атакуемый локальный порт;
- идентификатор устройства;
- версия операционной системы;
- номер сборки операционной системы;
- номер обновления операционной системы;
- выпуск операционной системы;

- расширенная информация о выпуске операционной системе;
- версия пакета обновлений операционной системы;
- идентификатор учетной записи, с правами которой был запущен контролируемый процесс;
- IP-адрес;
- уникальный идентификатор экземпляра установки программы на компьютере;
- список сетевых интерфейсов на компьютере;
- метод HTTP-запроса;
- местоположение вставки кода в процесс;
- уникальный идентификатор пользователя в системе правообладателя;
- дата активации лицензии;
- дата окончания срока действия лицензии;
- идентификатор лицензии;
- индекс зоны, к которой принадлежит IP-адрес узла;
- идентификатор ключа шифрования в хранилище ключей;
- имя компьютера в сети (доменное имя);
- статус лицензии, используемой программой;
- версия протокола, используемого для подключения к KSN;
- идентификатор веб-сервиса, к которому обращается программа;
- характеристики шифрования пакета данных, отправляемого в KSN;
- идентификатор пакета данных, отправляемого в KSN;
- внешний IP-адрес;
- локальный IP-адрес;
- MAC-адрес источника сетевой атаки;
- название сетевого протокола, используемого при обнаружении сетевой атаки;

- направление сетевого соединения;
- тип учетной записи пользователя, с правами которой был запущен возможно зараженный объект;
- атрибуты файла обрабатываемого объекта;
- последовательность фрагментов обрабатываемого объекта;
- данные внутреннего журнала, сформированного модулем антивирусной программы для обрабатываемого объекта;
- название источника сертификата;
- публичный ключ сертификата;
- алгоритм вычисления публичного ключа сертификата;
- серийный номер сертификата;
- дата и время подписания объекта;
- имя владельца и параметры сертификата;
- отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования;
- дата и время последнего изменения обрабатываемого объекта;
- дата и время создания обрабатываемого объекта;
- характеристики обнаружения;
- атрибуты обрабатываемого исполняемого файла;
- дата и время создания обрабатываемого исполняемого файла;
- описание обрабатываемого объекта, как указано в свойствах объекта;
- энтропия обрабатываемого файла;
- формат обрабатываемого объекта;
- тип контрольной суммы обрабатываемого объекта;
- размер образа программы;
- результат проверки статуса обрабатываемого объекта в KSN;

- дата и время ссылки на исполняемый файл;
- контрольная сумма (MD5) обрабатываемого объекта;
- название обрабатываемого объекта;
- названия упаковщиков, которые упаковали обрабатываемый объект;
- индикатор, показывающий, является ли обрабатываемый объект PE-файлом;
- значение атрибута характеристик из заголовка PE-файла;
- битовая маска раздела директорий данных в PE-файле;
- размер наложения в PE-файле;
- количество разделов в PE-файле;
- значение атрибута подсистемы из заголовка PE-файла;
- название программы;
- контрольная сумма (MD5) маски, блокирующей веб-сервис;
- контрольная сумма (SHA-256) обрабатываемого объекта;
- информация о том, кто подписал обрабатываемый файл;
- размер обрабатываемого объекта;
- флаг, показывающий, запускается ли программа автоматически при старте системы;
- название обнаруженного вредоносного ПО или легального ПО, которое может использоваться для причинения вреда компьютеру или данным пользователя;
- код типа объекта;
- имя поставщика программы;
- решение программы относительно обрабатываемого объекта;
- версия обрабатываемого объекта;
- время первого запуска обрабатываемого объекта;
- источник решения, принятого относительно обрабатываемого объекта;

- контрольная сумма обрабатываемого объекта;
- название родительской программы;
- уровень целостности обрабатываемого объекта;
- контрольная сумма (MD5) обрабатываемого объекта;
- результат проверки целостности модулей;
- обнаруженные файловые операции над обрабатываемым объектом;
- результат действия над обрабатываемым объектом;
- код файловой операции;
- путь к обрабатываемому объекту;
- код директории;
- системный идентификатор процесса (PID);
- дата и время установки обнаруженного ПО;
- источник даты и времени установки обнаруженного ПО;
- тип обнаруженного стороннего ПО;
- права доступа к обрабатываемому объекту;
- информация о результатах проверки сигнатуры файла;
- путь к файлу источника;
- идентификатор уязвимости;
- класс опасности уязвимости;
- выпуск операционной системы;
- полный пути к файлу родительского процесса, используемому для запуска процесса;
- системный идентификатор родительского процесса (PID);
- аргументы командной строки для процесса;
- контрольная сумма кода активации программы;

- идентификатор программы, полученный из лицензии;
- версия компонента программы;
- данные о лицензии для идентификации группы пользователей компании, которые приобрели лицензию, по комментарию в свойствах лицензионного ключа;
- полная версия программы;
- уникальный идентификатор компьютера;
- идентификатор обновления программы;
- идентификатор программы;
- дата и время установки программы;
- дата активации программы;
- идентификатор лицензии на программу;
- контрольная сумма файла ключа программы;
- идентификатор информационной модели, используемой для предоставления лицензии на программу;
- серийный номер ключа программы;
- идентификатор сертификата, используемого для подписи заголовка тикета лицензии на программу;
- дата и время создания тикета лицензии на программу;
- контрольная сумма тикета лицензии на программу;
- версия тикета лицензии на программу;
- версия кода активации программы;
- локализация программы;
- тип уведомления инициировавшего отправку статистики;
- версии операционной системы;
- версия программы;

- идентификатор организации-партнера, через которую был размещен заказ на приобретение лицензии на программу;
- информация об обновлениях программы;
- идентификатор установки ПО (PCID);
- идентификатор ребрэндинга программы;
- название компонента программы;
- идентификатор лицензионной программы;
- состояние работоспособности программы после обновления;
- флаг, показывающий, что программа подключена к My Kaspersky;
- индикатор участия в KSN;
- формат данных в запросе к инфраструктуре правообладателя;
- идентификатор тикета текущей лицензии;
- идентификатор компонента программы;
- название созданного / измененного сервиса операционной системы;
- ключ сеанса входа;
- алгоритм шифрования для ключа сеанса входа;
- результат действия программы;
- веб-адрес, с которого был загружен файл, соответствующий процессу;
- ответ DNS-сервера;
- IP-адрес DNS-сервера;
- дата и время окончания сбора статистики;
- код ошибки;
- действия пользователя с элементами интерфейса в окне программы;
- IP-адрес атакующего;

- индикатор обнаружения отладки;
- атрибут обрабатываемого объекта, позволяющий отозвать ложно-положительное решение касательно объекта;
- идентификатор задачи, в которой произошло обнаружение;
- количество подключений к KSN, выполненных из кеша;
- количество запросов с ответами в локальной базе запросов;
- количество неудачных подключений к KSN;
- количество неудачных транзакций с KSN;
- распределение по времени отмененных запросов к KSN;
- распределение по времени неудачных подключений к KSN;
- распределение по времени неудачных транзакций с KSN;
- распределение по времени успешных подключений к KSN;
- распределение по времени успешных транзакций с KSN;
- распределение по времени успешных запросов к KSN;
- распределение по времени запросов к KSN, выполнение которых превысило лимит;
- количество новых подключений к KSN;
- количество неудачных запросов к KSN; вызванных неправильной маршрутизацией;
- количество неудачных запросов, вызванных тем, что KSN была отключена в настройках программы;
- количество неудачных запросов к KSN; вызванных проблемами с сетью;
- количество успешных подключений к KSN;
- количество успешных транзакций с KSN;
- количество успешных запросов к KSN;
- задержка в отправке статистики;
- достоверность обнаружения доступа к фишинговому веб-сервису;

- цель фишинговой атаки;
- вес обнаруженного доступа к фишинговому веб-сервису;
- идентификатор протокола;
- идентификатор операции, выполняемой программой;
- дата и время начала сбора статистики;
- дата и время обнаружения ПО компонентом Анализ поведения;
- количество обнаруженных программ в контексте компонента Анализ поведения;
- причина обнаружения ПО компонентом Анализ поведения;
- версия отправляемой статистики;
- технические характеристики применяемых технологий обнаружения;
- 4-байтовый вектор, рассчитываемый по первым 4096-байтам раздела;
- числовая величина частоты, рассчитываемая по первым 4096-байтам раздела;
- нулевая величина частоты, рассчитываемая по первым 4096-байтам раздела;
- версия определенного компилятора;
- свойства и контрольные суммы путей в исполняемом файле;
- версия эмулятора;
- 4-байтовый вектор, рассчитываемый по последним 4096-байтам раздела;
- числовая величина частоты, рассчитываемая по последним 4096-байтам раздела;
- нулевая величина частоты, рассчитываемая по последним 4096-байтам раздела;
- глубина эмуляции;
- тип задачи проверки исполняемых файлов, которая отправляет статистику;
- время хранения обрабатываемого объекта;
- алгоритм вычисления отпечатка цифрового сертификата;
- название компонента;

- отметка времени обновления компонента (обновленная версия);
- отметка времени компонента (локальная версия);
- количество неудачных попыток установки обновлений, совершенных компонентом, выполняющим обновления;
- код категории ошибки;
- количество ошибок установки обновлений, совершенных компонентом, выполняющим обновления;
- отметка времени root-индекса для загружаемых обновлений;
- отметка времени root-индекса для доступных обновлений;
- код ошибки задачи обновлений;
- значение фильтра TARGET в задаче обновления;
- тип задачи обновления;
- версия компонента, выполняющего обновления;
- бинарная маска параметров для обрабатываемых объектов;
- контрольная сумма имени пользователя;
- идентификатор безопасности учетной записи пользователя (SID);
- адрес веб-сервиса, к которому обращается программа (URL, IP-адрес);
- заголовок обрабатываемого http-запроса;
- IPv4-адрес веб-сервиса, к которому обращается программа;
- IPv6-адрес веб-сервиса, к которому обращается программа;
- номер порта;
- веб-адрес источника запроса к веб-сервису (источник ссылки);
- обрабатываемый веб-адрес;
- информация о клиенте, использующем сетевой протокол (пользовательский агент);
- идентификатор зоны безопасности, полученный из потока NTFS.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Передача данных осуществляется по защищенному каналу.

Более подробную информацию об отправке в "Лабораторию Касперского" статистической информации, полученной во время использования KSN, ее хранении и уничтожении вы можете прочитать в Лицензионном соглашении, Положении о Kaspersky Security Network и Политике конфиденциальности на веб-сайте "Лаборатории Касперского". Файлы license.<ID языка> и ksn_license.<ID языка> с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки программы.

Запуск и остановка программы

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

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

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

```
systemctl start kesl
```

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

```
systemctl stop kesl
```

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

```
systemctl restart kesl
```

Чтобы запустить Kaspersky Endpoint Security, выполните следующую команду:

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

Чтобы остановить Kaspersky Endpoint Security, выполните следующую команду:

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

Чтобы перезапустить Kaspersky Endpoint Security, выполните следующую команду:

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

Подготовка к запуску программы в операционной системе Astra Linux

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

Для Astra Linux Special Edition версии 1.6 (ядро PaX)

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 диски оперативной памяти:

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

Для Astra Linux Special Edition версии 1.5 (ядро PaX)

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 диски оперативной памяти:

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

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

Мониторинг статуса программы

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

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

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

```
systemctl status kesl
```

Чтобы вывести статус Kaspersky Endpoint Security, выполните следующую команду:

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

Общие параметры Kaspersky Endpoint Security

В этом разделе описаны общие параметры Kaspersky Endpoint Security.

Общие параметры конфигурационного файла имеют следующие значения:

SambaConfigPath

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

По умолчанию указана стандартная директория конфигурационного файла Samba на компьютере.

После изменения значения этого параметра требуется перезапустить программу.

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

NfsExportPath

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

По умолчанию указана стандартная директория конфигурационного файла NFS на компьютере.

После изменения значения этого параметра требуется перезапустить программу.

Значение по умолчанию: `/etc/exports`

TraceFolder

Директория, в которой хранятся файлы трассировки программы. В файлах трассировки содержится информация об операционной системе, а также могут содержаться персональные данные.

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 заданной по умолчанию директории хранения файлов трассировки требуются root-права.

После изменения значения этого параметра требуется перезапустить программу.

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

TraceLevel

Уровень детализации журнала трассировки.

Доступные значения:

`Detailed` – наиболее детализированный журнал трассировки.

`NotDetailed` – журнал трассировки содержит оповещения об ошибках.

`None` – не создает журнал трассировки.

Значение по умолчанию: `None`

TraceMaxFileCount

Максимальное количество файлов трассировки программы.

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

После изменения значения этого параметра требуется перезапустить программу.

Доступные значения: `1 – 10000`

Значение по умолчанию: `5`

TraceMaxFileSize

Максимальный размер файла трассировки программы (в мегабайтах).

После изменения значения этого параметра требуется перезапустить программу.

Доступные значения: `1 – 1000`

Значение по умолчанию: `500`

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 технологи fanotify.

Доступные значения: `4096 – 33554432`

Значение по умолчанию: `16384`

DetectOtherObjects

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

Доступные значения:

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

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

Значение по умолчанию: `No`

NamespaceMonitoring

Включает или отключает проверку пространств имен и Docker-контейнеров.

Доступные значения:

`Yes` – включить проверку пространств имен и Docker-контейнеров.

`No` – выключить проверку пространств имен и Docker-контейнеров.

Значение по умолчанию: `Yes`

DockerSocket

Адрес файла или сетевого Docker-сокета.

Значение по умолчанию: `/var/run/docker.sock`

ContainerScanAction

Действие над Docker-контейнером при обнаружении зараженного объекта.

Действия над зараженным объектом *внутри Docker-контейнера* описаны в параметрах соответствующей задачи.

Доступные значения:

`StopContainerIfFailed` – остановить Docker-контейнер, если не удалось вылечить зараженный объект.

`StopContainer` – остановить Docker-контейнер при обнаружении зараженного объекта.

`Skip` – не выполнять никаких действий над Docker-контейнерами при обнаружении зараженного объекта.

Значение по умолчанию: `StopContainerIfFailed`

InterceptorProtectionMode

Показывает, блокирует ли программа файлы при проверке.

Доступные значения:

`Full` – блокировать файлы при проверке.

`Info` – не блокировать файлы при проверке, при обнаружении зараженного объекта фиксировать события в журнале событий.

Значение по умолчанию: `Full`

UseKSN

Включает или выключает участие в Kaspersky Security Network.

Доступные значения:

`No` – выключить участие в Kaspersky Security Network.

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

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

Значение по умолчанию: `No`

UseProxy

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

Доступные значения:

`Yes` – включить использование прокси.

`No` – выключить использование прокси.

Значение по умолчанию: `No`

ProxyServer

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

MaxEventsNumber

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

Значение по умолчанию: `500000`

LimitNumberOfScanFileTasks

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

Доступные значения: `0 – 4294967295`

Значение по умолчанию: `0`

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

UseSysLog

Включает или выключает запись информации о событиях в syslog.

Для доступа к syslog требуются root-права.

Доступные значения:

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

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

Значение по умолчанию: `No`

EventsStoragePath

Файл базы данных, в которой Kaspersky Endpoint Security 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`

ExcludedMountPoint.item_#

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

Доступные значения:

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

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

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

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

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

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

Параметр `ExcludedMountPoint.item_#` не указан по умолчанию.

Команды управления параметрами Kaspersky Endpoint Security и задачами

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

Получение общих параметров Kaspersky Endpoint Security

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

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

1. Сохраните общие параметры Kaspersky Endpoint Security в конфигурационном файле с помощью команды `--get-app-settings`.

2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.

3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `--set-app-settings`. Kaspersky Endpoint Security применит новые

значения параметров после того, как вы остановите и снова запустите Kaspersky Endpoint Security.

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

Синтаксис команды

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

kesl-control [-T] --get-app-settings
```

Аргументы и ключи

`--file <имя конфигурационного файла>`

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

Пример:

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

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

Изменение общих параметров Kaspersky Endpoint Security

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

Для изменения параметров программы необходимо наличие root-прав.

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

1. Сохраните общие параметры Kaspersky Endpoint Security в конфигурационном файле с помощью команды `--get-app-settings`.

2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.

3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `--set-app-settings`. Kaspersky Endpoint Security применит новые значения параметров после перезапуска.

Синтаксис команды

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

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

Аргументы и ключи

`--file <имя конфигурационного файла>`

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

Примеры:

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

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

Установить низкий уровень детализации журнала трассировки:

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

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

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

Вывод справки о командах Kaspersky Endpoint Security

Команда `kesl-control` с ключом `--help <набор команд Kaspersky Endpoint Security>` возвращает справку по командам Kaspersky Endpoint Security.

Синтаксис команды

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

<набор команд Kaspersky Endpoint Security>

Доступные значения:

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

`[-L]` – команды управления ключами.

`[-B]` – команды управления хранилищем.

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

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

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

`[-S]` – команды статистики.

`-W` – мониторинг событий.

Включение вывода событий

Команда `kesl-control -W` включает вывод событий Kaspersky Endpoint Security. Эту команду можно использовать либо отдельно для вывода всех событий безопасности Kaspersky Endpoint Security, либо совместно с командой `kesl-control --start-task` для вывода событий, связанных только с запущенной задачей. Чтобы указать условия для вывода только определенных событий, можно использовать команду `--query` с флагом `-W`.

Команда возвращает название события и дополнительную информацию о событии.

Синтаксис команды

```
kesl-control -W
```

Пример:

Включить режим вывода событий Kaspersky Endpoint Security:

```
kesl-control -W
```

Просмотр информации о программе

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

Синтаксис команды

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

Результат выполнения команды

- **Название**. Название программы.
- **Версия**. Текущая версия программы.
- **Статус ключа**. Статус ключа.
- **Статус подписки**. Статус подписки. Это поле отображается, если программа используется по подписке.
- **Дата окончания срока действия лицензии**. Дата окончания срока действия лицензии.
- **Состояние хранилища**. Состояние хранилища. Отображает информацию об ограничениях времени и размера.
- **Использование Хранилища**. Размер хранилища.
- **Дата последнего запуска задачи Scan_My_Computer**. Время последнего запуска задачи Scan_My_Computer.
- **Дата последнего выпуска баз**. Время последнего выпуска баз.
- **Антивирусные базы загружены**. Показывает, загружены ли антивирусные базы.
- **Состояние KSN**. Состояние участия в Kaspersky Security Network.
- **Политика**. Показывает, применяется ли политика Kaspersky Security Center или Linux Management Console.
- **Контроль файлов**. Состояние задачи Защита от файловых угроз.
- **Контроль целостности**. Состояние задачи Контроль целостности системы.
- **Управление сетевым экраном**. Состояние задачи Управление сетевым экраном.
- **Защита от шифрования**. Состояние задачи Защита от шифрования.
- **Защита от веб-угроз**. Состояние задачи Защита от веб-угроз.
- **Контроль устройств**. Состояние задачи Контроль устройств.
- **Проверка съемных дисков**. Состояние задачи Проверка съемных дисков.

- **Защита от сетевых угроз**. Состояние задачи Защита от сетевых угроз.
- **Анализ поведения**. Состояние задачи Анализ поведения.
- **Состояние обновления программы**. Показывает действия по обновлению программы и действия, которые должен выполнить пользователь.

Установка ограничения на использование памяти программой

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

Минимальное значение: 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 процентное значение изменить невозможно.

Чтобы указать ограничение на использование памяти, выполните следующие действия:

1. Остановите Kaspersky Endpoint Security.
2. В файле /var/opt/kaspersky/kesl/common/kesl.ini добавьте следующий параметр в раздел [General]:

   ```
   ScanMemoryLimit=<ограничение на использование памяти в мегабайтах>
   ```

3. Запустите Kaspersky Endpoint Security.

Ограничение на использование памяти изменяется при запуске программы.

Команды Kaspersky Endpoint Security

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

Ниже приведены правила использования команд Kaspersky Endpoint Security.

- Команды чувствительны к регистру.
- Ключи необходимо разделять символом "пробел".

- При использовании полного названия команды или ключа, значение необходимо указывать после символа "равно" (=).

  Пример:

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

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

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

Вывод справки о командах Kaspersky Endpoint Security

```
--help
```

Выводит справку о командах Kaspersky Endpoint Security.

Вывод событий Kaspersky Endpoint Security

```
-W
```

Включает вывод событий Kaspersky Endpoint Security.

Команды управления параметрами Kaspersky Endpoint Security и задачами

```
-T
```

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

```
[-S] --app-info
```

Выводит общую информацию о Kaspersky Endpoint Security.

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

Возвращает общие параметры Kaspersky Endpoint Security.

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

Устанавливает общие параметры Kaspersky Endpoint Security.

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

Возвращает список существующих задач Kaspersky Endpoint Security.

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

Выводит состояние указанной задачи.

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

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

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

Удаляет задачу.

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

Запускает задачу.

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

Останавливает задачу.

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

Приостанавливает задачу. Приостановить задачу Обновление невозможно.

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

Возобновляет задачу. Возобновить задачу Обновление невозможно.

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

Выводит параметры задачи.

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

Устанавливает параметры задачи.

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

Создает и запускает временную задачу `Scan_File`.

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

Импортирует параметры программы в конфигурационный файл.

`[-T] --update-application`

Обновляет программу.

`[-T] --set-settings {<ID задачи>|<имя задачи>} set-to-default`

Восстанавливает значения по умолчанию для параметров задачи.

`[-S] --omsinfo --file <путь>`

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

Команды управления ключами

`-L`

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

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

Добавляет активный ключ.

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

Добавляет дополнительный ключ.

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

Удаляет активный ключ.

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

Удаляет дополнительный ключ.

`[-L] --query`

Выводит информацию о ключе.

Команды для задачи Управление сетевым экраном

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

Добавляет новое правило.

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

Удаляет правило.

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

Изменяет приоритетность правила.

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

Добавляет в зону IP-адрес.

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

Удаляет из зоны IP-адрес.

`-F --query`

Отображает информацию.

Команды для задачи Защита от шифрования

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

Отображает список заблокированных компьютеров.

`[-H] --allow-hosts`

Разблокирует недоверенные компьютеры.

Команда для задачи проверки Docker-контейнеров и образов

`[-T] --scan-container <контейнер|образ[:тег]>`

Создает временную задачу проверки Docker-контейнеров с параметрами пользовательской задачи проверки контейнеров (название задачи: Custom_Container_Scan, идентификатор задачи: 19). После завершения проверки временная задача автоматически удаляется. Можно указать имена или маски имен контейнеров и образов. Можно также указать идентификаторы контейнеров и образов.

Команды управления пользователями

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

Выводит список пользователей и ролей.

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

Присваивает роль определенному пользователю.

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

Отзывает роль у определенного пользователя.

Команды управления хранилищами

`-B`

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

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

Очищает хранилище, полностью или выборочно.

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

Выводит информацию об объектах в хранилище.

`--limit`

Максимальное количество объектов, о которых выводится информация.

`--offset`

Количество записей, на которое следует отступить от начала выборки.

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

Восстанавливает объект из хранилища.

Команды управления журналом событий

`-E`

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

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

Максимальное количество событий, о которых выводится информация.

`--query`

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

`--offset`

Количество записей, на которое следует отступить от начала выборки.

`--db`

Имя файла базы данных.

Команды управления расписанием задач

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

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

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

Выводит параметры расписания задачи.

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

Расписание запуска задачи.

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

`BR` – запускать задачу после обновления антивирусных баз.

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

Время запуска задачи.

`RandomInterval=<мин.>`

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

`RunMissedStartRules`

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

Примеры:

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

```
RuleType=Hourly

RunMissedStartRules=No

StartTime=2019/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
```

Экспорт и импорт параметров программы

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

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

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

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

При импорте или экспорте параметров из более старой версии программы для новых параметров устанавливаются значения по умолчанию.

Импорт параметров в более старую версию программы недоступен.

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

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

Экспортируйте параметры программы в конфигурационный файл с помощью следующей команды:

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

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

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

Роли пользователей

В этом разделе описаны роли пользователей и приведены инструкции по назначению и отзыву ролей.

О ролях

Роль – это набор прав и разрешений на управление программой Kaspersky Endpoint Security.

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

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

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

Роли

Название роли	Роль в программе	Права
Администратор	admin	• 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	• Управление только задачами Scan_File • Запуск и остановка задач обновления • Просмотр отчетов для созданных им/ей задач • Просмотр особых событий, общих для всех пользователей программы
Аудитор	audit	• Просмотр параметров программы • Просмотр статуса программы

- Просмотр всех задач, их параметров и расписания запуска
- Просмотр всех событий
- Просмотр всех объектов в хранилище

Просмотр списка пользователей и ролей

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

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

Назначение роли пользователю

Чтобы назначить роль определенному пользователю, выполните следующую команду:

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

Пример:

Назначение роли 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:

Отзыв роли audit у пользователя test15:

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

Управление задачами Kaspersky Endpoint Security с помощью командной строки

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

О задачах Kaspersky Endpoint Security

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

Для работы с Kaspersky Endpoint Security существует два типа задач:

- *Стандартная задача* – задача, которая создается во время установки программы. Невозможно удалять стандартные задачи, но можно изменять параметры этих задач.

- *Пользовательская задача* – задача, которую вы можете создавать или удалять самостоятельно.

Задачи Kaspersky Endpoint Security перечислены в следующей таблице.

Задачи Kaspersky Endpoint Security

Название	ID	Тип	Возможность создавать пользовательские задачи этого типа
File_Threat_Protection	1	OAS	Нет
Scan_My_Computer	2	ODS	Да
Scan_File	3	ODS	Да
Boot_Scan	4	BootScan	Да
Memory_Scan	5	MemoryScan	Да
Update	6	Update	Да
Rollback	7	Rollback	Да
License	9	License	Нет
Backup	10	Backup	Нет
System_Integrity_Monitoring	11	OAFIM	Нет
Firewall_Management	12	Firewall	Нет
Anti_Cryptor	13	AntiCryptor	Нет
Web_Threat_Protection	14	WTP	Нет

Device_Control	15	DeviceControl	Нет
Removable_Drives_Scan	16	RDS	Нет
Network_Threat_Protection	17	NTP	Нет
Container_Scan	18	ContainerScan	Да
Custom_Container_Scan	19	ContainerScan	Да
Behavior_Detection	20	BehaviorDetection	Нет

ID – номер задачи, который Kaspersky Endpoint Security 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.

Вы можете выполнять следующие действия над задачами:

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

Просмотр списка задач Kaspersky Endpoint Security

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

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

Список, в котором представлены задачи Kaspersky Endpoint Security.

Для каждой задачи отображается следующая информация:

- `Название`. Название задачи.
- `ID`. Идентификатор задачи.
- `Тип`. Тип задачи.
- `Состояние`. 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.

Если ваша лицензия не покрывает функции Защита от шифрования и Контроль целостности системы, информация об этих задачах не отображается.

Создание задачи

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

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

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

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

Здесь:

- `<имя задачи>` – имя, которое вы указываете для новой задачи;
- `<тип задачи>` – предустановленный тип задачи;

Задача указанного типа создается с параметрами по умолчанию.

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

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

Здесь:

- `<имя задачи>` – имя, которое вы указываете для новой задачи;
- `<тип задачи>` – предустановленный тип задачи;

- `<полный путь к конфигурационному файлу>` – это полный путь к конфигурационному файлу.

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

Изменение параметров задачи с помощью конфигурационного файла

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

1. Сохраните параметры задачи в конфигурационный файл:
   ```
   kesl-control --get-settings <имя задачи>|<task ID> --file <полный путь к файлу>
   ```
2. Откройте созданный конфигурационный файл для редактирования.
3. Измените нужный параметр в конфигурационном файле.
4. Сохраните изменения в конфигурационном файле.
5. Импортируйте в задачу параметры из конфигурационного файла:
   ```
   kesl-control --set-settings <имя задачи>|<task ID> --file <полный путь к файлу>
   ```

В результате будут обновлены параметры задачи.

Изменение параметров задачи с помощью командной строки

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

1. Укажите нужное значение параметра:

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

   Kaspersky Endpoint Security изменит указанный параметр.

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

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

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

Пример:

Чтобы указать новую область проверки, выполните следующую команду:

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

В конфигурационный файл будет добавлен новый 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 из командной строки

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

Восстановление заданных по умолчанию параметров не доступно для задач Откат обновлений и Управление хранилищем.

Чтобы восстановить заданные по умолчанию параметры задачи из командной строки, выполните следующие действия:

1. Выполните следующую команду:

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

   Kaspersky Endpoint Security 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>
   ```

   В конфигурационном файле задачи содержатся заданные по умолчанию значения всех параметров.

Запуск и остановка задачи

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

Чтобы запустить задачу, выполните следующую команду:

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

Чтобы остановить задачу, выполните следующую команду:

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

Управление областями проверки из командной строки

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

Чтобы добавить новую область проверки, выполните следующую команду:

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

В конфигурационный файл будет добавлен новый раздел `[ScanScope.item_#]`. Kaspersky Endpoint Security проверяет объекты в директории, указанной параметром `Path`.

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

Чтобы удалить область проверки, выполните следующую команду:

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

Раздел `[ScanScope.item_#]`, содержащий указанный путь, удаляется из конфигурационного файла задачи. Kaspersky Endpoint Security не проверяет объекты в директории, указанной параметром `Path`.

Управление исключенными областями из командной строки

Из командной строки можно добавить или удалить область исключений с указанным параметром `Path` для задач OAS, ODS, OAFIM, ODFIM и AntiCryptor.

Чтобы добавить новую область исключения, выполните следующую команду:

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

В конфигурационный файл будет добавлен новый раздел `[ExcludedFromScanScope.item_#]`. Kaspersky Endpoint Security исключает объекты в директории, указанной параметром `Path`.

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

Чтобы удалить область исключения, выполните следующую команду:

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

Раздел `[ExcludedFromScanScope.item_#]`, содержащий указанный путь, удаляется из конфигурационного файла задачи. Kaspersky Endpoint Security не исключает объекты в директории, указанной параметром `Path`.

Просмотр состояния задачи

Вы можете просматривать состояние задачи.

Чтобы просмотреть состояние задачи, выполните следующую команду:

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

Здесь:

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

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

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

Настройка расписания задачи

Чтобы настроить расписание задачи, выполните следующие действия:

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

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

2. Откройте конфигурационный файл для редактирования.

3. Задайте параметры расписания.

4. Сохраните изменения в конфигурационном файле.

5. Импортируйте параметры расписания в задачу с помощью следующей команды:

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

Получение параметров расписания задачи

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

Вы можете использовать эту команду для изменения расписания задачи:

1. Сохраните параметры расписания в конфигурационном файле с помощью команды `kesl-control --get-schedule`.

2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.

3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `kesl-control --set-schedule`. Kaspersky Endpoint Security применит новые значения параметров расписания немедленно.

Синтаксис команды

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

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

Аргументы и ключи

`<ID задачи>`

Идентификационный номер задачи в Kaspersky Endpoint Security.

`<имя задачи>`

Имя задачи.

`--file <имя конфигурационного файла>`

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

Пример:

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

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

Возвращает расписание задачи Обновление:

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

Изменение параметров расписания задачи

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

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

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

Синтаксис команды

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

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

Аргументы и ключи

`<ID задачи>`

Идентификационный номер задачи в Kaspersky Endpoint Security.

`<имя задачи>`

Имя задачи.

`--file <имя конфигурационного файла>`

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

Пример:

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

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

Удаление задачи

Вы можете удалять задачи, которые вы создали.

Чтобы удалить задачу, выполните следующую команду:

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

Задача Защита от файловых угроз (File_Threat_Protection ID:1)

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

О защите от файловых угроз

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

Во время работы задачи Защита от файловых угроз Kaspersky Endpoint Security выполняет проверку всех пространств имен во всех поддерживаемых операционных системах, если в общих параметрах программы для параметра `NamespaceMonitoring` задано значение `Yes` или в Web Console включен параметр **Мониторинг пространств имен и Docker-контейнеров** (**Параметры политики** → **Общие параметры** → **Параметры перехватчика**).

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

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

Создавать пользовательские задачи Защита от файловых угроз невозможно. Вы можете изменять параметры стандартной задачи Защита от файловых угроз.

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

О зараженных файлах

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

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

Особенности проверки символических и жестких ссылок

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

Проверка символических ссылок

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

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

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

Параметры задачи Защита от файловых угроз

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

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

ScanArchived

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

Доступные значения:

`Yes` – проверять архивы; Если указано значение `FirstAction=Recommended`, программа удаляет архив, содержащий угрозу.

`No` – не проверять архивы.

Значение по умолчанию: `No`

ScanSfxArchived

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

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы;

`No` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `No`

ScanMailBases

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

Доступные значения:

`Yes` – проверять файлы почтовых баз;

`No` – не проверять файлы почтовых баз.

Значение по умолчанию: `No`

ScanPlainMail

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

Доступные значения:

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

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

Значение по умолчанию: `No`

SizeLimit

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

Доступные значения:

`0` – `999,999`

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

Значение по умолчанию: `0`

TimeLimit

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

Доступные значения:

`0` – `9999`

`0` – продолжительность проверки объектов не ограничена.

Значение по умолчанию: `60`

FirstAction

Выбор первого действия Kaspersky Endpoint Security над зараженными объектами.

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

Доступные значения:

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

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

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

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

Значение по умолчанию: `Recommended`

SecondAction

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

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

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

Значение по умолчанию: `Block`

UseExcludeMasks

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeMasks

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

Значение по умолчанию не задано.

Пример:

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

UseExcludeThreats

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeThreats

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

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

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

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии. Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

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

ReportCleanObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportPackedObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

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

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

Значение по умолчанию: `No`

UseAnalyzer

Включает или отключает эвристический анализатор.

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

Доступные значения:

`Yes` – включить эвристический анализатор;

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`

HeuristicLevel

Уровень эвристического анализа.

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

Доступные значения:

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

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

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

`Recommended` – рекомендуемое значение.

Значение по умолчанию: `Recommended`

UseIChecker

Включает или отключает использование технологии iChecker.

Доступные значения:

`Yes` – включить использование технологии iChecker;

`No` – отключить использование технологии iChecker.

Значение по умолчанию: `Yes`

ScanByAccessType

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

Доступные значения:

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

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

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

Значение по умолчанию: `SmartCheck`

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

AreaDesc

Описание области проверки; содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.

Значение по умолчанию: `All objects`

Пример:

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

UseScanArea

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

Доступные значения:

`Yes` – проверять указанную область;

`No` – не проверять указанную область.

Значение по умолчанию: `Yes`

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

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

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

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

Пример:

```
AreaMask=*doc
```

Путь

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

Значение параметра `Path` состоит из двух элементов: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

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

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

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

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

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

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

AreaDesc

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

Значение по умолчанию не задано.

Пример:

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

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`

Путь

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

Значение параметра `Path` состоит из двух элементов: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

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

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

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

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

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

Формирование глобальной области исключения

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

Чтобы создать глобальную область исключения, выполните следующие действия:

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

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

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

   - AreaMask – маски имени файла для файлов, которые требуется исключить из области защиты.
   - AreaDesc – описание области исключений, содержащее дополнительную информацию об области исключения.
   - Path – путь к файлам или директориям, которые требуется 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>
   ```

Управлять исключенными областями можно также из командной строки.

Задача антивирусной проверки (Scan_My_Computer ID:2)

В этом разделе содержится информация о задаче антивирусной проверки.

Об антивирусной проверке

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

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

Пользователи могут создавать пользовательские задачи антивирусной проверки.

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

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

Параметры задачи антивирусной проверки

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

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

ScanArchived

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

Доступные значения:

`Yes` – проверять архивы; Если указано значение `FirstAction=Recommended`, программа удаляет архив, содержащий угрозу.

`No` – не проверять архивы.

Значение по умолчанию: `Yes`

ScanSfxArchived

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

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы;

`No` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `Yes`

ScanMailBases

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

Доступные значения:

`Yes` – проверять файлы почтовых баз;

`No` – не проверять файлы почтовых баз.

Значение по умолчанию: `No`

ScanPlainMail

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ScanPriority

Приоритет задачи. Приоритет задачи проверки – это параметр, сочетающий несколько внутренних параметров Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.

Доступные значения:

`Idle` – запустить задачу проверки с низким приоритетом. Выберите это значение, чтобы выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени.

`Normal` – запустить задачу проверки со стандартным приоритетом. Выберите это значение, чтобы текущая задача выполнялась быстрее.

Значение по умолчанию: `Idle`

SizeLimit

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

Доступные значения:

`0` – `999,999`

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

Значение по умолчанию: `0`

FirstAction

Выбор первого действия Kaspersky Endpoint Security 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 `Удалить`, программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.

Доступные значения:

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

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

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

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

Значение по умолчанию: `Recommended`

SecondAction

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

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

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

Значение по умолчанию: `Skip`

UseExcludeMasks

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeMasks

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

Значение по умолчанию не задано.

Пример:

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

UseExcludeThreats

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeThreats

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

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

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

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии. Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

```
UseExcludeThreats=Yes

ExcludeThreats.item_0000=EICAR-Test-*

ExcludeThreats.item_0001=?rojan.Linux
```

ReportCleanObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportPackedObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

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

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

Значение по умолчанию: `No`

UseAnalyzer

Включает или отключает эвристический анализатор.

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

Доступные значения:

`Yes` – включить эвристический анализатор;

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`

HeuristicLevel

Уровень эвристического анализа.

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

Доступные значения:

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

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

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

`Recommended` – рекомендуемое значение.

Значение по умолчанию: `Recommended`

UseIChecker

Включает или отключает использование технологии iChecker.

Доступные значения:

`Yes` – включить использование технологии iChecker;

`No` – отключить использование технологии iChecker.

Значение по умолчанию: `Yes`

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

AreaDesc

Описание области проверки; содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.

Значение по умолчанию: `All objects`

Пример:

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

UseScanArea

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

Доступные значения:

`Yes` – проверять указанную область;

`No` – не проверять указанную область.

Значение по умолчанию: `Yes`

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

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

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

Значение по умолчанию: * (проверять все объекты)

Пример:

```
AreaMask_<номер элемента>=*.doc
```

Путь

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

Значение параметра `Path` состоит из двух элементов: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

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

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

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

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

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

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

AreaDesc

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

Значение по умолчанию не задано.

Пример:

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

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`

Путь

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

Значение параметра `Path` состоит из двух элементов: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

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

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

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

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

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

Задача выборочной проверки (Scan_File ID:3)

В этом разделе содержится информация о задаче выборочной проверки.

О задаче выборочной проверки

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

Вы можете проверить файл или директорию с помощью следующей команды:

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

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

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

Настройка параметров задачи выборочной проверки

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

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

ScanArchived

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

Доступные значения:

`Yes` – проверять архивы; Если указано значение `FirstAction=Recommended`, программа удаляет архив, содержащий угрозу.

`No` – не проверять архивы.

Значение по умолчанию: `Yes`

ScanSfxArchived

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

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы;

`No` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `Yes`

ScanMailBases

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

Доступные значения:

`Yes` – проверять файлы почтовых баз;

`No` – не проверять файлы почтовых баз.

Значение по умолчанию: `No`

ScanPlainMail

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ScanPriority

Приоритет задачи. Приоритет задачи проверки – это параметр, сочетающий несколько внутренних параметров Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.

Доступные значения:

`Idle` – запустить задачу проверки с низким приоритетом. Выберите это значение, чтобы выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени.

`Normal` – запустить задачу проверки со стандартным приоритетом. Выберите это значение, чтобы текущая задача выполнялась быстрее.

Значение по умолчанию: `Normal`

SizeLimit

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

Доступные значения:

`0 – 999,999`

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

Значение по умолчанию: `0`

TimeLimit

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

Доступные значения:

`0 – 9999`

`0` – продолжительность проверки объектов не ограничена.

Значение по умолчанию: `0`

FirstAction

Выбор первого действия Kaspersky Endpoint Security 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 `Удалить`, программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.

Доступные значения:

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

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

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

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

Значение по умолчанию: `Recommended`

SecondAction

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

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

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

Значение по умолчанию: `Skip`

UseExcludeMasks

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeMasks

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

Значение по умолчанию не задано.

Пример:

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

UseExcludeThreats

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeThreats

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

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

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

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии. Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

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

ReportCleanObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportPackedObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

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

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

Значение по умолчанию: `No`

UseAnalyzer

Включает или отключает эвристический анализатор.

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

Доступные значения:

`Yes` – включить эвристический анализатор;

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`

HeuristicLevel

Уровень эвристического анализа.

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

Доступные значения:

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

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

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

`Recommended` – рекомендуемое значение.

Значение по умолчанию: `Recommended`

UseIChecker

Включает или отключает использование технологии iChecker.

Доступные значения:

`Yes` – включить использование технологии iChecker;

`No` – отключить использование технологии iChecker.

Значение по умолчанию: `Yes`

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

AreaDesc

Описание области проверки; содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.

Значение по умолчанию: `Все объекты`.

Пример:

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

UseScanArea

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

Доступные значения:

`Yes` – проверять указанную область;

`No` – не проверять указанную область.

Значение по умолчанию: `Yes`

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

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

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

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

Пример:

```
AreaMask=*doc
```

Путь

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

Значение параметра `Path` состоит из двух элементов: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

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

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

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

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

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

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

AreaDesc

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

Значение по умолчанию не задано.

Пример:

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

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`

Путь

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

Значение параметра `Path` состоит из двух элементов: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

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

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

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

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

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

Задача проверки загрузочных секторов (Boot_Scan ID:4)

В этом разделе содержится информация о задаче проверки загрузочных секторов.

О задаче проверки загрузочных секторов

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

Параметры задачи проверки загрузочных секторов

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

Описаны все доступные значения и значения по умолчанию для каждого параметра. Можно изменить значения параметра во время выполнения задачи из командной строки.

Действие

Выбор действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

`Disinfect` – Kaspersky Endpoint Security пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным.

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

Значение по умолчанию: `Disinfect`

UseExcludeMasks

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeMasks.item_#

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

Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks` (`UseExcludeMasks=Yes`).

Значение по умолчанию не задано.

UseExcludeThreats

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeThreats.item_#

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

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

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

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

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

ReportCleanObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportUnprocessedObjects

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

Доступные значения:

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

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

Значение по умолчанию: `No`

UseAnalyzer

Включает или отключает эвристический анализатор.

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

Доступные значения:

`Yes` – включить эвристический анализатор;

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`

HeuristicLevel

Уровень эвристического анализа.

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

Доступные значения:

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

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

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

`Recommended` – рекомендуемое значение.

Значение по умолчанию: `Recommended`

DeviceNameMasks.item_#

Список масок имен проверяемых устройств.

Необходимо указать хотя бы одну маску имени устройства. Значение этого параметра не должно быть пустым.

Доступные значения:

`AllObjects` – проверять все устройства.

`<Маска имени устройства>` – проверять устройства, имена которых содержат указанную маску.

Значение по умолчанию: `/**` – любой набор символов в имени маски устройства, включая символ `/`.

Задача проверки памяти процессов (Memory_Scan ID:5)

В этом разделе содержится информация о задаче проверки памяти процессов.

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

Ниже перечислены параметры, которые вы можете указать для задачи проверки памяти процессов.

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

UseExcludeThreats

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeThreats

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

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

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

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии. Чтобы найти название угрозы, введите название программы в поле Поиск.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

ReportCleanObjects

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

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportUnprocessedObjects

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

Доступные значения:

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

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

Значение по умолчанию: `No`

Действие

Выбор действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

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

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

Значение по умолчанию: `Disinfect`

Задача обновления (Update ID:6)

В этом разделе содержится информация о задаче обновления.

Об обновлении баз и модулей программы

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Об источниках обновлений

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

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

Если по каким-то причинам вы не можете использовать в качестве источника обновлений серверы обновлений "Лаборатории Касперского", можно получать обновления из *пользовательского источника обновлений* – из указанной локальной или сетевой директории (SMB/NFS), смонтированной пользователем, или с FTP- или HTTP-сервера. Вы можете указать пользовательский источник обновлений в конфигурационном файле задачи обновления.

Параметры задач обновления

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

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

SourceType

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

Доступные значения:

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

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

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

Значение по умолчанию: `KLServers`

UseKLServersWhenUnavailable

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

Доступные значения:

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

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

Значение по умолчанию: `Yes`

IgnoreProxySettingsForKLServers

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

Доступные значения:

`Yes` – Kaspersky Endpoint Security не использует прокси-сервер для подключения к серверам обновлений "Лаборатории Касперского".

`No` – Kaspersky Endpoint Security использует прокси-сервер для подключения к серверам обновлений "Лаборатории Касперского".

Значение по умолчанию: `No`

IgnoreProxySettingsForCustomSources

С помощью этого параметра вы можете настроить использование прокси-сервера для соединения с пользовательскими источниками обновлений. Вам нужно включить этот параметр, если для соединения с каким-либо из пользовательских HTTP-серверов обновлений требуется доступ к прокси-серверу.

Доступные значения:

`Yes` – Kaspersky Endpoint Security не использует прокси-сервер для подключения к пользовательским источникам обновлений.

`No` – Kaspersky Endpoint Security использует прокси-сервер для подключения к пользовательским источникам обновлений.

Значение по умолчанию: `No`

ApplicationUpdateMode

Отображает режим загрузки и установки обновлений программы.

Доступные значения:

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

`DownloadOnly` – загружать обновления программы, но не устанавливать их.

`DownloadAndInstall` – автоматически загружать и устанавливать обновления программы.

Значение по умолчанию: `DownloadOnly`

ConnectionTimeout

С помощью этого параметра вы можете указать время ожидания (в секундах) ответа от источника обновлений – HTTP-сервера при соединении с ним. Если в течение указанного промежутка времени от источника обновлений не приходит ответ, Kaspersky Endpoint Security обращается к другому указанному источнику обновлений.

Вы можете указывать только целые числа в диапазоне от 0 до 120.

Значение по умолчанию: `10`

Блок `[CustomSources.item_#]` содержит следующие параметры:

URL

С помощью этого параметра вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.

Значение по умолчанию не задано.

Пример:

```
URL=http://example.com/bases/ – адрес HTTP-сервера, на котором помещается директория с обновлениями.

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

Enabled

С помощью этого параметра вы можете включить или отключить использование источника обновлений, указанного в параметре `URL`. Для выполнения задачи необходимо, чтобы использование хотя бы одного источника обновлений было включено.

Доступные значения:

`Yes` – Kaspersky Endpoint Security использует источник обновлений.

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

Значение по умолчанию не задано.

Пример:

```
Enabled=Yes
```

Установка обновления программы вручную

Вы можете вручную установить обновление программы из командной строки. Для установки обновления на вашем компьютере должен быть установлен Kaspersky Endpoint Security. Для обновления программы Kaspersky Endpoint Security необходимо остановить ее работу. Если процесс обновления завершается с ошибкой, Kaspersky Endpoint Security автоматически откатывает обновления до предыдущей версии.

Патчи программы можно устанавливать непоследовательно (только для Kaspersky Endpoint Security Service Pack 1 и выше).

Чтобы установить обновление Kaspersky Endpoint Security из пакета формата RPM, выполните следующую команду:

```
# rpm –U <имя пакета в формате rpm>.rpm
```

Чтобы установить пакет формата RPM для Kaspersky Endpoint Security той же версии, выполните следующую команду:

```
# rpm –U --replacefiles --replacepkgs <имя пакета в формате rpm>.rpm
```

Чтобы установить обновление Kaspersky Endpoint Security из пакета формата DEB, выполните следующую команду:

```
# dpkg -i <имя пакета в формате deb>.deb
```

Запустится процесс обновления программы.

Может потребоваться перезагрузка программы или операционной системы. Отобразится соответствующее сообщение. После перезапуска программы или операционной системы запускается обновленная версия Kaspersky Endpoint Security.

После обновления программы необходимо принять Лицензионное соглашение, Политику конфиденциальности и Положение о Kaspersky Security Network, если эти документы были изменены "Лабораторией Касперского". Отобразится соответствующее сообщение.

Чтобы принять Лицензионное соглашение, Политику Конфиденциальности или Положение о Kaspersky Security Network,

1. Прочитайте текст Лицензионного соглашения (/opt/kaspersky/kesl/doc/license.<ID языка>).

   Если вы согласны с текстом Лицензионного соглашения, укажите переменную среды, выполнив следующую команду:

   - `# KESL_EULA_AGREED=yes rpm -U <имя пакета в формате rpm>.rpm` для пакета в формате rpm.
   - `# KESL_EULA_AGREED=yes dpkg -i <имя пакета в формате deb>.deb` для пакета в формате deb.

2. Прочитайте текст Политики Конфиденциальности (/opt/kaspersky/kesl/doc/license.<ID языка>).

   Если вы согласны с текстом Политики Конфиденциальности, укажите переменную среды, выполнив следующую команду:

   - `# KESL_PRIVACY_POLICY_AGREED=yes rpm -U <имя пакета в формате rpm>.rpm` для пакета в формате rpm.
   - `# KESL_PRIVACY_POLICY_AGREED=yes dpkg -i <имя пакета в формате deb>.deb` для пакета в формате deb.

3. Прочитайте текст Положения о Kaspersky Security Network (/opt/kaspersky/kesl/doc/ksn_license.<ID языка>).

   Если вы согласны с текстом Положения о Kaspersky Security Network, укажите переменную среды:

   - `# KESL_USE_KSN=yes rpm -U <имя пакета в формате rpm>.rpm` для пакета в формате rpm.
   - `# KESL_USE_KSN=yes dpkg -i <имя пакета в формате deb>.deb` для пакета в формате deb.

Если вы не согласны с текстом Положения о Kaspersky Security Network, укажите переменную среды:

- `# KESL_USE_KSN=no rpm -U <имя пакета в формате rpm>.rpm` для пакета в формате rpm.
- `# KESL_USE_KSN=no dpkg -i <имя пакета в формате deb>.deb` для пакета в формате deb.

Отказ от участия в Kaspersky Security Network не прерывает процесс обновления Kaspersky Endpoint Security. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент.

4. Перезапустите установку программы.

Если вы не согласны с положениями Лицензионного соглашения и Политики конфиденциальности, процесс обновления программы будет прерван.

Задача Откат обновления баз (Rollback ID:7)

В этом разделе содержится информация о задаче отката обновлений.

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

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

Задача Откат обновления баз не имеет параметров.

Задача Лицензия (License ID:9)

В этом разделе содержится информация о задаче Лицензия.

О задаче Лицензия

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

Добавление активного ключа

Команда `kesl-control --install-active-key` добавляет активный ключ. Подробнее о ключах см. в разделе "О ключе".

Синтаксис команды

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

Аргументы и ключи

`<путь к файлу ключа>`

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

`<код активации>`

Код активации используется для добавления лицензионного ключа для активации программы.

Пример:

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

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

Добавление дополнительного ключа или кода активации

Команда `kesl-control --install-additional-key` добавляет дополнительный ключ. Подробнее о ключах см. в разделе "О ключе".

Если активный ключ не установлен, то дополнительный ключ будет установлен как основной.

Синтаксис команды

```
kesl-control [-L] --install-additional-key <путь к файлу ключа>|<код
активации>
```

Аргументы и ключи

`<путь к файлу ключа>`

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

`<код активации>`

Код активации используется для добавления лицензионного ключа для активации программы.

Пример:

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

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

Удаление активного ключа

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

Синтаксис команды

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

Удаление дополнительного ключа

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

Синтаксис команды

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

Задача управления Хранилищем (Backup ID:10)

В этом разделе содержится информация о задаче Управление Хранилищем.

О Хранилище

Хранилище – это список резервных копий файлов, которые были удалены или изменены в процессе лечения. Резервная копия – копия файла, которая создается при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности. Резервные копии могут содержать персональные данные. По умолчанию Хранилище расположено в директории /var/opt/kaspersky/kesl/common/objects-backup/.

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

Параметры задачи Управление Хранилищем

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

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

DaysToLive

Интервал времени, в течение которого объекты хранятся в хранилище (в сутках).

Чтобы снять ограничение для времени хранения объектов в хранилище, укажите значение 0.

Значение по умолчанию: 90.

BackupSizeLimit

Максимальный размер хранилища.

При достижении максимального размера хранилища, Kaspersky Endpoint Security удаляет самые старые объекты.

Доступные значения:

0 – 999,999 (в мегабайтах).

Чтобы снять ограничение для размера хранилища, укажите значение 0.

Значение по умолчанию: `0`.

BackupFolder

Путь к директории хранилища. Можно 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 Kaspersky Endpoint Security.

Если указанная директория не существует или недоступна, Kaspersky Endpoint Security использует директорию хранилища, 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, Kaspersky Endpoint Security присваивает ему числовой идентификатор. Идентификатор используется для действий с объектом, например, при восстановлении или удалении объекта из хранилища.

Чтобы просмотреть идентификаторы объектов в хранилище, выполните следующую команду:

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

Идентификатор объекта будет выведен в строке `ObjectId`.

О восстановлении объектов из Хранилища

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

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

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

Восстановление зараженных объектов может привести к заражению компьютера.

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

Восстановление объектов из Хранилища

Чтобы восстановить объект из хранилища, выполните следующие действия:

- Чтобы восстановить объект с исходным именем и в исходное местоположение, выполните команду:
  ```
  kesl-control --restore <ID объекта>
  ```
  где `ID объекта` – это идентификатор объекта в хранилище.
- Чтобы восстановить объект с новым именем в указанную директорию, выполните команду:
  ```
  [-B] --restore <ID объекта> --file <имя и директория файла>
  ```

Если указанная директория не существует, Kaspersky Endpoint Security создает ее.

Удаление объектов из Хранилища

Чтобы удалить 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><оператор сравнения>
'<значение>' [и <поле> <оператор сравнения>'<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
```

Задача Контроль целостности системы (System_Integrity_Monitoring ID:11)

В этом разделе содержится информация о задаче Контроль целостности системы.

О Контроле целостности системы

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

Для использования функции контроля целостности системы необходимо приобрести лицензию, которая включает эту функцию. По умолчанию контроль целостности системы выключен.

Контроль целостности системы может выполняться в режиме реального времени при запуске задачи *Контроль целостности системы при доступе* (OAFIM). Кроме этого можно создавать и запускать задачи *Контроль целостности системы по требованию* (ODFIM).

Оба типа задачи отправляют уведомления об изменениях в списках контроля доступа к объектам. В случае задачи OAFIM в отчет не включаются данные о том, какие именно изменения внесены. В случае задачи ODFIM в отчет включаются данные об измененных атрибутах и перемещенных файлах и директориях.

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 Kaspersky Endpoint Security отправляет событие на Сервер администрирования Kaspersky Security Center. Во время работы задачи контрольная сумма файла не рассчитывается. Задача OAFIM не отслеживает изменения файлов (атрибутов и содержимого) с жесткими ссылками, которые расположены вне области мониторинга.

Kaspersky Endpoint Security отслеживает операции с конкретными файлами или в областях, указанных в параметрах задачи.

Области мониторинга

Области мониторинга для задачи Контроль целостности системы всегда должны быть указаны. Администратор может изменять области проверки и мониторинга в режиме реального времени. Если область мониторинга не указана, параметры задачи невозможно сохранить в конфигурационном файле. При добавлении области мониторинга или области исключения программа не проверяет, существует ли такая директория.

Вы можете указать несколько областей мониторинга.

Исключения из области мониторинга

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

Исключения имеют более высокий приоритет, чем область мониторинга, и не проверяются задачей, даже если указанная 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.

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 компоненту 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*.

Вы можете создать несколько задач ODFIM.

Снимок состояния системы

Снимок состояния системы определяется во время первого выполнения задачи ODFIM на компьютере. 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, Kaspersky Endpoint Security создает событие о нарушении целостности системы. Снимок состояния системы содержит пути к контролируемым объектам и их метаданные.

Вы можете заново создать снимок состояния системы для задачи с помощью соответствующего параметра. Снимок состояния системы создается заново после завершения задачи ODFIM.

Снимок состояния системы также создается при изменении параметров задачи, например, при добавлении новой области мониторинга. При следующем выполнении задачи снимок состояния системы формируется заново.

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.

Удалить снимок состояния системы можно, удалив соответствующую задачу ODFIM.

Параметры задачи Контроль целостности системы при доступе

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Контроль целостности системы при доступе.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

UseExcludeMasks

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

Параметр `UseExcludeMasks` работает, только если указано значение параметра `ExcludeMasks`.

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeMasks

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

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

Маски указываются в формате командной оболочки.

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

Значение по умолчанию: не задано

Раздел [ScanScope.item_#]

В разделе `[ScanScope.item_#]` указываются области мониторинга для задачи Контроль целостности системы. Для задачи должна быть указана минимум одна область мониторинга.

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

Каждый раздел `[ScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области мониторинга.

UseScanArea

Включает или выключает мониторинг указанной области.

Доступные значения:

`Yes` – контролировать указанную область;

`No` – не контролировать указанную область.

Значение по умолчанию: `Yes`

Path

Указывает полный путь к объекту или директориям для мониторинга.

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

AreaMask.item_#

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

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

Значение по умолчанию: `*` (обрабатываются все объекты)

Раздел [ExcludedFromScanScope.item_#]

В разделах `[ExcludedFromScanScope.item_#]` укажите объекты, которые требуется исключить из всех разделов `[ScanScope.item_#]`.

Объекты, удовлетворяющие правилам любого из разделов `[ExcludedFromScanScope.item_#]`, будут исключены из мониторинга. Формат раздела `[ExcludedFromScanScope.item_#]` аналогичен формату раздела `[ScanScope.item_#]`.

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

Каждый раздел `[ScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области, которую нужно исключить из мониторинга.

UseScanArea

Указывает, будут ли указанные области исключены из мониторинга.

Доступные значения:

`Yes` – исключать указанные области из мониторинга;

`No` – не исключать указанные области из мониторинга.

Значение по умолчанию: `Yes`

Path

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

AreaMask.item_#

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

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

Значение по умолчанию: `*` (выполняется мониторинг всех объектов)

Параметры задачи Контроль целостности системы по требованию

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

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

RebuildBaseline

Включает или отключает повторное создание снимка состояния системы после завершения задачи ODFIM.

Доступные значения:

`Yes` – создавать снимок состояния системы повторно после завершения задачи ODFIM.

`No` – не создавать снимок состояния системы повторно после завершения задачи ODFIM.

Значение по умолчанию: `No`

CheckFileHash

Включает или выключает проверку хеша (SHA-256).

Доступные значения:

`Yes` – включить проверку хеша;

`No` – выключить проверку хеша.

Значение по умолчанию: `No`

TrackDirectoryChanges

Включает или выключает мониторинг директорий.

Доступные значения:

`Yes` – контролировать директории;

`No` – не контролировать директории.

Значение по умолчанию: `No`

TrackLastAccessTime

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

Доступные значения:

`Yes` – проверять время последнего доступа к файлу;

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

Значение по умолчанию: `No`

UseExcludeMasks

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

Этот параметр работает, только если указано значение параметра `ExcludeMasks`.

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeMasks

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

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

Маски указываются в формате командной оболочки.

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

Значение по умолчанию: не задано

Раздел [ScanScope.item_#]

В разделе `[ScanScope.item_#]` указываются области мониторинга для задачи Контроль целостности системы. Для задачи должна быть указана минимум одна область мониторинга.

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

Каждый раздел `[ScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области мониторинга.

UseScanArea

Включает или выключает мониторинг указанной области.

Доступные значения:

`Yes` – контролировать указанную область;

`No` – не контролировать указанную область.

Значение по умолчанию: `Yes`

Path

Указывает полный путь к объекту или директориям для мониторинга.

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

AreaMask.item_#

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

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

Значение по умолчанию: `*` (обрабатываются все объекты)

Раздел [ExcludedFromScanScope.item_#]

В разделах `[ExcludedFromScanScope.item_#]` укажите объекты, которые требуется исключить из всех разделов `[ScanScope.item_#]`.

Объекты, удовлетворяющие правилам любого из разделов `[ExcludedFromScanScope.item_#]`, будут исключены из мониторинга. Формат раздела `[ExcludedFromScanScope.item_#]` аналогичен формату раздела `[ScanScope.item_#]`.

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

Каждый раздел `[ScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области, которую нужно исключить из мониторинга.

UseScanArea

Указывает, будут ли указанные области исключены из мониторинга.

Доступные значения:

`Yes` – исключать указанные области из мониторинга;

`No` – не исключать указанные области из мониторинга.

Значение по умолчанию: `Yes`

Path

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

AreaMask.item_#

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

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

Значение по умолчанию: `*` (выполняется мониторинг всех объектов).

Задача управления сетевым экраном (Firewall ID:12)

В этом разделе содержится информация о задаче Управление сетевым экраном.

Об Управлении сетевым экраном

Во время работы в локальных сетях и интернете компьютер подвержен не только заражению вирусами и другими вредоносными программами, но и различного рода атакам, использующим уязвимости операционных систем и программного обеспечения.

Сетевой экран операционной системы защищает персональные данные, которые хранятся на компьютере пользователя. Сетевой экран блокирует большую часть потенциальных угроз для операционной системы, когда компьютер подключен к интернету или локальной сети. Управление сетевым экраном позволяет обнаружить все сетевые соединения на компьютере пользователя и предоставить список их IP-адресов с указанием статуса сетевого соединения по умолчанию.

Компонент Управление сетевым экраном фильтрует всю сетевую активность в соответствии с сетевыми пакетными правилами. Настройка сетевых пакетных правил позволяет вам задать нужный уровень защиты компьютера, от полной блокировки доступа в интернет для всех программ до разрешения неограниченного доступа.

Во время работы задачи Управление сетевым экраном Kaspersky Endpoint Security управляет параметрами и правилами сетевого экрана операционной системы. Программа блокирует любую настройку параметров сетевого экрана операционной системы, когда, например, программа или инструмент добавляют или удаляют какое-то правило. Kaspersky Endpoint Security проверяет сетевой экран операционной системы каждые 60 секунд и при необходимости восстанавливает набор правил сетевого экрана. Периодичность проверки изменить невозможно.

> В операционных системах Red Hat Enterprise Linux и CentOS 8 правила сетевого экрана, созданные с помощью Kaspersky Endpoint Security, можно просмотреть только с помощью Kaspersky Endpoint Security (команда `kesl-control -F --query`).

Проверка сетевого экрана операционной системы по-прежнему выполняется, когда задача Управление сетевым экраном остановлена. Это позволяет программе восстанавливать динамические правила.

Все исходящие соединения разрешены по умолчанию (параметр действия по умолчанию) за исключением случаев, когда указаны соответствующие запрещающие правила задачи Управление сетевым экраном. Действие по умолчанию выполняется с самым низким приоритетом: если не сработало никакое другое сетевое пакетное правило или другие сетевые пакетные правила не указаны, соединение разрешается.

> Перед включением задачи Управление сетевым экраном мы рекомендуем отключить другие средства управления сетевым экраном операционной системы.

О сетевых пакетных правилах

Сетевое пакетное правило представляет собой разрешающее или запрещающее действие, которое совершает задача Управление сетевым экраном, обнаружив попытку сетевого соединения.

Используются для ввода ограничений на сетевые пакеты независимо от программы. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных.

Управление сетевым экраном задает по умолчанию некоторые сетевые пакетные правила. Вы можете создавать собственные сетевые пакетные правила и указывать приоритетность выполнения для каждого сетевого пакетного правила.

О динамических правилах

Компоненты Kaspersky Endpoint Security позволяют добавлять и удалять *динамические правила*, необходимые для правильной работы, в сетевой экран. Например, Агент администрирования добавляет динамические правила, которые разрешают соединение с Kaspersky Security Center, инициируемые как программой, так и Kaspersky Security Center. Таким образом, правила задачи Защита от шифрования являются динамическими.

Задача Управление сетевым экраном не контролирует динамические правила и не блокирует доступ к сетевым ресурсам для компонентов программы. Динамические правила не зависят от состояния задачи Управление сетевым экраном (запущена / остановлена) или от изменения параметров этой задачи. Приоритет выполнения динамических правил выше приоритета сетевых пакетных правил. Kaspersky Endpoint Security восстанавливает набор динамических правил, если какие-либо из них были удалены, например, с помощью утилиты iptables.

Вы можете просмотреть набор динамических правил (с помощью команды `kesl-control -F --query`), но не можете изменить параметры динамических правил.

О предустановленных именах сетевых зон

Заданная сетевая зона представляет собой конкретную группу IP-адресов или подсетей. С помощью заданной сетевой зоны вы можете использовать одно и то же правило для нескольких IP-адресов или подсетей, не создавая отдельное правило для каждого IP-адреса или подсети. Сетевую зону можно использовать в качестве значения для параметра `--remote`. В Kaspersky Endpoint Security есть три заданные сетевые зоны с конкретными именами:

- **Публичные**. Добавьте сетевой адрес или подсеть в эту зону, если они назначены сетям, не защищенным антивирусной программой, брандмауэром или фильтрами (таким как сети интернет-кафе).

- **Локальные**. Добавьте сетевой адрес или подсеть в эту зону, если они назначены сетям, у пользователей которых есть право доступа к файлам и принтерам на этом компьютере (таким как локальные или домашние сети).

- **Доверенные**. Эта зона предназначена для безопасных сетей, в которых компьютеры не подвержены атакам или несанкционированным попыткам доступа к данным.

Вы не можете создать или удалить сетевую зону. Вы можете добавлять IP-адреса и подсети в сетевую зону и удалять их из нее.

Параметры задачи Управление сетевым экраном

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Управление сетевым экраном.

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

DefaultIncomingAction

Действие по умолчанию, применяемое к входящему соединению, если другие сетевые правила не применяются к этому виду соединения.

Доступные значения:

`Allow` – разрешать входящие соединения;

`Block` – запрещать входящие соединения.

Значение по умолчанию: `Allow`

DefaultIncomingPacketAction

Действие по умолчанию, применяемое к входящему пакету, если другие сетевые пакетные правила не применяются к этому виду соединения.

Доступные значения:

`Allow` – разрешать входящие пакеты;

`Block` – запрещать входящие пакеты.

Значение по умолчанию: `Allow`

Раздел [PacketRules.item_#]

В разделе `[PacketRules.item_#]` указываются сетевые пакетные правила для задачи Управление сетевым экраном.

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

Каждый раздел `[PacketRules.item_#]` содержит следующие параметры:

Name

Имя сетевого пакетного правила.

Значение по умолчанию: `Packet rule #<n>`, где `n` – это индекс.

FirewallAction

Действие, применяемое к соединениям, указанным в сетевом пакетном правиле.

Доступные значения:

`Allow` – разрешать сетевые соединения;

`Block` – запрещать сетевые соединения.

Значение по умолчанию: `Allow`

Protocol

Тип протокола, для которого необходим мониторинг сетевой активности.

Доступные значения:

`Any` – задача Управление сетевым экраном контролирует всю сетевую активность.

`TCP`

`UDP`

`ICMP`

`ICMPv6`

`IGMP`

`GRE`

Значение по умолчанию: `Any`

RemotePorts

Номера портов удаленных компьютеров, соединение между которыми отслеживается.

Этот параметр можно указать, только если для параметра `Protocol` установлено значение `TCP` или `UDP`.

Для этого параметра можно указать значение в виде целого числа или интервала.

Доступные значения:

`Any` – контролировать все удаленные порты.

`0 – 65535`.

Значение по умолчанию: `Any`

LocalPorts

Номера портов локальных компьютеров, соединение между которыми отслеживается.

Этот параметр можно указать, только если для параметра `Protocol` установлено значение `TCP` или `UDP`.

Для этого параметра можно указать значение в виде целого числа или интервала.

Доступные значения:

`Any` – контролировать все локальные порты.

`0 – 65535`.

Значение по умолчанию: `Any`

ICMPType

Тип пакета ICMP.

Этот параметр можно указать, только если для параметра `Protocol` установлено значение `ICMP` или `ICMPv6`.

Доступные значения:

`Any` – контролировать все типы пакетов ICMP.

Целое число согласно спецификации протокола передачи данных.

Значение по умолчанию: `Any`

ICMPCode

Код пакета ICMP.

Этот параметр можно указать, только если для параметра `Protocol` установлено значение `ICMP` или `ICMPv6`.

Доступные значения:

`Any` – контролировать все коды пакетов ICMP.

Целое число согласно спецификации протокола передачи данных.

Значение по умолчанию: `Any`

Direction

Направление отслеживаемой сетевой активности.

Доступные значения:

`IncomingOutgoing` или `InOut` – контролировать как входящие, так и исходящие соединения.

`Incoming` или `In` – контролировать входящие соединения.

`Outgoing` или `Out` – контролировать исходящие соединения.

`IncomingPacket` или `InPacket` – контролировать входящие пакеты.

`OutgoingPacket` или `OutPacket` – контролировать исходящие пакеты.

`IncomingOutgoingPacket` или `InOutPacket` – контролировать как входящие, так и исходящие пакеты.

Значение по умолчанию: `IncomingOutgoing` или `InOut`

RemoteAddress

Сетевые адреса удаленных компьютеров, которые могут передавать и получать сетевые пакеты.

Доступные значения:

`Any` – контролируется отправка и / или получение сетевых пакетов удаленными компьютерами с любым IP-адресом.

`Trusted` – заданная сетевая зона для доверенных сетей.

`Local` – заданная сетевая зона для локальных сетей.

`Public` – заданная сетевая зона для публичных сетей.

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

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

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

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

Значение по умолчанию: `Any`

LocalAddress

Сетевые адреса компьютеров с установленной программой Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты.

Доступные значения:

`Any` – контролируется отправка и / или получение сетевых пакетов удаленными компьютерами с любым IP-адресом.

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

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

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

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

Значение по умолчанию: `Any`

LogAttempts

Указывает, следует ли включать в отчет действия сетевого правила.

Доступные значения:

`Yes` – отражать действия в отчете.

`No` – не отражать действия в отчете.

Значение по умолчанию: `No`

Раздел [NetworkZonesPublic]

В разделе `[NetworkZonesPublic]` указываются сетевые адреса, связанные с публичными сетями.

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

Address.item_#

Доступные значения:

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

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

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

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

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

Раздел [NetworkZonesLocal]

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

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

Address.item_#

Доступные значения:

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

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

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

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

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

Раздел [NetworkZonesTrusted]

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

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

Address.item_#

Доступные значения:

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

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

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

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

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

Добавление сетевого пакетного правила

Вы можете добавить сетевое пакетное правило вручную.

Сетевые пакетные правила можно добавлять только по одному.

Чтобы добавить сетевое пакетное правило, выполните следующую команду:

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

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

Параметр `--at` позволяет указать индекс создаваемого правила в списке сетевых пакетных правил. Если параметр `--at` не указан или его значение больше числа правил в списке, новое правило добавляется в конец списка.

Примеры:

Чтобы создать правило, блокирующее все входящие и создаваемые соединения по протоколу TCP через порт 23, выполните следующую команду:

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in
--protocol TCP --local any:23

--remote any
```

Чтобы создать правило, блокирующее входящие и создаваемые соединения по протоколу TCP через порт 23 для сетевой зоны *Публичные*, выполните следующую команду:

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in
--protocol TCP --local any:23

--remote Public
```

Удаление сетевого пакетного правила

Вы можете удалить сетевое пакетное правило вручную.

Сетевые пакетные правила можно удалять только по одному.

Чтобы удалить сетевое пакетное правило, выполните одну из следующих команд:

- `kesl-control -F --del-rule --name <имя>`

  Сетевое пакетное правило будет удалено по имени. Если список сетевых пакетных правил содержит несколько правил с одинаковым именем, Kaspersky Endpoint Security не удаляет ни одно из них.

- `kesl-control -F --del-rule --index <индекс>`

  Сетевое пакетное правило будет удалено по индексу в списке сетевых пакетных правил.

Из конфигурационного файла задачи Управление сетевым экраном будет удален блок, содержащий параметры сетевого пакетного правила.

Если список сетевых пакетных правил не содержит правило с указанным именем или индексом, происходит ошибка.

Изменение приоритета выполнения сетевого пакетного правила

Вы можете вручную изменить приоритетность выполнения сетевого пакетного правила.

Чтобы изменить приоритетность выполнения сетевого пакетного правила, выполните следующую команду:

```
kesl-control -F --move-rule [--name <имя>|--index <индекс>] --at <индекс>
```

Приоритетность сетевого пакетного правила будет изменена в соответствии с указанным индексом.

Добавление сетевого адреса в блок зоны

Вы можете вручную добавить в конфигурационный файл задачи Управление сетевым экраном сетевые адреса, связанные с определенным типом сети.

Чтобы добавить сетевой адрес в зону, выполните следующую команду:

```
kesl-control -F --add-zone <Public|Local|Trusted> --address <адрес>
```

Сетевой адрес будет добавлен в блок конкретной зоны в конфигурационном файле задачи.

Удаление сетевого адреса из раздела зоны

Вы можете вручную удалить из конфигурационного файла задачи Управление сетевым экраном сетевые адреса, связанные с определенным типом сети. Это может понадобиться, если сетевые адреса больше не используются.

Чтобы удалить сетевой адрес из зоны, выполните следующую команду:

```
kesl-control -F --del-zone <зона> [--address <адрес>| --index <индекс адреса в зоне>]
```

Указанный сетевой адрес будет удален из раздела конкретной зоны в конфигурационном файле.

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

Если указанный сетевой адрес или индекс не существует, отображается сообщение об ошибке.

Задача Защита от шифрования (AntiCryptor ID:13)

В этом разделе содержится информация о задаче Защита от шифрования.

О задаче Защита от шифрования

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

В 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.

Kaspersky Endpoint Security не расценивает действия как шифрование, если обнаруженная активность шифрования имеет место в директориях, исключенных из области задачи Защита от шифрования.

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

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

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

О блокировке доступа к недоверенным компьютерам

При обнаружении вредоносного шифрования Kaspersky Endpoint Security создает и включает правило для сетевого экрана операционной системы, которое блокирует сетевой трафик от скомпрометированного компьютера. Скомпрометированный компьютер добавляется в список недоверенных компьютеров. Kaspersky Endpoint Security блокирует доступ к общим сетевым директориям для всех удаленных компьютеров в списке недоверенных компьютеров. Информация обо всех заблокированных компьютерах защищаемого сервера отправляется в Kaspersky Security Center.

Правила сетевого экрана, созданные задачей Защита от шифрования, нельзя удалить с помощью утилиты iptables: Kaspersky Endpoint Security восстанавливает набор правил каждую минуту. Используйте команду `--allow-hosts`, чтобы разблокировать компьютер.

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

Параметры задачи Защита от шифрования

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

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

UseHostBlocker

Включает или выключает блокировку недоверенных компьютеров.

Если блокировка недоверенных компьютеров выключена, Kaspersky Endpoint Security 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.

Доступные значения:

`Yes` – включить блокировку недоверенных компьютеров.

`No` – выключить блокировку недоверенных компьютеров.

Значение по умолчанию: `Yes`

BlockTime

Указывает 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.

Доступные значения:

Целое значение от `1` до `4294967295`.

Значение по умолчанию: `30`

UseExcludeMasks

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

Этот параметр работает, только если указано значение параметра `ExcludeMasks`.

Доступные значения:

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

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

Значение по умолчанию: `No`

ExcludeMasks

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

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

Маски указываются в формате командной оболочки.

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

Значение по умолчанию: не задано

Раздел [ScanScope.item_#]

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

Для задачи Защита от шифрования можно указывать только общие директории.

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

Каждый раздел `[ScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области защиты.

Значение по умолчанию: `All shared folders`

UseScanArea

Включает или выключает защиту указанной области.

Доступные значения:

`Yes` – защищать указанную область.

`No` – не защищать указанную область.

Значение по умолчанию: `Yes`

Path

Указывает путь к защищаемым объектам.

Доступные значения:

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

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

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

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

Значение по умолчанию: `AllShared`

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты для защиты.

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

Значение по умолчанию: * (обрабатываются все объекты).

Раздел [ExcludedFromScanScope.item_#]

В разделах `[ExcludedFromScanScope.item_#]` укажите объекты, которые требуется исключить из всех разделов `[ScanScope.item_#]`.

Объекты, удовлетворяющие правилам любого из разделов `[ExcludedFromScanScope.item_#]`, не проверяются. Формат раздела `[ExcludedFromScanScope.item_#]` аналогичен формату раздела `[ScanScope.item_#]`.

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

Каждый раздел `[ScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области, которую нужно исключить из проверки.

Значение по умолчанию: `All objects`

UseScanArea

Указывает, будут ли указанные области исключены из защиты.

Доступные значения:

`Yes` – исключать указанную область из защиты.

`No` – не исключать указанную область из защиты.

Значение по умолчанию: `Yes`

Path

Указывает путь к объектам, исключенным из защиты.

Можно указать только абсолютный путь к локальной директории (например, `/root /tmp/123`), которую не требуется защищать компонентом Защита от шифрования.

Для указания пути можно использовать маски.

Значение по умолчанию: не задано

AreaMask.item_#

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

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

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

Просмотр списка заблокированных компьютеров

Вы можете просматривать список недоверенных компьютеров, заблокированных задачей Защита от шифрования.

Чтобы просмотреть список заблокированных компьютеров, выполните следующую команду:

```
kesl-control -H --get-blocked-hosts
```

Будут выведены компьютеры, заблокированные задачей Защита от шифрования.

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 - ::
```

Задача Защита от веб-угроз (Web_Threat_Protection ID: 14)

В этом разделе содержится информация о задаче Защита от веб-угроз.

О задаче Защита от веб-угроз

Во время работы задачи 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.

Kaspersky Endpoint Security проверяет трафик, передаваемый по протоколам HTTP, HTTPS и FTP. Также выполняется проверка веб-сайтов и IP-адресов. Можно указать определенные сетевые порты или диапазоны сетевых портов для проверки.

> Для проверки HTTPS-трафика вам нужно включить проверку защищенных соединений.

> Для проверки FTP-трафика вам нужно указать параметр `MonitorNetworkPorts=All`.

При попытке открытия опасного веб-сайта, Kaspersky Endpoint Security выполняет следующие действия:

- Для HTTP- или FTP-трафика программа блокирует доступ и показывает предупреждение.
- Для HTTPS-трафика в браузере отображается страница с ошибкой.

При открытии веб-сайта задача Защита от веб-угроз выполняет следующие действия:

1. Проверяет надежность веб-сайта с помощью загруженных антивирусных баз.
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.

Задача Защита от веб-угроз запускается по умолчанию при запуске Kaspersky Endpoint Security. При необходимости можно остановить задачу в любой момент.

Параметры задачи Защита от веб-угроз

В этом разделе описаны параметры задачи Защита от веб-угроз. Задача Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета и блокирует доступ к вредоносным, фишинговым, рекламным и прочим опасным веб-сайтам.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

ActionOnDetect

Действия, выполняемые при обнаружении зараженного объекта в веб-трафике.

Доступные значения:

`Notify` – разрешить загрузку обнаруженного объекта, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.

`Block` – запретить доступ к обнаруженному объекту, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.

Значение по умолчанию: `Block`

CheckMalicious

Показывает, выполняется ли проверка ссылок по базе вредоносных веб-адресов.

Доступные значения:

`Yes` – проверять ссылки на вхождение в базу вредоносных веб-адресов.

`No` – не проверять ссылки на вхождение в базу вредоносных веб-адресов.

Значение по умолчанию: `Yes`

CheckPhishing

Показывает, выполняется ли проверка ссылок по базе фишинговых веб-адресов.

Доступные значения:

`Yes` – проверять ссылки на вхождение в базу фишинговых веб-адресов.

`No` – не проверять ссылки на вхождение в базу фишинговых веб-адресов.

Значение по умолчанию: `Yes`

UseHeuristicForPhishing

Показывает, используется ли эвристический анализ для проверки веб-страниц на наличие фишинговых ссылок.

Доступные значения:

`Yes` – 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.

Значение по умолчанию: `Yes`

CheckAdware

Показывает, выполняется ли проверка ссылок по базе рекламных веб-адресов.

Доступные значения:

`Yes` – проверять ссылки на вхождение в базу рекламных веб-адресов.

`No` – не проверять ссылки на вхождение в базу рекламных веб-адресов.

Значение по умолчанию: `No`

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.

Доступные значения:

`Yes` – проверять ссылки на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда компьютеру или персональным данным.

`No` – не проверять ссылки на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда компьютеру или персональным данным.

Значение по умолчанию: `No`

UseTrustedAddresses

Включает или отключает 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_#`.

Доступные значения:

`Yes` – использовать список доверенных веб-адресов.

`No` – не использовать список доверенных веб-адресов.

Значение по умолчанию: `Yes`

TrustedAddresses.item_#

Доверенные веб-адреса. Для указания веб-адресов можно использовать маски.

Задача Контроль устройств (Device_Control ID: 15)

В этом разделе содержится информация о задаче Контроль устройств.

О задаче Контроль устройств

Во время выполнения задачи Контроль устройств программа Kaspersky Endpoint Security управляет доступом пользователей к устройствам, установленным или подключенным к компьютеру (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. Это позволяет защитить компьютер от заражения при подключении таких устройств, а также предотвратить потерю и утечку данных.

Задача Контроль устройств управляет доступом пользователей к устройствам с помощью правил доступа.

Задача Контроль устройств управляет доступом на следующих уровнях:

- **Класс устройства**. Например, принтеры, съемные диски, CD/DVD-приводы.

  Для каждого типа устройств можно указать следующие правила доступа: *Allow*, *Block* или *DependsOnBus*. Если указано значение *DependsOnBus*, доступ к устройству определяется правилом доступа к шине подключения.

- **Шина подключения**. *Шина подключения* – это интерфейс, используемый для подключения устройств к компьютеру (*USB* или *FireWire*).

  Для каждой шины подключения можно указать следующие правила доступа: *Allow* или *Block*. Например, можно разрешить или запретить подключение всех устройств по USB.

- **Доверенные устройства**. *Доверенные устройства* – это устройства, к которым у пользователей есть полный доступ.

  Можно добавить устройства в список доверенных по идентификатору устройства. У каждого устройства есть уникальный идентификатор. Идентификаторы подключенных устройств можно посмотреть, выполнив команду `kesl-control --get-device-list`.

Если устройство, заблокированное задачей Контроль устройств, подключено к компьютеру, Kaspersky Endpoint Security запрещает пользователям доступ к этому устройству и выводит уведомление. Заблокированные устройства отображаются в списке подключенных устройств (**Заблокировано**: **Да**).

Задача Контроль устройств запускается по умолчанию при запуске Kaspersky Endpoint Security. При необходимости можно остановить задачу в любой момент.

О правилах доступа

Правило доступа к устройству – это параметр, определяющий могут ли пользователи получить доступ к устройствам, установленным или подключенным к компьютеру.

По умолчанию, правила доступа создаются для всех классов устройств по классификации компонента Контроль устройств. Такие правила предоставляют пользователям полный доступ к устройствам, если разрешен доступ к шинам подключения для соответствующих типов устройств.

Правило доступа к шине подключения разрешает или запрещает доступ к шине подключения (USB или FireWire).

Можно изменять правила доступа к устройствам и правила доступа к шинам подключения.

Параметры задачи Контроль устройств

В этом разделе описаны параметры задачи Контроль устройств.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

Раздел [DeviceClass]

В разделе `[DeviceClass]` указаны правила доступа к устройствам в зависимости от их типа.

HardDrive

Правила доступа к жестким дискам, подключенным к компьютеру.

Доступные значения:

`Allow` – пользователям разрешен доступ к жестким дискам.

`DependsOnBus` – доступ к жестким дискам зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ ко всем жестким дискам (за исключением системных жестких дисков, которые задача Device Control не блокирует).

Значение по умолчанию: `DependsOnBus`

RemovableDrive

Правила доступа к съемным дискам, подключенным к компьютеру.

Доступные значения:

`Allow` – пользователям разрешен доступ к съемным дискам.

`DependsOnBus` – доступ к съемным дискам зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к съемным дискам.

Значение по умолчанию: `DependsOnBus`

FloppyDrive

Правила доступа к дискетам, подключенным к компьютеру.

Kaspersky Endpoint Security не блокирует дискеты, подключенные к компьютеру с помощью шины ISA.

Доступные значения:

`Allow` – пользователям разрешен доступ к дискетам.

`DependsOnBus` – доступ к дискетам зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к дискетам.

Значение по умолчанию: `DependsOnBus`

OpticalDrive

Правила доступа к CD/DVD-приводам, подключенным к компьютеру.

Доступные значения:

`Allow` – пользователям разрешен доступ к CD/DVD-приводам.

`DependsOnBus` – доступ к CD/DVD-приводам зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к CD/DVD-приводам.

Значение по умолчанию: `DependsOnBus`

SerialPortDevice

Правила доступа к устройствам, подключенным к компьютеру через последовательный порт.

Kaspersky Endpoint Security не блокирует устройства, подключенные к компьютеру через последовательный порт с помощью шины ISA.

Доступные значения:

`Allow` – пользователям разрешен доступ к устройствам, подключенным через последовательный порт.

`DependsOnBus` – доступ к устройствам, подключенным через последовательный порт, зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к устройствам, подключенным через последовательный порт.

Значение по умолчанию: `DependsOnBus`

ParallelPortDevice

Правила доступа к устройствам, подключенным к компьютеру через параллельный порт.

Доступные значения:

`Allow` – пользователям разрешен доступ к устройствам, подключенным через параллельный порт.

`DependsOnBus` —доступ к устройствам, подключенным через параллельный порт, зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к устройствам, подключенным через параллельный порт.

Значение по умолчанию: `DependsOnBus`

Printer

Правила доступа к принтерам, подключенным к компьютеру.

Доступные значения:

`Allow` – пользователям разрешен доступ к принтерам.

`DependsOnBus` – доступ к принтерам зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к принтерам.

Значение по умолчанию: `DependsOnBus`

Modem

Правила доступа к модемам, подключенным к компьютеру.

Доступные значения:

`Allow` – пользователям разрешен доступ к модемам.

`DependsOnBus` – доступ к модемам зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к модемам.

Значение по умолчанию: `DependsOnBus`

TapeDrive

Правила доступа к стримерам, подключенным к компьютеру.

Доступные значения:

`Allow` – пользователям разрешен доступ к стримерам.

`DependsOnBus` – доступ к стримерам зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к стримерам.

Значение по умолчанию: `DependsOnBus`

MultifuncDevice

Правила доступа к мультифункциональным устройствам, подключенным к компьютеру.

Доступные значения:

`Allow` — пользователям разрешен доступ к мультифункциональным устройствам.

`DependsOnBus` — доступ к мультифункциональным устройствам зависит от правила доступа к шине подключения.

`Block` — пользователям запрещен доступ к мультифункциональным устройствам.

Значение по умолчанию: `DependsOnBus`

SmartCardReader

Правила доступа к устройствам чтения смарт-карт, подключенным к компьютеру.

Доступные значения:

`Allow` — пользователям разрешен доступ к устройствам чтения смарт-карт.

`DependsOnBus` — доступ к устройствам чтения смарт-карт зависит от правила доступа к шине подключения

`Block` — пользователям запрещен доступ к устройствам чтения смарт-карт.

Значение по умолчанию: `DependsOnBus`

WiFiAdapter

Правила доступа к Wi-Fi-адаптерам, подключенным к компьютеру.

Доступные значения:

`Allow` — пользователям разрешен доступ к Wi-Fi-адаптерам.

`DependsOnBus` — доступ к Wi-Fi-адаптерам зависит от правила доступа к шине подключения.

`Block` — пользователям запрещен доступ к Wi-Fi-адаптерам.

Значение по умолчанию: `DependsOnBus`

NetworkAdapter

Правила доступа к внешним сетевым адаптерам, подключенным к компьютеру.

Доступные значения:

`Allow` — пользователям разрешен доступ к внешним сетевым адаптерам.

`DependsOnBus` — доступ к внешним сетевым адаптерам зависит от правила доступа к шине подключения.

Значение по умолчанию: `DependsOnBus`

PortableDevice

Правила доступа к портативным устройствам, подключенным к компьютеру.

Доступные значения:

`Allow` – пользователям разрешен доступ к портативным устройствам.

`DependsOnBus` – доступ к портативным устройствам зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к портативным устройствам.

Значение по умолчанию: `DependsOnBus`

BluetoothDevice

Правила доступа к Bluetooth-устройствам, подключенным к компьютеру.

Доступные значения:

`Allow` – пользователям разрешен доступ к Bluetooth-устройствам.

`DependsOnBus` – доступ к Bluetooth-устройствам зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к Bluetooth-устройствам.

Значение по умолчанию: `DependsOnBus`

ImagingDevice

Правила доступа к устройствам обработки изображений, подключенным к компьютеру.

Доступные значения:

`Allow` – пользователям разрешен доступ к устройствам обработки изображений.

`DependsOnBus` – доступ к устройствам обработки изображений зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к устройствам обработки изображений.

Значение по умолчанию: `DependsOnBus`

InputDevice

Правила доступа к устройствам ввода, подключенным к компьютеру (клавиатура, мышь, тачпад, и другие).

Доступные значения:

`Allow` – пользователям разрешен доступ к устройствам ввода.

`DependsOnBus` – доступ к устройствам ввода зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к устройствам ввода.

Значение по умолчанию: `DependsOnBus`

SoundAdapter

Правила доступа к звуковым адаптерам, подключенным к компьютеру.

Доступные значения:

`Allow` – пользователям разрешен доступ к звуковым адаптерам.

`DependsOnBus` – доступ к звуковым адаптерам зависит от правила доступа к шине подключения.

`Block` – пользователям запрещен доступ к звуковым адаптерам.

Значение по умолчанию: `DependsOnBus`

Раздел [DeviceBus]

В разделе `[DeviceBus]` указаны правила доступа к шине подключения, определяющие, разрешено или запрещено подключение устройств.

USB

Правила доступа к шине подключения для устройств, подключенных к компьютеру через USB-интерфейс.

Доступные значения:

`Allow` – пользователям разрешен доступ к USB-устройствам.

`Block` – пользователям запрещен доступ к USB-устройствам.

Значение по умолчанию: `Allow`

FireWire

Правила доступа к шине подключения для устройств, подключенных к компьютеру через интерфейс FireWire.

Доступные значения:

`Allow` – пользователям разрешен доступ к устройствам, подключенным через интерфейс FireWire.

`Block` – пользователям запрещен доступ к устройствам, подключенным через интерфейс FireWire.

Значение по умолчанию: `Allow`

Раздел [TrustedDevices.item_#]

В разделе `[TrustedDevices.item_#]` указаны доверенные устройства, к которым у пользователей есть полный доступ в любое время.

ID

Идентификатор или маска идентификатора доверенного устройства. Можно использовать маски `*` (любая последовательность символов) или `?` (один любой символ), чтобы указать идентификатор устройства.

Комментарий

Добавить комментарий к указанному доверенному устройству.

Просмотр списка подключенных устройств

Можно просматривать список устройств, подключенных к компьютеру.

> Только пользователи с ролями *admin* и *audit* могут просматривать список подключенных устройств.

Чтобы просмотреть список устройств, подключенных к компьютеру, выполните следующую команду:

```
kesl-control --get-device-list
```

Kaspersky Endpoint Security отобразит следующую информацию о подключенных устройствах:

- **Класс**. Класс подключенного устройства. Например, *OpticalDrive* или *HardDrive*.
- **ID**. Идентификатор подключенного устройства.
- **Название**. Название подключенного устройства.
- **Заблокировано**. Параметр показывает, заблокирован ли доступ к подключенному устройству программой Kaspersky Endpoint Security (**Да** или **Нет**).
- **Системный диск**. Параметр показывает, является ли подключенное устройство системным диском (**Да** или **Нет**).

Задача Проверка съемных дисков (Removable_Drives_Scan ID: 16)

В этом разделе содержится информация о задаче Проверка съемных дисков.

О задаче Проверка съемных дисков

Когда запущена задача 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.

При запуске задача Проверка съемных дисков создает две задачи:

- Временная задача проверки по требованию (тип ODS) с параметрами по умолчанию как у задачи Scan_File. При необходимости пользователь с правами администратора может остановить выполнение этой задачи.

- Временная задача проверки загрузочных секторов (тип BootScan) с параметрами по умолчанию. Эту задачу остановить невозможно.

При изменении параметров задачи Проверка съемных дисков, новые значения не применяются к уже запущенным задачам Scan_File и Boot_Scan.

При остановке задачи Проверка съемных дисков уже запущенные задачи Scan_File и Boot_Scan не останавливаются.

По умолчанию задача Проверка съемных дисков не запущена. При необходимости вы можете запустить или остановить задачу в любой момент.

Параметры задачи Проверка съемных дисков

В этом разделе описаны параметры задачи Проверка съемных дисков.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanRemovableDrives

Включает или отключает проверку съемных дисков при подключении к компьютеру.

Этот параметр не применяется к CD/DVD-приводам и Blu-ray дискам (см. описание параметра `ScanOpticalDrives` ниже).

Доступные значения:

`DetailedScan` – 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 проверки по требованию.

`QuickScan` – проверять только файлы определенных типов на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При быстрой проверке используются параметры, заданные по умолчанию для задачи Защита от файловых угроз.

`NoScan` – не проверять съемные диски при подключении.

Значение по умолчанию: `NoScan`

ScanOpticalDrives

Включает или отключает проверку CD/DVD-приводов и Blu-ray дисков при подключении к компьютеру.

Доступные значения:

`DetailedScan` – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. При подробной проверке используются параметры, заданные по умолчанию для задачи проверки по требованию.

`QuickScan` – проверять только файлы определенных типов на CD/DVD-приводах и Blu-ray дисках. При быстрой проверке используются параметры, заданные по умолчанию для задачи Защита от файловых угроз.

`NoScan` – не проверять CD/DVD-приводы и Blu-ray диски при подключении.

Значение по умолчанию: `NoScan`

BlockDuringScan

Показывает, будут ли при проверке заблокированы файлы на подключенном диске. При проверке загрузочных секторов файлы не блокируются.

Доступные значения:

`Yes` – блокировать файлы при проверке.

`No` – не блокировать файлы при проверке.

Значение по умолчанию: `No`

Задача Защита от сетевых угроз (Network_Threat_Protection ID: 17)

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

О задаче Защита от сетевых угроз

Во время работы задачи Защита от сетевых угроз Kaspersky Endpoint Security проверяет входящий сетевой трафик на действия, характерные для сетевых атак. Программа проверяет входящий трафик для TCP-портов 80, 139, 445 и 8080.

При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, программа блокирует сетевую активность со стороны атакующего компьютера и записывает в журнал соответствующее событие.

Kaspersky Endpoint Security блокирует сетевой трафик со стороны атакующего компьютера на один час. Можно изменить параметры блокировки атакующего компьютера.

Задача Защита от сетевых угроз запускается по умолчанию при запуске Kaspersky Endpoint Security.

Параметры задачи Защита от сетевых угроз

В этом разделе описаны параметры задачи Защита от сетевых угроз.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

BlockAttackingHosts

Включает или отключает блокировку сетевой активности со стороны атакующих компьютеров.

Доступные значения:

`Yes` – запретить сетевую активность со стороны атакующих компьютеров.

`No` – разрешить сетевую активность со стороны атакующих компьютеров.

Значение по умолчанию: `Yes`

BlockDurationMinutes

Продолжительность блокировки атакующих компьютеров (в минутах).

Доступные значения:

`1 - 32768`

Значение по умолчанию: `60`

UseExcludeIPs

Включает или отключает использование списка IP-адресов, сетевую активность которых не требуется блокировать при обнаружении сетевой атаки. Программа записывает в журнал данные о вредоносной активности со стороны этих компьютеров.

Можно добавить IP-адреса в список исключений с помощью параметра `ExcludeIPs.item_#`. По умолчанию список пуст.

Доступные значения:

`Yes` – использовать список исключений IP-адресов.

`No` – не использовать список исключений IP-адресов.

Значение по умолчанию: `No`

ExcludeIPs.item_#

IP-адреса, сетевая активность которых не блокируется программой.

Доступные значения:

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

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

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

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

Задача Сканирование контейнеров (Container_Scan ID: 18)

В этом разделе содержится информация о задаче Сканирование контейнеров.

О задаче Сканирование контейнеров

Во время работы задачи Сканирование контейнеров, программа проверяет Docker-контейнеры, образы и пространства имен на вирусы и вредоносные программы. Задача Сканирование контейнеров – это однократная полная или пользовательская проверка файлов, выполняемая Kaspersky Endpoint Security. Вы можете одновременно запустить несколько задач Сканирование контейнеров.

По умолчанию задача проверки Docker-контейнеров и образов включена.

Проверка Docker-контейнеров доступна, если программа активирована по лицензии Enterprise.

Параметры задачи Проверка контейнеров

В этом разделе описаны параметры проверки, применяемые к Docker-контейнерам и образам.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanContainers

Включает или отключает проверку Docker-контейнеров, заданных по маске. Маски можно указывать с помощью параметра `ContainerNameMask`.

Доступные значения:

`Yes` – проверять Docker-контейнеры, заданные по маске.

`No` – не проверять Docker-контейнеры, заданные по маске.

Значение по умолчанию: `Yes`

ContainerNameMask

Имя или маска имени проверяемого Docker-контейнера.

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

Доступные значения:

Маски указываются в формате командной оболочки. Можно использовать символы `?` и `*`.

Значение по умолчанию: `*` (выполняется проверка всех Docker-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 отключает проверку образов, заданных по маске. Маски можно указывать с помощью параметра `ImageNameMask`.

Доступные значения:

`Yes` – проверять образы, заданные по маске.

`No` – не проверять образы, заданные по маске.

Значение по умолчанию: `Yes`

ImageNameMask

Имя или маска имени проверяемых образов.

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

Доступные значения:

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 отключает проверку всех слоев образа.

Доступные значения:

`Yes` – проверять все слои.

`No` – не проверять все слои.

Значение по умолчанию: `No`

ContainerScanAction

Действие над Docker-контейнером при обнаружении зараженного объекта. Действия над зараженным объектом внутри Docker-контейнера описаны ниже.

Доступные значения:

`StopContainerIfFailed` – программа останавливает Docker-контейнер, если не удалось вылечить зараженный объект.

`StopContainer` – программа останавливает Docker-контейнер при обнаружении зараженного объекта.

`Skip` – программа не выполняет никаких действий над Docker-контейнерами при обнаружении зараженного объекта.

Значение по умолчанию: `StopContainerIfFailed`

ImageAction

Действие над образом при обнаружении зараженного объекта. Действия над зараженным объектом внутри образа описаны ниже.

Доступные значения:

`Skip` – 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 Docker-контейнеры будут остановлены, а затем удалены.

Значение по умолчанию: `Skip`

Параметры проверки

Описанные ниже параметры применяются к объектам внутри Docker-контейнеров и образов.

ScanArchived

Включает или отключает проверку архивов, включая самораспаковывающиеся архивы (SFX-архивы). Kaspersky Endpoint Security обнаруживает зараженные объекты в архивах, но не лечит их.

Доступные значения:

`Yes` – проверять архивы, включая самораспаковывающиеся архивы (SFX-архивы). Если указано значение `FirstAction=Recommended`, программа удаляет архив, содержащий угрозу.

`No` – не проверять архивы.

Значение по умолчанию: `Yes`

ScanSfxArchived

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

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы;

`No` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `Yes`

ScanMailBase

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

Доступные значения:

`Yes` – проверять почтовые базы.

`No` – не проверять почтовые базы.

Значение по умолчанию: `No`

ScanPlainMail

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ScanPriority

Приоритет задачи. Приоритет задачи проверки – это параметр, сочетающий несколько внутренних параметров Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.

Доступные значения:

`Idle` – запустить задачу проверки с низким приоритетом. Выберите это значение, чтобы выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени.

`Normal` – запустить задачу проверки со стандартным приоритетом. Выберите это значение, чтобы текущая задача выполнялась быстрее.

Значение по умолчанию: `Idle`

TimeLimit

Продолжительность проверки отдельного архива (в секундах).

Программа пропускает архивы, проверка которых выполняется дольше указанного времени.

Доступные значения:

`0 - 9999`

Если указано значение `0`, продолжительность проверки не ограничена.

Значение по умолчанию: `0`

SizeLimit

Максимальный размер проверяемого архива (в мегабайтах).

Если архив больше указанного значения, программа пропускает его при проверке.

Доступные значения:

`0 – 999999`

Если указано значение `0`, выполняется проверка объектов любого размера.

Значение по умолчанию: `0`

Каждому обнаруженному объекту присваивается статус, показывающий его опасность для системы. Можно выбрать два действия, выполняемые над зараженными объектами. Сначала программа пытается выполнить первое действие над зараженным объектом. Если выполнить первое действие не удалось, выполняется второе действие.

Указанные действия выполняются на том уровне, на котором был обнаружен зараженный объект.

FirstAction

Первое действие, выполняемое над зараженным объектом.

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 `Удалить`, программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.

Доступные значения:

`Disinfect` – программа блокирует доступ к зараженному объекту и пытается его вылечить.

`Remove` – программа блокирует доступ к зараженному объекту и удаляет его.

`Recommended` – программа выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

`Skip` – программа пропускает зараженный объект при проверке.

Значение по умолчанию: `Recommended`

SecondAction

Действие, выполняемое над зараженным объектом, если не удалось выполнить действие, заданное параметром `FirstAction`.

Доступные значения:

`Disinfect` – программа блокирует доступ к зараженному объекту и пытается его вылечить.

`Remove` – программа блокирует доступ к зараженному объекту и удаляет его.

`Recommended` – программа выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

`Skip` – программа блокирует доступ к зараженному объекту.

Значение по умолчанию: `Skip`

UseExcludeMasks

Включает или отключает исключение объектов из проверки.

Доступные значения:

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

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

Значение по умолчанию: `No`

UseExcludeThreats

Включает или отключает исключение из проверки заданных угроз.

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportCleanObjects

Включает или отключает запись в журнал информации о проверенных объектах, относительно которых во время проверки программа приняла решение "чистые".

Доступные значения:

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

`No` – не записывать в журнал информацию о "чистых" объектах.

Значение по умолчанию: `No`

ReportPackedObjects

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportUnprocessedObjects

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

Доступные значения:

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

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

Значение по умолчанию: `No`

UseAnalyzer

Включает или отключает эвристический анализатор.

Доступные значения:

`Yes` – включить эвристический анализатор;

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`

HeuristicLevel

Уровень эвристического анализа.

Доступные значения:

`Light` – наименее детализированная проверка, минимальная нагрузка на систему.

`Medium` – средняя детализация при проверке, сбалансированная нагрузка на систему.

`Deep` – наиболее детализированная проверка, максимальная нагрузка на систему.

`Рекомендованный` – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского".

Значение по умолчанию: `Recommended`

UseIChecker

Включает или отключает использование технологии iChecker при проверке.

Доступные значения:

`Yes` – использовать технологию iChecker при проверке.

`No` – не использовать технологию iChecker при проверке.

Значение по умолчанию: `Yes`

Интеграция с Jenkins

Kaspersky Endpoint Security 11 для Linux поддерживает интеграцию с Jenkins. Плагины Jenkins Pipeline можно использовать для сканирования Docker-образов на разных этапах. Например, можно сканировать Docker-образы в репозитории в процессе разработки или перед публикацией.

Интеграция с Jenkins доступна, только если программа Kaspersky Endpoint Security активирована по лицензии Kaspersky Hybrid Cloud Security Enterprise.

Jenkins нельзя устанавливать на сервере, на котором установлена программа Kaspersky Endpoint Security.

Для интеграции Kaspersky Endpoint Security с Jenkins выполните следующие действия:

1. Установите Docker Engine на узле Jenkins.

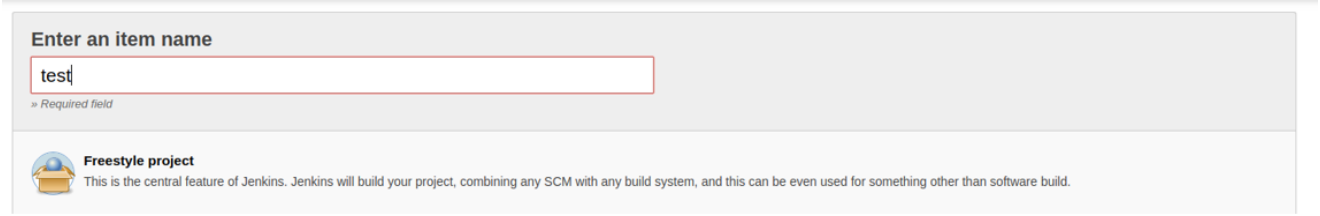
   Дополнительная информация приведена в документации Docker Engine.

2. Добавьте пользователя Jenkins в группу `docker`:

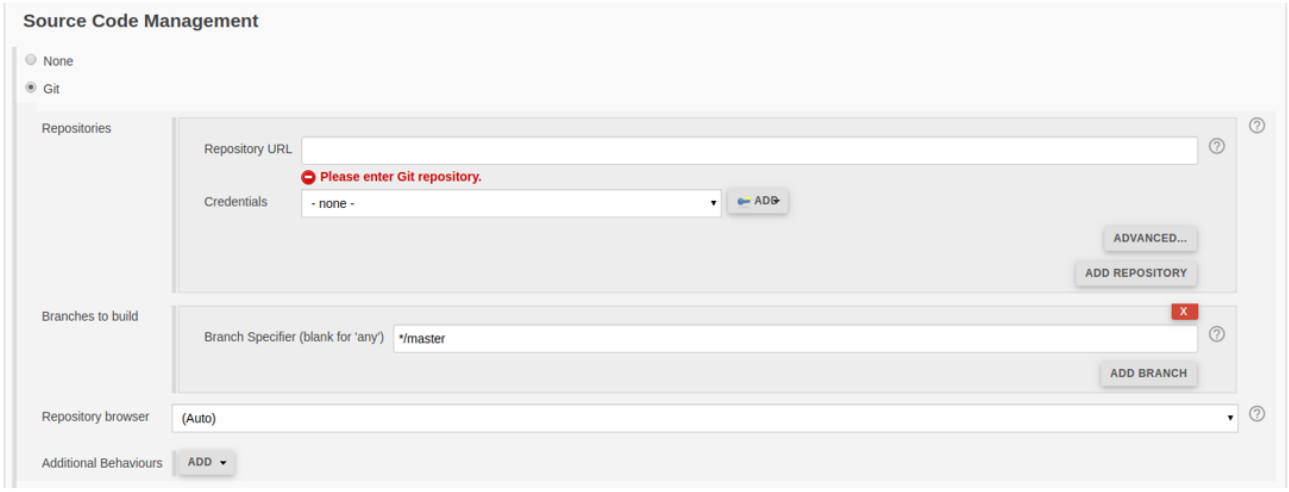
   ```
   sudo usermod -aG docker <имя пользователя Jenkins>
   ```

   Обычно используется имя `jenkins`.

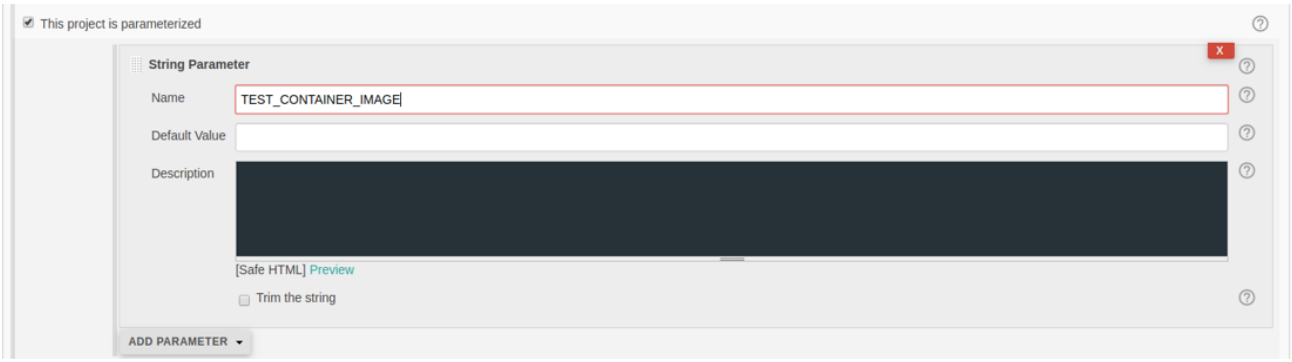
3. В Jenkins создайте новое задание на сборку с название `test` (**Создать элемент** → **Указать название элемента**).

4. Укажите репозиторий Git для вашего проекта.



5. В параметрах задания на сборку добавьте название Docker-образа (строковый параметр), например, `TEST_CONTAINER_IMAGE`.

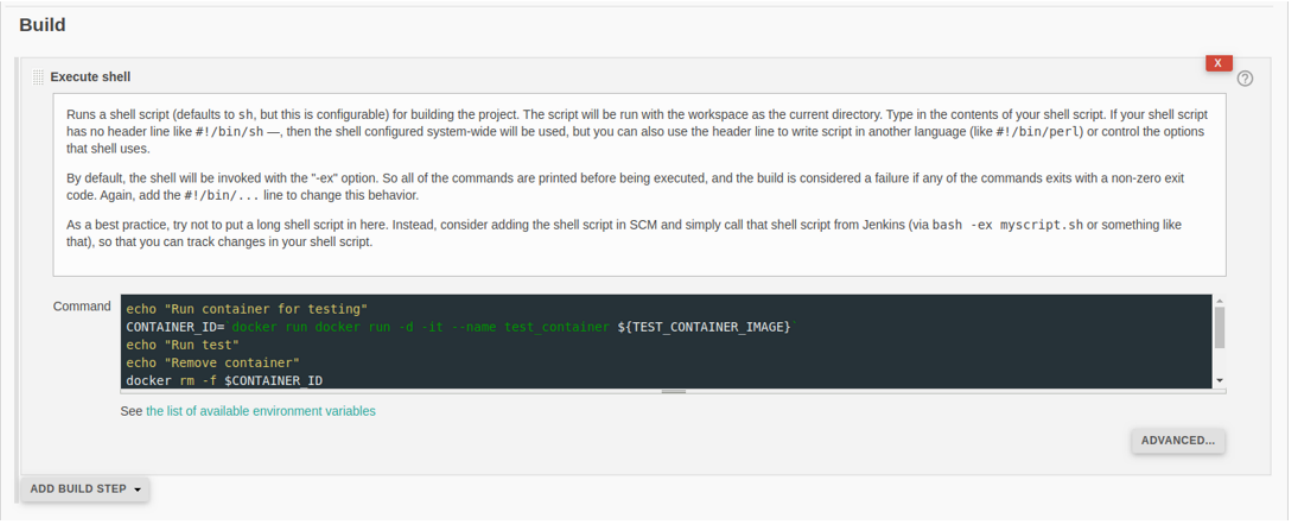


6. В поле **Команда** введите скрипт shell, чтобы выполнить сканирование контейнера:

```
echo "Сканирование контейнера"
CONTAINER_ID=`/opt/kaspersky/kesl/bin/kesl-control --scan-container
${TEST_CONTAINER_IMAGE}`
echo "Тест"
echo "Удаление контейнера"
docker rm -f $CONTAINER_ID
```

7. Чтобы выполнить сканирование контейнера, выполните следующий скрипт:

```
echo "Сканирование контейнера"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container
${TEST_IMAGE_NAME}*)
echo "Сканирование выполнено: " "
echo $SCAN_RESULT
```



8. Чтобы выполнить сканирование 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 "Собрать образ из ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
    echo "Docker-файл получен: ${DOCKER_FILE_FETCHED}"
else
    echo "Docker-файл не получен"
    exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME} .
echo "Сканирование Docker-образа"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container
${TEST_IMAGE_NAME}*)
echo "Сканирование выполнено: " "
echo $SCAN_RESULT
```

9. Сохраните задание на сборку.

Пользовательская задача Сканирование контейнеров (Container_Scan ID: 19)

В этом разделе содержится информация о пользовательской задаче Сканирование контейнеров.

О пользовательской задаче Сканирование контейнеров

Во время работы пользовательской задачи Сканирование контейнеров программа проверяет Docker-контейнеры и образы на вирусы и вредоносные программы. Можно одновременно запустить несколько пользовательских задач Сканирование контейнеров.

В пользовательской задаче Сканирование контейнеров используются те же значения параметров, что и в задаче полной проверки (Container_Scan), за исключением параметра `ScanPriority=Normal`. В пользовательской задаче не выполняется проверка пространства имен.

После завершения проверки программа автоматически удаляет пользовательскую задачу.

Пользовательская задача Сканирование контейнеров (Container_Scan ID: 19)

В этом разделе описаны параметры проверки, применяемые к Docker-контейнерам и образам.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanContainers

Включает или отключает проверку Docker-контейнеров, заданных по маске. Маски можно указывать с помощью параметра `ContainerNameMask`.

Доступные значения:

`Yes` – проверять Docker-контейнеры, заданные по маске.

`No` – не проверять Docker-контейнеры, заданные по маске.

Значение по умолчанию: `Yes`

ContainerNameMask

Имя или маска имени проверяемого Docker-контейнера.

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

Доступные значения:

Маски указываются в формате командной оболочки. Можно использовать символы `?` и `*`.

Значение по умолчанию: `*` (выполняется проверка всех Docker-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 отключает проверку образов, заданных по маске. Маски можно указывать с помощью параметра `ImageNameMask`.

Доступные значения:

`Yes` – проверять образы, заданные по маске.

`No` – не проверять образы, заданные по маске.

Значение по умолчанию: `Yes`

ImageNameMask

Имя или маска имени проверяемых образов.

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

Доступные значения:

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 отключает проверку всех слоев образа.

Доступные значения:

`Yes` – проверять все слои.

`No` – не проверять все слои.

Значение по умолчанию: `No`

ContainerScanAction

Действие над Docker-контейнером при обнаружении зараженного объекта. Действия над зараженным объектом внутри Docker-контейнера описаны ниже, в разделе **Параметры проверки**.

Доступные значения:

`StopContainerIfFailed` – программа останавливает Docker-контейнер, если не удалось вылечить зараженный объект.

`StopContainer` – программа останавливает Docker-контейнер при обнаружении зараженного объекта.

`Skip` – программа не выполняет никаких действий над Docker-контейнерами при обнаружении зараженного объекта.

Значение по умолчанию: `StopContainerIfFailed`

ImageAction

Действие над образом при обнаружении зараженного объекта. Действия над зараженным объектом внутри образа описаны ниже, в разделе **Параметры проверки**.

Доступные значения:

`Skip` – 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 Docker-контейнеры будут остановлены, а затем удалены.

Значение по умолчанию: `Skip`

Параметры проверки

Описанные ниже параметры применяются к объектам внутри Docker-контейнеров и образов.

ScanArchived

Включает или отключает проверку архивов, включая самораспаковывающиеся архивы (SFX-архивы). Kaspersky Endpoint Security обнаруживает зараженные объекты в архивах, но не лечит их.

Доступные значения:

`Yes` – проверять архивы, включая самораспаковывающиеся архивы (SFX-архивы). Если указано значение `FirstAction=Recommended`, программа удаляет архив, содержащий угрозу.

`No` – не проверять архивы.

Значение по умолчанию: `Yes`

ScanSfxArchived

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

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы;

`No` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `Yes`

ScanMailBase

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

Доступные значения:

`Yes` – проверять почтовые базы.

`No` – не проверять почтовые базы.

Значение по умолчанию: `No`

ScanPlainMail

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ScanPriority

Приоритет задачи. Приоритет задачи проверки – это параметр, сочетающий несколько внутренних параметров Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.

Доступные значения:

`Idle` – запустить задачу проверки с низким приоритетом. Выберите это значение, чтобы выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени.

`Normal` – запустить задачу проверки со стандартным приоритетом. Выберите это значение, чтобы текущая задача выполнялась быстрее.

Значение по умолчанию: `Normal`

TimeLimit

Продолжительность проверки отдельного архива (в секундах).

Программа пропускает архивы, проверка которых выполняется дольше указанного времени.

Доступные значения:

`0 – 9999`

Если указано значение `0`, продолжительность проверки не ограничена.

Значение по умолчанию: `0`

SizeLimit

Максимальный размер проверяемого архива (в мегабайтах).

Если архив больше указанного значения, программа пропускает его при проверке.

Доступные значения:

`0 – 999999`

Если указано значение `0`, выполняется проверка объектов любого размера.

Значение по умолчанию: `0`

Каждому обнаруженному объекту присваивается статус, показывающий его опасность для системы. Можно выбрать два действия, выполняемые над зараженными объектами. Сначала программа пытается выполнить первое действие над зараженным объектом. Если выполнить первое действие не удалось, выполняется второе действие.

Указанные действия выполняются на том уровне, на котором был обнаружен зараженный объект.

FirstAction

Первое действие, выполняемое над зараженным объектом.

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 `Удалить`, программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.

Доступные значения:

`Disinfect` – программа блокирует доступ к зараженному объекту и пытается его вылечить.

`Remove` – программа блокирует доступ к зараженному объекту и удаляет его.

`Recommended` – программа выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

`Skip` – программа пропускает зараженный объект при проверке.

Значение по умолчанию: `Recommended`

SecondAction

Действие, выполняемое над зараженным объектом, если не удалось выполнить действие, заданное параметром `FirstAction`.

Доступные значения:

`Disinfect` – программа блокирует доступ к зараженному объекту и пытается его вылечить.

`Remove` – программа блокирует доступ к зараженному объекту и удаляет его.

`Recommended` – программа выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

`Skip` – программа блокирует доступ к зараженному объекту.

Значение по умолчанию: `Skip`

UseExcludeMasks

Включает или отключает исключение объектов из проверки.

Доступные значения:

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

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

Значение по умолчанию: `No`

UseExcludeThreats

Включает или отключает исключение из проверки заданных угроз.

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportCleanObjects

Включает или отключает запись в журнал информации о проверенных объектах, относительно которых во время проверки программа приняла решение "чистые".

Доступные значения:

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

`No` – не записывать в журнал информацию о "чистых" объектах.

Значение по умолчанию: `No`

ReportPackedObjects

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

Доступные значения:

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

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

Значение по умолчанию: `No`

ReportUnprocessedObjects

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

Доступные значения:

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

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

Значение по умолчанию: `No`

UseAnalyzer

Включает или отключает эвристический анализатор.

Доступные значения:

`Yes` – включить эвристический анализатор;

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`

HeuristicLevel

Уровень эвристического анализа.

Доступные значения:

`Light` – наименее детализированная проверка, минимальная нагрузка на систему.

`Medium` – средняя детализация при проверке, сбалансированная нагрузка на систему.

`Deep` – наиболее детализированная проверка, максимальная нагрузка на систему.

`Рекомендованный` – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского".

Значение по умолчанию: `Recommended`

UseIChecker

Включает или отключает использование технологии iChecker при проверке.

Доступные значения:

`Yes` – использовать технологию iChecker при проверке.

`No` – не использовать технологию iChecker при проверке.

Значение по умолчанию: `Yes`

Запуск пользовательской задачи Сканирование контейнеров

Чтобы запустить пользовательскую задачу Сканирование контейнеров, выполните следующую команду:

```
kesl-control --scan-container <ID Docker-контейнера или образа|имя Docker-контейнера|имя образа[:тег]>
```

Если существует несколько элементов с одинаковым именем, программа проверяет их все.

Задача Анализ поведения (Behavior_Detection ID: 20)

В этом разделе содержится информация о задаче Анализ поведения.

Задача Анализ поведения контролирует вредоносную активность в операционной системе. При обнаружении вредоносной активности Kaspersky Endpoint Security завершает этот процесс.

По умолчанию задача запускается при старте Kaspersky Endpoint Security. Можно запускать и останавливать задачу Анализ поведения.

Задача Анализ поведения не имеет параметров.

Проверка зашифрованных соединений

В этом разделе содержится информация о параметрах проверки зашифрованных соединений.

Параметры сети

В этом разделе описаны параметры проверки зашифрованных соединений. Эти параметры используются в задачах Защита от веб-угроз и Защита от сетевых угроз.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

EncryptedConnectionsScan

Включает или отключает проверку зашифрованного трафика.

Для FTP протокола проверка зашифрованных соединений отключена по умолчанию.

Доступные значения:

`Yes` – включить проверку зашифрованных соединений.

`No` – выключить проверку зашифрованных соединений. Программа не расшифровывает зашифрованный трафик.

Значение по умолчанию: `Yes`

EncryptedConnectionsScanErrorAction

Действие, выполняемое программой при возникновении ошибки проверки зашифрованных соединений на веб-сайте.

Доступные значения:

`AddToAutoExclusions` – 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.

Значение по умолчанию: `AddToAutoExclusions`

UntrustedCertificateAction

Действие, выполняемое программой при возникновении ошибки проверки зашифрованных соединений на веб-сайте.

Доступные значения:

`Allow` – разрешить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом.

`Block` – запретить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом.

Значение по умолчанию: `Allow`

ManageExclusions

Включает или отключает использование исключений при проверке зашифрованного трафика.

Доступные значения:

`Yes` – не проверять веб-сайты, указанные в разделе `[Exclusions.item_#]`.

`No` – проверять все веб-сайты.

Значение по умолчанию: `No`

MonitorNetworkPorts

Способ контроля сетевых портов программой Kaspersky Endpoint Security.

Доступные значения:

`Selected` – 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.

Значение по умолчанию: `Selected`

Раздел [Exclusions.item_#]

В разделе `[Exclusions.item_#]` указаны домены, исключенные из проверки. Программа не проверяет зашифрованные соединения, установленные при посещении указанных доменов.

DomainName

Имя домена. Для указания домена можно использовать маски.

Раздел [NetworkPorts.item_#]

В разделе `[NetworkPorts.item_#]` указаны сетевые порты, контролируемые программой.

PortName

Описание сетевого порта.

Порт

Номера сетевых портов, контролируемые программой.

Доступные значения:

`1 – 65535`

Управление параметрами проверки зашифрованных соединений

Из командной строки можно управлять параметрами проверки зашифрованных соединений.

Чтобы вывести список исключений из проверки зашифрованных соединений, добавленных пользователем, выполните следующую команду:

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

Чтобы вывести список исключений из проверки зашифрованных соединений, добавленных Kaspersky Endpoint Security, выполните следующую команду:

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

Чтобы вывести список исключений из проверки зашифрованных соединений, полученных из баз "Лаборатории Касперского", выполните следующую команду:

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

Чтобы очистить список доменов, которые программа Kaspersky Endpoint Security автоматически исключила из проверки, выполните следующую команду:

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

Чтобы выгрузить параметры проверки зашифрованных соединений из хранилища, выполните следующую команду:

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

Выходной файл имеет формат INI.

Чтобы сохранить параметры проверки зашифрованных соединений в файл, выполните следующую команду:

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

Участие в Kaspersky Security Network

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

Об участии в Kaspersky Security Network

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на 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).

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.

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 "Лаборатории Касперского" (https://www.kaspersky.ru/products-and-services-privacy-policy). Файл с текстом Положения о Kaspersky Security Network входит в комплект поставки программы.

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа 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 .

Настроить параметры KSN Proxy можно в свойствах политики Kaspersky Security Center.

Участие в Kaspersky Security Network является добровольным. Программа предлагает участвовать в KSN во время установки. Начать или прекратить использование KSN можно в любой момент.

Включение и выключение использования Kaspersky Security Network

Чтобы включить использование Kaspersky Security Network, выполните одну из следующих команд:

- Чтобы включить использование Kaspersky Security Network со статистикой, выполните команду:

  ```
  kesl-control --set-app-settings UseKSN=Extended
  ```

- Чтобы включить использование Kaspersky Security Network без статистики, выполните команду:

  ```
  kesl-control --set-app-settings UseKSN=Basic
  ```

Чтобы выключить использование Kaspersky Security Network, выполните следующую команду:

```
kesl-control --set-app-settings UseKSN=No
```

Чтобы включить или выключить использование Kaspersky Security Network с помощью конфигурационного файла, выполните следующую команду:

```
kesl-control --set-app-settings --file <имя конфигурационного файла>
```

Если программа Kaspersky Endpoint Security, установленная на компьютере, работает под управлением политики, которая была назначена в Kaspersky Security Center, значение параметра `UseKSN` можно изменить только в Kaspersky Security Center.

Если программа Kaspersky Endpoint Security, установленная на компьютере, прекратила работать под управлением политики, параметру присваивается следующее значение: `UseKSN=No`.

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

Проверка подключения к Kaspersky Security Network

Чтобы проверить подключение к Kaspersky Security Network, выполните следующую команду:

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

Строка `KSN state` показывает статус подключения к Kaspersky Security Network:

- Если отображается статус `Extended`, Kaspersky Endpoint Security подключается к Kaspersky Security Network, можно получить информацию из базы знаний, отправляется анонимная статистика и информация о типах и источниках угроз.
- Если отображается статус `Basic`, Kaspersky Endpoint Security подключается 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 `No`, Kaspersky Endpoint Security не подключается к Kaspersky Security Network.

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Ваш компьютер не подключен к интернету.
- Вы не участвуете в Kaspersky Security Network.
- Программа не активирована, или срок действия лицензии истек.

- Выявлены проблемы, связанные с ключом. Например, ключ попал в черный список ключей.

Дополнительная защита с использованием Kaspersky Security Network

"Лаборатория Касперского" предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков "Лаборатории Касперского" обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте "Лаборатории Касперского".

Проверка целостности компонентов программы

Kaspersky Endpoint Security содержит множество различных бинарных модулей в форме библиотек динамических ссылок, 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, Kaspersky Endpoint Security может проверять целостность компонентов программы.

Программа проверяет модули и файлы на наличие несанкционированных изменений и повреждений. Если контрольная сумма модуля или файла программы является некорректной, он считается поврежденным.

Программа проверяет целостность *файла манифеста*, содержащего список файлов программы, целостность которых критична для корректной работы компонентов программы.

Целостность компонентов программы проверяется с помощью инструмента integrity_check_tool, расположенного в директории /opt/kaspersky/kesl/bin. Эта же директория содержит файл манифеста – integrity_check.xml, защищенный криптографической сигнатурой "Лаборатории Касперского".

> Для запуска инструмента проверки целостности необходима учетная запись с root-правами.

Проверку целостности можно выполнять с помощью инструмента, устанавливаемого совместно с программой, или с помощью инструмента, поставляемого на сертифицированном CD-диске.

Инструмент проверки целостности рекомендуется запускать с сертифицированного CD-диска, чтобы гарантировать целостность самого инструмента. При запуске инструмента с CD-диска необходимо указать полный путь к файлу манифеста в директории программы.

Чтобы проверить целостность компонентов программы, выполните следующую команду:

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

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

Инструмент проверки целостности можно запустить со следующими дополнительными параметрами:

- `-h, --help` – показать справку для параметров инструмента.
- `-V, --verbose` – раскрыть вывод информации о выполненных действиях и результатах. Если вы не укажите этот параметр, будут отображаться только ошибки, объекты, не прошедшие проверку, и общая статистика проверки.
- `-L, -- log-file <файл>`, где `<файл>` – это имя файла, используемое для записи событий, произошедших во время проверки. По умолчанию события передаются в стандартный поток stdout.
- `-l, -- log-level <0-1000>`, где `<0-1000>` – это уровень детализации вывода событий. По умолчанию уровень детализации – `0`.

Результат проверки каждого файла манифеста отображается рядом с именем файла манифеста в следующем формате:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата `0`).
- `FAILED` – целостность файлов не подтверждена (код возврата отличен от `0`).

Управление программой через Kaspersky Security Center

Этот раздел содержит информацию об управлении программой Kaspersky Endpoint Security через Kaspersky Security Center. Описание приведено для Kaspersky Security Center 11.

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Security, настраивать параметры работы программы и запускать задачи на управляемых устройствах.

Управление программой через Kaspersky Security Center осуществляется с помощью плагина управления Kaspersky Endpoint Security.

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

Вы можете выполнять следующие действия в Консоли администрирования Kaspersky Security Center:

- просматривать состояние защиты устройств;
- настраивать общие параметры защиты устройств;
- управлять политиками;
- управлять следующими задачами:
  - Добавление ключа
  - Проверка контейнеров
  - Проверка целостности системы по требованию
  - Проверка загрузочных секторов
  - Проверка памяти процессов
  - Обновление
  - Откат обновлений
  - Антивирусная проверка

Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере

Чтобы запустить или остановить Kaspersky Endpoint Security на клиентском компьютере, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит

нужный вам компьютер.

3. В рабочей области выберите закладку **Устройства**.

4. В списке управляемых устройств выберите компьютер, на котором вы хотите запустить или остановить программу.

5. Правой клавишей мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.

   Откроется окно свойств компьютера.

6. В окне свойств компьютера выберите раздел **Программы**.

   Справа в окне свойств компьютера отобразится список программ "Лаборатории Касперского", установленных на компьютере.

7. Выберите программу Kaspersky Endpoint Security 11 для Linux.

8. Если вы хотите запустить программу, нажмите на кнопку ▶ справа от списка программ "Лаборатории Касперского" или выполните следующие действия:

   a. Правой клавишей мыши откройте контекстное меню программы Kaspersky Endpoint Security 11 для Linux и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ "Лаборатории Касперского".

      Откроется окно **Параметры Kaspersky Endpoint Security 11 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. Правой клавишей мыши откройте контекстное меню программы Kaspersky Endpoint Security 11 для Linux и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ.

      Откроется окно **Параметры Kaspersky Endpoint Security 11 для Linux** на закладке **Общие**.

   b. Нажмите на кнопку **Остановить**.

Просмотр состояния защиты компьютера

Чтобы просмотреть состояние защиты компьютера, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый

компьютер.

2. В рабочей области выберите закладку **Устройства**.

3. Правой клавишей мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.

4. В окне **Свойства** выберите закладку **Защита**.

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

- **Статус устройства** – статус клиентского устройства, присвоенный на основе критерия, заданного администратором для статусов антивирусной защиты устройства и активности устройства в сети.

- **Все проблемы** – полный 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.

- **Общее количество обнаруженных 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.

Просмотр параметров Kaspersky Endpoint Security

Чтобы просмотреть параметры Kaspersky Endpoint Security, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый компьютер.

2. В рабочей области выберите закладку **Устройства**.

3. Правой клавишей мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.

4. В окне **Свойства: <Имя компьютера>** выберите раздел **Программы**.

5. В разделе **Программы** выберите Kaspersky Endpoint Security 11 для Linux в списке установленных программ и в контекстном меню программы выберите пункт **Свойства**.

   В результате откроется окно **Параметры Kaspersky Endpoint Security 11 для Linux** на разделе **Общие**.

В окне **Параметры Kaspersky Endpoint Security 11 для Linux** отображается следующая информация о Kaspersky Endpoint Security:

- В разделе **Общие** содержится общая информация об установленной программе:
  - **Номер версии** – номер версии Kaspersky Endpoint Security.
  - **Установлено** – дата и время установки Kaspersky Endpoint Security на защищаемом компьютере.
  - **Текущее состояние** – состояние задачи Защита от файловых угроз, например: *Выполняется* или *Приостановлена*.
  - **Последнее обновление ПО** – дата и время последнего обновления программных модулей Kaspersky Endpoint Security.
  - **Установленные обновления** – список программных модулей, для которых установлены обновления.
  - **Базы программы** – дата и время последнего обновления антивирусных баз, а также количество записей в базах.
- В разделе **Компоненты** содержится список стандартных задач. Для каждой задачи отображается ее статус (например, *Запущена* или *Остановлена*) и версия.
- В разделе **Ключи** приведена информация об активном и дополнительном ключе:
  - **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.
- **Ограничение** – количество компьютеров, на которых вы можете использовать ключ.

- В разделе **Настройка событий** содержатся события, которые Kaspersky Endpoint Security сохраняет в хранилище событий.
- В разделе **Дополнительно** содержится информация о плагине управления программой.

Управление политиками

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

О политиках

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

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

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

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

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

Вы можете использовать политики для настройки параметров таких задач Kaspersky Endpoint Security, как Защита от файловых угроз, Управление сетевым экраном, Защита от шифрования, Контроль целостности системы при доступе, Управление хранилищем и других параметров.

Права на доступ к параметрам политики (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, и отдельно для каждой функциональной области Kaspersky Endpoint Security. Для настройки прав доступа к параметрам политики перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center.

Вы можете выполнять следующие действия над политикой:

- Создавать политику.
- Изменять параметры политики.

  > Если учетная запись пользователя, под которой вы осуществили доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Удалять политику.
- Изменять состояние политики.

Информацию о работе с политиками, не касающуюся взаимодействия с Kaspersky Endpoint Security, вы можете прочитать в документации для Kaspersky Security Center.

Создание политики

Чтобы создать политику, выполните следующие действия:

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

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

Запустится Мастер создания политики.

5. Следуйте указаниям Мастера создания политики.

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. Правой клавишей мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название политики>**.

   Параметры политики для Kaspersky Endpoint Security включают в себя параметры задач и параметры программы. В разделе **Базовая защита** содержатся разделы **Параметры защиты от файловых угроз**, **Области исключений**, **Управление сетевым экраном**, **Защита от веб-угроз** и **Защита от сетевых угроз**. В разделе **Продвинутая защита** содержатся разделы **Параметры KSN**, **Параметры защиты от шифрования**, **Параметры контроля целостности системы**, **Контроль устройств** и **Анализ поведения**. В разделе **Общие параметры** содержатся разделы **Параметры прокси-сервера**, **Параметры программы**, **Параметры перехватчика**, **Параметры сети**, **Глобальные исключения** и **Хранилища**.
6. Измените параметры политики.
7. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**, чтобы сохранить изменения.

Управление задачами

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

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

О задачах для Kaspersky Endpoint Security

Kaspersky Security Center управляет работой программы Kaspersky Endpoint Security, установленной на компьютерах, с помощью задач.

При работе с Kaspersky Endpoint Security через Kaspersky Security Center вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного компьютера;
- групповые задачи, определенные для компьютеров, входящих в группы администрирования;
- задачи для наборов компьютеров, не входящих в группы администрирования.

> Такие задачи для наборов компьютеров распространяются только на компьютеры, указанные в параметрах задачи. Если в набор компьютеров, для которого сформирована задача, добавлены новые компьютеры, то для них эта задача не выполняется. В этом случае вам нужно создать новую задачу или изменить параметры уже существующей задачи.

Вы можете создавать задачи следующих типов:

- **Добавление ключа**. В процессе выполнения задачи Kaspersky Endpoint Security добавляет ключ, в том числе дополнительный, для активации программы.
- **Проверка контейнеров**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет Docker-контейнеры и образы.
- **Проверка целостности системы по требованию**. В процессе выполнения этой задачи изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.
- **Проверка загрузочных секторов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет загрузочные сектора компьютера.
- **Проверка памяти процессов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет системную память компьютера.
- **Обновление**. В процессе выполнения задачи Kaspersky Endpoint Security обновляет антивирусные базы в соответствии с установленными параметрами обновления.
- **Откат обновлений**. В процессе выполнения задачи Kaspersky Endpoint Security откатывает последнее обновление антивирусных баз.

- **Антивирусная проверка**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи.

Вы можете выполнять следующие действия над задачами:

- Запускать, останавливать, приостанавливать и возобновлять выполнение задач.

  Задачу Обновление невозможно приостановить и возобновить. Ее можно только запустить или остановить;

- Создавать новые задачи.

- изменять параметры задач.

Права на доступ к параметрам задач Kaspersky Endpoint Security (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через параметры доступа к функциональным областям Kaspersky Endpoint Security. Для настройки прав доступа к параметрам функциональных областей Kaspersky Endpoint Security, перейдите в раздел Безопасность окна свойств Сервера администрирования Kaspersky Security Center.

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

Создание локальной задачи

Чтобы создать локальную задачу, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.

3. В рабочей области выберите закладку **Устройства**.

4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите создать локальную задачу.

5. Правой клавишей мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.

   Откроется окно свойств компьютера.

6. Выберите раздел **Задачи**.

7. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания задачи.

8. Следуйте указаниям Мастера создания задачи.

Создание групповой задачи

Чтобы создать групповую задачу, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** в дереве Консоли администрирования.
3. Выполните одно из следующих действий:

   - Нажмите на кнопку **Создать задачу**.
   - Правой клавишей мыши откройте контекстное меню. Выберите пункт **Создать задачу**.

   Запустится Мастер создания задачи.

4. Следуйте указаниям Мастера создания задачи.

Создание задачи для выбора устройства

Чтобы создать задачу для выбора устройства, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** в дереве Консоли администрирования.
3. Нажмите на кнопку **Создать задачу**.

   Запустится Мастер создания задачи.

4. Следуйте указаниям Мастера создания задачи.
5. В окне мастера **Выбор устройств, которым будет назначена задача** нажмите на кнопку **Назначить задачу набору устройств**.
6. В следующем окне мастера нажмите на кнопку **Обзор**.

   Откроется окно **Выбор устройства**.

7. Выберите нужное устройство.

8. Нажмите на кнопку **OK** в окне **Выбор устройства**.

9. Следуйте указаниям Мастера создания задачи.

Запуск, остановка, приостановка и возобновление выполнения задачи вручную

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

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

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.

3. В рабочей области выберите закладку **Устройства**.

4. В списке клиентских компьютеров выберите компьютер, на котором вы хотите запустить / остановить / приостановить / возобновить выполнение локальной задачи.

5. Выберите пункт **Свойства** в контекстном меню компьютера.

   Откроется окно свойств компьютера.

6. Выберите раздел **Задачи**.

   В правой части окна отобразится список локальных задач.

7. Выберите локальную задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.

8. Выполните одно из следующих действий:

   - Правой клавишей мыши откройте контекстное меню локальной задачи. Выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

- Нажмите на кнопку ▶ / ■ справа от списка локальных задач, чтобы запустить или остановить локальную задачу.

- Нажмите на кнопку **Свойства** под списком локальных задач. Откроется окно **Свойства: <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, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите
запустить / остановить / приостановить / возобновить выполнение групповой задачи.

3. В рабочей области выберите закладку **Задачи**.

   В правой части окна отобразится список групповых задач.

4. В списке групповых задач выберите групповую задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.

5. Правой клавишей мыши откройте контекстное меню групповой задачи. Выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

Изменение параметров локальной задачи

Чтобы изменить параметры локальной задачи, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.

3. В рабочей области выберите закладку **Устройства**.

4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите настроить параметры программы.

5. 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 **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 групповой задачи

Чтобы изменить параметры групповой задачи, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** откройте папку с названием нужной группы администрирования.

3. В рабочей области выберите закладку **Задачи**.

4. В нижней части панели задач отобразится список групповых задач.

5. Выберите в списке групповых задач нужную групповую задачу.

6. 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, выполните следующие действия:

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. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - В контекстном меню задачи выберите пункт **Свойства**.
   - Перейдите по ссылке **Настроить задачу**, расположенной в правой части рабочей области Консоли администрирования.
4. Измените параметры задачи для набора устройств.
5. Чтобы сохранить изменения, в окне **Свойства: <Название задачи для набора устройств>** нажмите на кнопку **ОК**.

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.

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-разрядной операционной системе и в директории /opt/kaspersky/klnagent64/bin в 64-разрядной операционной системе. В зависимости от используемых ключей Агент выполняет следующие действия при запуске:

- выводит на экран или заносит в файл журнала событий значения параметров подключения установленного на клиентском компьютере Агента администрирования к Серверу администрирования;

- записывает в файл журнала событий статистику Агента администрирования (с момента последнего запуска данного компонента) и результаты выполнения утилиты либо выводит информацию на экран;

- предпринимает попытку установить соединение Агента администрирования с Сервером администрирования;

- если соединение установить не удалось, посылает ICMP-пакет для проверки статуса компьютера, на котором установлен Сервер администрирования.

Синтаксис утилиты

```
klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>] [-restart]
```

Описание ключей

- `-logfile <имя файла>` – 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-разрядной операционной системе и в директории /opt/kaspersky/klnagent64/bin в 64-разрядной операционной системе. В зависимости от используемых ключей Агент выполняет следующие действия при запуске:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;

- записывает результаты выполнения операции в файл журнала событий или выводит их на экран.

Синтаксис утилиты

```
klmover [-logfile <имя файла>] {-address <адрес сервера>} [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>] [-silent] [-dupfix]
```

Описание ключей:

- `-logfile <имя файла>` – записать результаты 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 порта SSL>` – 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 не-интерактивном 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.

Управление программой через Kaspersky Security Center Web Console и Cloud Console

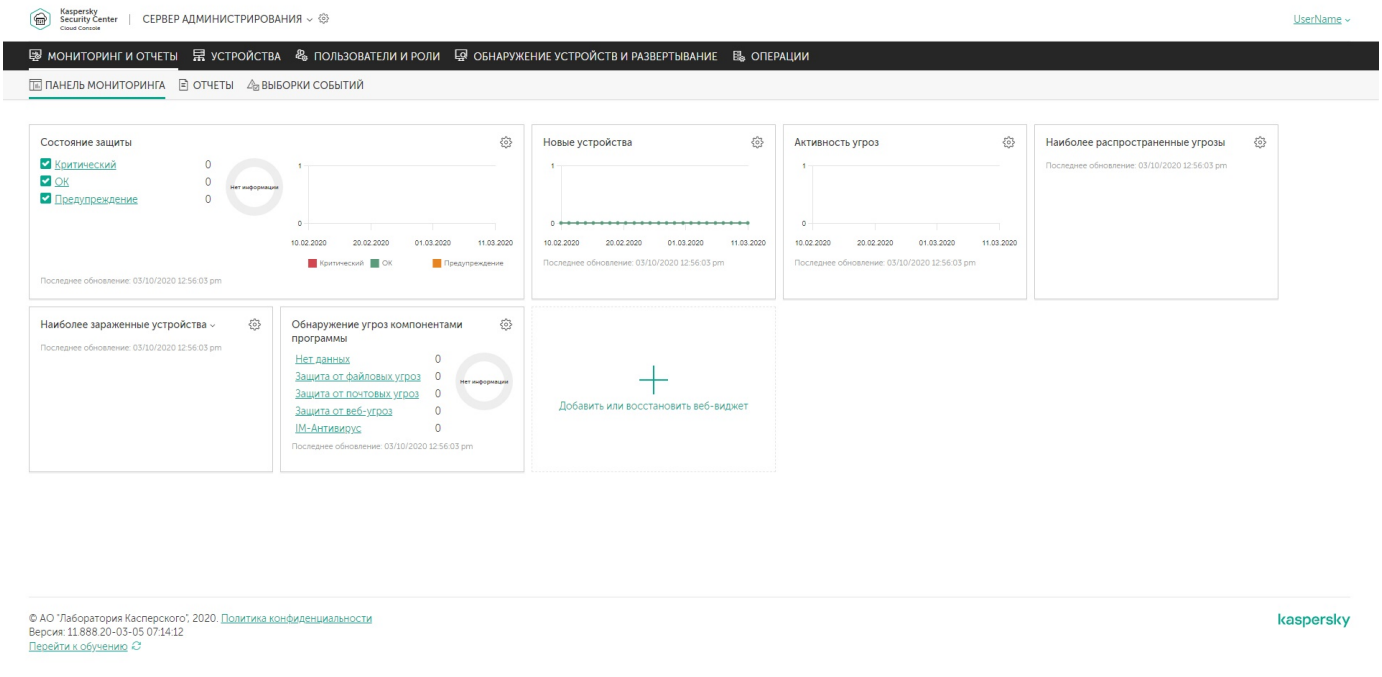
Kaspersky Security Center Web Console (далее также "Web Console") представляет собой программу (веб-приложение), предназначенную для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Web Console является компонентом Kaspersky Security Center, предоставляющим пользовательский интерфейс. Дополнительная информация о Kaspersky Security Center Web Console приведена в документации Kaspersky Security Center.

Kaspersky Security Center Cloud Console (далее также "Cloud Console") представляет собой облачное решение для защиты и контроля сети организации. Дополнительная информация о Kaspersky Security Center Cloud Console приведена в документации Kaspersky Security Center Cloud Console.

С помощью Web Console и Cloud Console вы можете 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 Security Center с помощью Web Console, Cloud Console и Консоли администрирования Kaspersky Security Center отличается. Доступные компоненты и задачи также отличаются в зависимости от типа консоли.



Интерфейс Kaspersky Security Center 12 Web Console

Плагин управления Kaspersky Endpoint Security

Веб-плагин управления Kaspersky Endpoint Security (далее также "*веб-плагин*") обеспечивает взаимодействие Kaspersky Endpoint Security с Kaspersky Security Center 12 Web Console. Веб-плагин позволяет управлять Kaspersky Endpoint Security с помощью следующих инструментов: политики, задачи и локальные параметры программы.

Веб-плагин по умолчанию не установлен в Kaspersky Security Center 12 Web Console. В отличие от плагина управления для Консоли администрирования Kaspersky Security Center, который устанавливается на рабочее место администратора, веб-плагин требуется установить на компьютер с установленной программой Kaspersky Security Center 12 Web Console. При этом функции веб-плагина доступны всем администраторам, у которых есть доступ к Web Console в браузере. Вы можете просмотреть список установленных веб-плагинов в интерфейсе Web Console: **Параметры Консоли** → **Плагины**. Дополнительная информация о совместимости версий веб-плагина и Web Console приведена в документации Kaspersky Security Center.

Установка веб-плагина

> Все необходимые плагины для Kaspersky Security Center Cloud Console устанавливаются по умолчанию. Закладка **Плагин** недоступна в интерфейсе Cloud Console.

Вы можете установить веб-плагин следующими способами:

- Установить веб-плагин с помощью мастера первоначальной настройки Kaspersky Security Center 12 Web Console.

  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 12 Web Console приведена в документации Kaspersky Security Center.

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

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

- Загрузить дистрибутив в Web Console из стороннего источника.

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

Обновление веб-плагина

При появлении новой версии веб-плагина 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 будут 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 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 Web Console: **Параметры Консоли** → **Плагины**. Дистрибутив веб-плагина можно загрузить, например, на веб-сайте "Лаборатории Касперского". Для локальной версии программы также необходимо загрузить текстовый файл, содержащий сигнатуру.

  Вы можете обновить веб-плагин Kaspersky Endpoint Security 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.

Вход и выход из Kaspersky Security Center Web Console

Чтобы войти в Kaspersky Security Center Web Console, необходимо знать веб-адрес Сервера администрирования и номер порта, указанные во время установки (по умолчанию используется порт 8080). Необходимо включить JavaScript в браузере.

Чтобы войти в Kaspersky Security Center Web Console, выполните следующие действия:

1. В браузере перейдите по адресу <Веб-адрес Сервера администрирования>:<Номер порта>.

   Откроется страница входа.

2. Войдите с использованием имени пользователя и пароля локального администратора.

   Если Сервер администрирования не отвечает или вы указали неверные учетные данные, отобразится сообщение об ошибке.

3. После входа отобразится информационная панель с последним используемым языком и темой.

   Если вы вошли в Kaspersky Security Center Web Console впервые, в нижней части экрана отобразится учебник. Можно следовать инструкциям учебника или закрыть его соответствующей кнопкой (X).

Вы можете переходить по страницам Kaspersky Security Center Web Console и работать с ней. Дополнительная информация об интерфейсе Kaspersky Security Center Web Console приведена в документации Kaspersky Security Center .

Чтобы выйти из Kaspersky Security Center Web Console, выполните следующие действия:

1. В правом верхнем углу экрана щелкните по вашему имени пользователя.

2. В контекстном меню выберите пункт **Выход**.

Kaspersky Security Center Web Console закроется и отобразится страница входа.

Для Kaspersky Security Center Cloud Console используйте веб-токен для входа в учетную запись на портале Cloud Console.

Развертывание Kaspersky Endpoint Security

Kaspersky Endpoint Security можно разворачивать на компьютерах в сети организации несколькими способами. Вы можете выбрать наиболее подходящий для вашей организации способ развертывания, а также использовать несколько способов развертывания одновременно. Kaspersky Security Center Web Console поддерживает следующие основные способы развертывания:

- Установка программы с помощью мастера развертывания защиты.

Стандартный метод установки удобен, если вам подходят параметры Kaspersky Endpoint Security, 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 Kaspersky Endpoint Security и гибко управлять задачами удаленной установки. Установка Kaspersky Endpoint Security состоит из следующих этапов:

  1. Создание инсталляционного пакета
  2. Создание задачи удаленной установки

Kaspersky Security Center также поддерживает другие способы установки Kaspersky Endpoint Security, например, развертывание в составе образа операционной системы. Дополнительная информация о других способах развертывания приведена в документации Kaspersky Security Center.

Стандартная установка программы

Для установки программы на компьютерах организации в Kaspersky Security Center Web Console предусмотрен мастер развертывания защиты. Мастер развертывания защиты включает в себя следующие основные действия:

1. Выбор инсталляционного пакета Kaspersky Endpoint Security.

   Инсталляционный пакет – набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы. Инсталляционный пакет Kaspersky Endpoint Security является общим для всех поддерживаемых операционных систем и типов архитектуры процессора.

2. Создание задачи Сервера администрирования Kaspersky Security Center *Удаленная установка программы*.

Чтобы развернуть Kaspersky Endpoint Security,

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

В результате запустится мастер развертывания защиты. Следуйте его указаниям.

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

Шаг 1. Выбор инсталляционного пакета

На этом шаге в списке инсталляционных пакетов выберите пакет Kaspersky Endpoint Security. Если в списке отсутствует инсталляционный пакет Kaspersky Endpoint Security, вы можете создать пакет по кнопке **Добавить**. Для создания инсталляционного пакета вам не нужно искать дистрибутив и сохранять его в память компьютера. В Web Console доступен список дистрибутивов, размещенных на серверах "Лаборатории Касперского", и создание инсталляционного пакета выполняется автоматически. "Лаборатория Касперского" обновляет список после выпуска новых версий программ.

Параметры инсталляционного пакета можно настроить с помощью Web Console.

Шаг 2. Активация программы

На этом шаге добавьте 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 с помощью задачи *Добавить ключ*.

Шаг 3. Выбор Агента администрирования

На этом шаге выберите версию Агента администрирования, который будет установлен вместе с 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 Kaspersky Endpoint Security. Возможны следующие варианты:

Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.

Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. На нераспределенных устройствах не установлен Агент администрирования. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 5. Настройка дополнительных параметров

На этом шаге настройте следующие дополнительные параметры программы:

- **Форсировать загрузку инсталляционного пакета**. 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 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 распределения* – 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 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. Перезагрузка компьютера

На этом шаге выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера. При установке Kaspersky Endpoint Security перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые программы. Также перезагрузка может потребоваться при обновлении версии программы.

Шаг 7. Удаление несовместимых программ

На этом шаге ознакомьтесь со списком несовместимых программ и разрешите удаление этих программ. Если на компьютере установлены несовместимые программы, установка 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 необходимо для применения политик и групповых задач. 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 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 инсталляционного пакета

Инсталляционный пакет – набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы. Инсталляционный пакет Kaspersky Endpoint Security является общим для всех поддерживаемых операционных систем и типов архитектуры процессора.

Kaspersky Security Center Cloud Console не поддерживает создание инсталляционных пакетов из файла.

Чтобы создать инсталляционный пакет, выполните следующие действие:

1. В главном окне Web Console выберите **Обнаружение 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.

Шаг 1. Выбор типа инсталляционного пакета

На этом шаге 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.

Шаг 2. Инсталляционные пакеты

На этом шаге выберите инсталляционный пакет Kaspersky Endpoint Security 11 для Linux. Справа откроется информация о дистрибутиве Kaspersky Endpoint Security. Нажмите на кнопку **Загрузить и создать инсталляционный пакет**. Запустится процесс создания инсталляционного пакета. Во время создания инсталляционного пакета необходимо принять условия Лицензионного соглашения.

Инсталляционный пакет будет создан и добавлен в Web Console. С помощью инсталляционного пакета вы можете установить Kaspersky Endpoint Security на компьютеры сети организации или обновить версию программы. В параметрах инсталляционного пакета можно настроить параметры установки программы (см. таблицу ниже). Инсталляционный пакет содержит антивирусные базы из хранилища Сервера администрирования. Можно обновить базы в инсталляционном пакете, чтобы снизить потребление трафика при обновлении баз после установки Kaspersky Endpoint Security.

Параметры инсталляционного пакета

Раздел	Описание
Параметры программы	**Выбрать язык сервиса**. Установите флажок, чтобы указать языковой стандарт, используемый при работе Kaspersky Endpoint Security. Языковой

	стандарт в формате, определенном в RFC 3066. Если этот параметр не указан, используется языковой стандарт системы по умолчанию. **Активировать программу**. Установите флажок, чтобы указать код активации или лицензионный ключ для активации Kaspersky Endpoint Security.
Источник обновлений	Можно указать источник обновлений: • **Серверы обновлений "Лаборатории Касперского"** • **Сервер администрирования Kaspersky Security Center** • **Другой источник в локальной или глобальной сети**
Параметры установки	**Запустить задачу обновления после установки**. Установите флажок, чтобы запустить задачу обновления после установки Kaspersky Endpoint Security. **Указать 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 графический пользовательский интерфейс**. Установите флажок, чтобы включить использование графического пользовательского интерфейса.

Обновление баз в инсталляционном пакете

Инсталляционный пакет содержит антивирусные базы из хранилища Сервера администрирования, актуальные при создании инсталляционного пакета. После создания инсталляционного пакета вы можете обновлять антивирусные базы в инсталляционном пакете. Это позволяет уменьшить расход трафика на обновление антивирусных баз после установки Kaspersky Endpoint Security.

Чтобы обновить антивирусные базы в хранилище Сервера администрирования, используйте задачу Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования*. Дополнительная информация об обновлении антивирусных баз в хранилище Сервера администрирования приведена в документации Kaspersky Security Center .

Вы можете обновлять базы в инсталляционном пакете только в Консоли администрирования и Kaspersky Security Center Web Console. Обновлять базы в инсталляционном пакете в программе Kaspersky Security Center Cloud Console невозможно.

Чтобы обновить антивирусные базы в инсталляционном пакете, выполните следующие действия:

1. В главном окне Web Console выберите **Обнаружение и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Web Console.

2. Нажмите на название инсталляционного пакета Kaspersky Endpoint Security, в котором вы хотите обновить антивирусные базы.

   Откроется окно свойств инсталляционного пакета.

3. На закладке **Общая информация** нажмите на ссылку **Обновить базы**.

В результате антивирусные 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.

Создание задачи удаленной установки

Чтобы создать задачу удаленной установки, выполните следующие действия:

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, например, `Kaspersky Endpoint Security для отдела Контроля качества`.

4. В разделе **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 Kaspersky Endpoint Security, 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 for Linux.

   Для установки инсталляционных пакетов с помощью Kaspersky Security Center Cloud Console используются точки распространения. Агент администрирования для Linux можно использовать в качестве точки распространения только для загрузки и распространения инсталляционных пакетов.

2. Выберите инсталляционный пакет Агента администрирования.

   Выбранная версия Агента администрирования будет установлена вместе с 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 **Форсировать загрузку инсталляционного пакета** 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.

   - **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 количества запросов к Серверу администрирования для загрузки инсталляционного пакета. Ограничение запросов позволит избежать перегрузки сети.

5. В поле **Количество попыток установки** установите ограничение попыток установить программу. Если установка Kaspersky Endpoint Security 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 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.

8. Если требуется, установите флажок **Предлагать пользователю закрыть работающие программы**. Установка Kaspersky Endpoint Security 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 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. 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 Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 5. 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.

Подготовка программы к работе

После развертывания программы на клиентских компьютерах для работы с Kaspersky Endpoint Security из Kaspersky Security Center Web Console вам нужно выполнить следующие действия:

- Создать и настроить политику.

При помощи политик вы можете установить одинаковые значения параметров работы программы Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования. Мастер первоначальной настройки Kaspersky Security Center Web Console создает политику для Kaspersky Endpoint Security автоматически.

- Создать задачи *Обновление* и *Антивирусная проверка*.

  Задача Обновление требуется для поддержания защиты компьютера в актуальном состоянии. При выполнении задачи Kaspersky Endpoint Security обновляет антивирусные базы и модули программы. Задача Обновление создается автоматически мастером первоначальной настройки Kaspersky Security Center Web Console. Для создания задачи Обновления во время работы мастера установите веб-плагин Kaspersky Endpoint Security 11 для Linux.

  Задача Антивирусная проверка требуется для своевременного обнаружения вирусов и других программ, представляющих угрозу. Необходимо вручную создать задачу Антивирусная проверка.

Чтобы выполнить задачу Антивирусная проверка, выполните следующие действия:

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 **Kaspersky Endpoint Security 11 для Linux**.

   b. В раскрывающемся списке **Тип задачи** выберите **Антивирусная проверка**.

   c. В поле **Название задачи** введите короткое описание, например, `Еженедельная проверка`.

   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.

6. Для настройки расписания выполнения задачи перейдите в свойства задачи.

   Рекомендуется настроить расписание выполнения задачи минимум раз в неделю.

7. Установите флажок напротив задачи. Нажмите на кнопку **Запустить**.

   Вы можете отслеживать статус задачи, количество устройств, на которых задача выполнена успешно или завершилась с ошибкой.

В результате на компьютерах пользователей будет выполняться антивирусная проверка в соответствии с установленным расписанием.

О мастере первоначальной настройки

Мастер первоначальной настройки в Kaspersky Security Center Cloud Console позволяет создать минимальный необходимый набор задач и политик, настроить минимум параметров и запустить создание инсталляционных пакетов для программ "Лаборатории Касперского".

Kaspersky Security Center Cloud Console автоматически предлагает запустить Мастер первоначальной настройки после создания рабочей области компании и первого запуска Kaspersky Security Center Cloud Console. Мастер первоначальной настройки можно запустить вручную в любое время.

Чтобы запустить Мастер первоначальной настройки вручную, выполните следующие действия:

1. В главном окне Kaspersky Security Center Cloud Console щелкните по значку **Настройка** рядом с именем Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Общие**.

3. Выберите пункт **Запустить Мастер первоначальной настройки**.

   Мастер первоначальной настройки можно также запустить, выбрав **Обнаружение и развертывание** → **Развертывание и назначение** → **Мастер первоначальной настройки**.

При повторном запуске Мастера первоначальной настройки задачи и политики, созданные при предыдущем запуске Мастера первоначальной настройки, не создаются повторно.

Наряду с настройкой параметров Сервера администрирования и созданием пакетов, Мастер первоначальной настройки создает следующие политики и базовые запускаемые по требованию задачи для всех установленных плагинов:

- Политика для Kaspersky Endpoint Security 11 для Linux
- Задача Антивирусная проверка
- Задача Контроль целостности системы (только для Kaspersky Security Center Web Console)

- Задача обновления
- Задача Проверка памяти процессов
- Задача Проверка загрузочных секторов

Дополнительная информация о Kaspersky Security Center Cloud Console приведена в документации Kaspersky Security Center Cloud Console.

Активация Kaspersky Endpoint Security

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии. Процедура активации программы заключается в добавлении ключа.

Вы можете активировать программу дистанционно из интерфейса Kaspersky Security Center Web Console следующими способами:

- С помощью задачи *Добавление ключа*.

  Этот способ позволяет добавить ключ на конкретный компьютер или компьютеры, входящие в группу администрирования.

- Путем распространения на компьютеры 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 на Сервер администрирования Kaspersky Security Center. Дополнительная информация о добавлении ключей на Сервер администрирования Kaspersky Security Center приведена в документации Kaspersky Security Center.

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 запускаются по пробной лицензии Kaspersky Security Center Cloud Console автоматически, включая Kaspersky Endpoint Security. При этом активировать Kaspersky Endpoint Security по собственной пробной лицензии по истечении пробной лицензии Kaspersky Endpoint Security 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 вам впоследствии перейти на коммерческую версию. Любое пробное рабочее пространство будет автоматически удалено со всем его содержимым по истечении 30-дневного срока.

Вы можете контролировать использование лицензий следующими способами:

- Просмотреть *Отчет об использовании ключей* в инфраструктуре организации (**Мониторинг и отчеты** → **Отчеты**).
- Просмотреть статусы компьютеров на закладке **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**).

Чтобы активировать программу с помощью задачи Добавить ключ, выполните следующие действия:

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 **Kaspersky Endpoint Security 11 для Linux**.

   b. В раскрывающемся списке **Тип задачи** выберите **Добавить ключ**.

   c. В поле **Название задачи** введите короткое описание, например, `Активация Kaspersky Endpoint Security 11 для Linux`.

   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**.

5. Выберите лицензию, по которой вы хотите активировать программу. Нажмите на кнопку **Далее**.

Вы можете добавлять ключи в Web Console (**Операции** → **Лицензирование**).

6. Ознакомьтесь с информацией о лицензии. Нажмите на кнопку **Далее**.

7. Завершите работу мастера по кнопке **Создать**.

   В списке задач отобразится новая задача.

8. Установите флажок напротив задачи. Нажмите на кнопку **Запустить**.

   В результате на компьютерах пользователей будет активирована программа Kaspersky Endpoint Security.

В свойствах задачи *Добавить ключ* вы можете добавить на компьютер дополнительный ключ. *Дополнительный* ключ становится активным либо по истечении срока годности активного ключа, либо при удалении активного ключа. Наличие дополнительного ключа позволяет избежать ограничения функциональности программы в момент окончания срока действия лицензии.

Чтобы активировать программу путем распространения на компьютеры ключа, размещенного на Сервере администрирования Kaspersky Security Center, выполните следующие действия:

1. В главном окне Web Console выберите **Операции** → **Лицензирование**.

2. Откройте свойства ключа с помощью нажатия на название продукта, к которому относится ключ.

3. Включите переключатель **Распространять ключ автоматически**.

4. Нажмите на кнопку **Сохранить**.

В результате 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**.

Удаление Kaspersky Endpoint Security

Вы можете удалить программу дистанционно с помощью задачи *Удаленная деинсталляция программы*. При выполнении задачи Kaspersky Endpoint Security загрузит на компьютер пользователя утилиту для удаления программы. После завершения удаления программы, утилита будет удалена автоматически.

Чтобы удалить Kaspersky Endpoint Security, выполните следующие действия:

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 12**.

2. В раскрывающемся списке **Тип задачи** выберите **Удаленная деинсталляция программы**.

3. В поле **Название задачи** введите короткое описание, например, `Удаление Kaspersky Endpoint Security на компьютерах Службы технической поддержки`.

4. В разделе **Выбор устройств, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Выбор компьютеров для удаления

На этом шаге выберите компьютеры, на которых будет удалена программа Kaspersky Endpoint Security, в соответствии с выбранным вариантом области действия задачи.

Шаг 3. Настройка параметров удаления программы

На этом шаге настройте параметры удаления программы:

1. Выберите **Удалить управляемую программу**.

2. Выберите программу **Kaspersky Endpoint Security 11 для Linux**.

3. При необходимости укажите режим удаления в разделе **Параметры удаления**.

4. В разделе **Форсировать загрузку утилиты удаления** выберите способ доставки утилиты:

   - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security удаляется средствами Агента администрирования.

- **Средствами Microsoft Windows с помощью Сервера администрирования**. Доставка утилиты 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.

- **Средствами операционной системы с помощью точек распространения**. Утилита 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 справке Kaspersky Security Center.

5. В поле **Максимальное количество одновременных загрузок** установите ограничение количества запросов к Серверу администрирования для загрузки утилиты для удаления программы. Ограничение запросов позволит избежать перегрузки сети.

6. В поле **Количество попыток деинсталляции** установите ограничение попыток удалить программу. Если удаление Kaspersky Endpoint Security завершается с ошибкой, задача автоматически запускает удаление повторно.

7. Если требуется, снимите флажок **Проверять версию операционной системы перед загрузкой**. Это позволит избежать загрузки утилиты деинсталляции, если операционная система компьютера не соответствует программным требованиям. Если вы уверены, что операционная система компьютера соответствует программным требованиям, проверку можно пропустить.

Шаг 4. Выбор учетной записи для доступа к компьютерам

На этом шаге выберите учетную запись для удаления Kaspersky Endpoint Security 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 удаления использует следующую учетную запись. Для удаления Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 5. 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**. Удаление программы будет выполнено в фоновом режиме. После завершения удаления Kaspersky Endpoint Security покажет запрос на перезагрузку компьютера.

Запуск и остановка Kaspersky Endpoint Security

После установки Kaspersky Endpoint Security на компьютер пользователя запуск программы выполняется автоматически. Далее по умолчанию запуск Kaspersky Endpoint Security выполняется сразу после операционной системы. Вы можете контролировать статус работы программы с помощью веб-виджета **Состояние защиты** на закладке **Мониторинг и отчеты**.

Чтобы запустить или остановить Kaspersky Endpoint Security дистанционно, выполните следующие действия:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите запустить или остановить Kaspersky Endpoint Security.

   Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Установите флажок напротив программы **Kaspersky Endpoint Security 11 для Linux**.
5. Нажмите на кнопку **Запустить** или **Остановить**.

Обновление баз и модулей программы

Обновление баз и модулей программы Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули программы.

На компьютерах пользователей обновляются следующие объекты:

- Антивирусные базы. Антивирусные базы включают в себя базы сигнатур вредоносных программ, описание сетевых атак, базы вредоносных и фишинговых веб-адресов, базы баннеров, спам-базы и другие данные.
- Модули программы. Обновление модулей предназначено для устранения уязвимостей в программе и улучшения методов защиты компьютера. Обновления модулей могут менять поведение компонентов программы и добавлять новые возможности.

Kaspersky Endpoint Security поддерживает следующие схемы обновления баз и модулей программы:

- Обновление с серверов "Лаборатории Касперского"

  Серверы обновлений "Лаборатории Касперского" расположены в разных странах по всему миру. Это обеспечивает высокую надежность обновления. Если обновление не может быть выполнено с одного сервера, Kaspersky Endpoint Security переключается к следующему серверу.

- Централизованное обновление.

  Централизованное обновление обеспечивает снижение внешнего интернет-трафика, а также удобство контроля за обновлением.

  Централизованное обновление состоит из следующих этапов:

  1. Загрузка пакета обновлений в хранилище внутри сети организации.

     Загрузку пакета обновлений в хранилище обеспечивает задача Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования*.

  2. Распространение пакета обновлений на клиентские компьютеры.

     Распространение пакета обновлений на клиентские компьютеры обеспечивает задача Kaspersky Endpoint Security 11 для Linux *Обновление*. Вы можете создать неограниченное количество задач обновления для каждой из групп администрирования.

Для Web Console по умолчанию список источников обновлений содержит Сервер администрирования Kaspersky Security Center и серверы обновлений "Лаборатории Касперского". Для Kaspersky Security Center Cloud Console по умолчанию список источников обновлений содержит точки распространения и серверы обновлений "Лаборатории Касперского". Дополнительная информация о точках распространения приведена в документации Kaspersky Security Center Cloud Console. Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений можно указать HTTP, HTTPS и FTP-серверы. Если обновление не может быть выполнено с одного источника обновлений, Kaspersky Endpoint Security переключается к следующему.

Загрузка обновлений с серверов обновлений "Лаборатории Касперского" или с других FTP- или HTTP-серверов осуществляется по стандартным сетевым протоколам. Если для доступа к источникам обновлений требуется подключение к прокси-серверу, укажите параметры прокси-сервера в параметрах политики Kaspersky Endpoint Security.

Обновление с серверного хранилища

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы на компьютерах локальной сети организации с серверного хранилища. Для этого Kaspersky Security Center должен загружать пакет обновлений в хранилище (FTP, HTTP или HTTPS-сервер, сетевая или локальная директория) с серверов обновлений "Лаборатории Касперского". В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений с серверного хранилища.

Настройка обновления баз и модулей программы с серверного хранилища состоит из следующих этапов:

1. Настройка перемещения пакета обновлений в хранилище на Сервере администрирования (задача *Загрузка обновлений в хранилище Сервера администрирования*).

2. Настройка обновления баз и модулей программы из указанного серверного хранилища на остальных компьютерах локальной сети организации (задача *Обновление*).

Чтобы настроить загрузку пакета обновлений в серверное хранилище, выполните следующие действия:

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. Выберите задачу **Загрузка обновлений в хранилище Сервера администрирования**.

   Откроется окно свойств задачи.

   Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически мастером первоначальной настройки Kaspersky Security Center Web Console и может существовать только в единственном экземпляре.

3. Выберите закладку **Параметры программы**.

4. В разделе **Прочие параметры** нажмите на кнопку **Настроить**.

5. В поле **Папка для хранения обновлений** укажите адрес FTP, HTTP или HTTPS-сервера, сетевой или локальной директории, в которую Kaspersky Security Center копирует пакет обновлений, полученный с серверов обновлений "Лаборатории Касперского".

   Формат пути для источника обновлений следующий:

   - Для FTP- или HTTP-сервера введите веб-адрес или IP-адрес сайта.

     Например, `http://dnl-01.geo.kaspersky.com/` или `93.191.13.103`.

     Для FTP-сервера укажите параметры аутентификации в адресе в формате `ftp://<имя пользователя>:<пароль>@<узел>:<порт>`.

   - Для сетевой или локальной директории введите полный путь к директории.

6. Нажмите **ОК**.

7. Подтвердите изменения по кнопке **Сохранить**.

Чтобы настроить обновление Kaspersky Endpoint Security из указанного серверного хранилища, выполните следующие действия:

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. Выберите задачу **Обновление** для Kaspersky Endpoint Security.

   Откроется окно свойств задачи.

Задача *Обновление* создается автоматически мастером первоначальной настройки Kaspersky Security Center Web Console. Для создания задачи *Обновления* во время работы мастера установите веб-плагин Kaspersky Endpoint Security 11 для Linux.

3. Перейдите на закладку **Параметры программы** → **Источник обновлений баз**.
4. Выберите вариант **Другие источники в локальной или глобальной сети**.
5. В списке источников обновлений нажмите на кнопку **Добавить**.
6. В поле **Источник обновлений** укажите адрес FTP, HTTP или HTTPS-сервера, сетевой или локальной директории, в которую Kaspersky Security Center копирует пакет обновлений, полученный с серверов обновлений "Лаборатории Касперского".

   Адрес источника должен совпадать с адресом, указанный ранее в поле **Папка для хранения обновлений** при настройке загрузки обновлений в серверное хранилище (см. инструкцию выше).

7. Установите флажок **Использовать этот источник**. Нажмите **ОК**.
8. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.
9. Нажмите на кнопку **Сохранить**.

Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

Обновление с помощью Kaspersky Update Utility

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы на компьютерах локальной сети организации из общей директории с помощью утилиты Kaspersky Update Utility. Для этого один из компьютеров локальной сети организации должен получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или серверов обновлений "Лаборатории Касперского" и копировать полученные пакеты обновлений в общую директорию с помощью утилиты. В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений из общей директории.

Настройка обновления баз и модулей программы из общей директории состоит из следующих этапов:

1. Установка Kaspersky Update Utility на одном из компьютеров локальной сети организации.
2. Настройка копирования пакета обновлений в общую директорию в параметрах Kaspersky Update Utility.

3. Настройка обновления баз и модулей программы из указанной общей директории на остальных компьютерах локальной сети организации.

Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта службы технической поддержки "Лаборатории Касперского". После установки утилиты выберите источник обновлений (например, хранилище Сервера администрирования) и общую директорию, в которую Kaspersky Update Utility будет копировать пакеты обновлений. Дополнительная информация о работе с Kaspersky Update Utility приведена в Базе знаний "Лаборатории Касперского".

Чтобы настроить обновление из общей директории, выполните следующие действия:

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

   Откроется окно свойств задачи.

   Задача *Обновление* создается автоматически мастером первоначальной настройки Kaspersky Security Center Web Console. Для создания задачи Обновления во время работы мастера установите веб-плагин Kaspersky Endpoint Security 11 для Linux.

3. Перейдите на закладку **Параметры программы** → **Источник обновлений баз**.

4. Выберите вариант **Другие источники в локальной или глобальной сети**.

5. В списке источников обновлений нажмите на кнопку **Добавить**.

6. В поле **Источник обновлений** укажите путь к общей директории.

   Адрес источника должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.

7. Нажмите **ОК**.

8. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

9. Нажмите на кнопку **Сохранить**.

Использование прокси-сервера при обновлении

Для загрузки обновлений баз и модулей программы из источника обновлений может потребоваться указать параметры прокси-сервера. Если источников обновлений несколько, параметры прокси-сервера применяются для всех источников. Если для некоторых источников обновлений прокси-сервер не нужен, вы можете выключить использование прокси-сервера в свойствах политики. Kaspersky Endpoint Security также будет использовать прокси-сервер для доступа к Kaspersky Security Network и серверам активации.

Чтобы настроить подключение к источникам обновлений через прокси-сервер, выполните следующие действия:

1. В главном окне Web Console нажмите ⚙.

   Откроется окно свойств Сервера администрирования.

2. Перейдите в раздел **Настройка доступа в интернет**.

3. Установите флажок **Использовать прокси-сервер**.

4. Настройте параметры подключения к прокси-серверу: адрес прокси-сервера, порт и параметры аутентификации (имя пользователя и пароль).

5. Нажмите на кнопку **Сохранить**.

Чтобы выключить использование прокси-сервера для определенной группы администрирования, выполните следующие действия:

1. В главном окне Web Console выберите закладку **Устройства** → **Политики и профили**.

2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите выключить использование прокси-сервера.

   Откроется окно свойств политики.

3. Выберите закладку **Параметры программы**.

4. Перейдите в раздел **Общие параметры** → **Параметры прокси-сервера**.

5. Выберите вариант **Не использовать прокси-сервер**.

6. Нажмите **ОК**.

7. Подтвердите изменения по кнопке **Сохранить**.

Просмотр состояния защиты устройства

Чтобы просмотреть состояние защиты устройства, выполните следующие действия:

1. В Kaspersky Security Center Web Console откройте список управляемых устройств (**Устройства** → **Управляемые устройства**).

2. В списке выберите требуемое устройство, чтобы просмотреть о нем подробную информацию.

   Откроется окно, содержащее общую информацию о выбранном устройстве.

3. Откройте закладку **Защита** (**Общие** → **Защита**).

На закладке **Защита** отображается следующая информация о выбранном устройстве:

- **Видимость** – видимость выбранного устройства в сети.
- **Статус** – текущий статус выбранного устройства: *OK*, *Критический* или *Предупреждение*.
- **Описание статуса** – причины смены выбранного статуса устройства на *Критический* или *Предупреждение*.

  Статус устройства меняется на *Критический*, если не запущена задача Контроль целостности системы.

  Статус устройства меняется на *Предупреждение*, если требуется перезапуск программы или перезагрузка операционной системы. После перезапуска статус устройств меняется на *OK*.

  Дополнительная информация об изменении статуса приведена в документации Kaspersky Security Center .
- **Статус 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.
- **Объектов, 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 задачами

Kaspersky Security Center Web Console управляет работой программы Kaspersky Endpoint Security, установленной на компьютерах, с помощью задач. Задачи реализуют основные функции управления, например, добавлений ключей, проверку объектов, обновление баз и модулей программы.

Для управления Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console можно создавать следующие типы задач:

- локальные задачи, определенные для отдельного компьютера;
- групповые задачи, определенные для компьютеров, входящих в группы администрирования;
- задачи для наборов компьютеров, не входящих в группы администрирования.

> Задачи для наборов компьютеров, не входящих в группы администрирования, выполняются только для указанных в параметрах задачи компьютеров. Если в набор компьютеров, для которого сформирована задача, добавлены новые компьютеры, то для них эта задача не выполняется. В этом случае вам нужно создать новую задачу или изменить параметры уже существующей задачи.

Вы можете создавать задачи следующих типов:

- **Антивирусная проверка**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи.
- **Контроль целостности системы по требованию**. В процессе выполнения этой задачи изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы (недоступно для Kaspersky Security Center Cloud Console).
- **Проверка контейнеров**. При выполнении этой задачи программа проверяет Docker-контейнеры и Docker-образы на вирусы и другие вредоносные объекты. Можно одновременно запустить несколько пользовательских задач Проверка контейнеров (недоступно для Kaspersky Security Center Cloud Console).
- **Добавление ключа**. В процессе выполнения задачи Kaspersky Endpoint Security добавляет ключ, в том числе дополнительный, для активации программы.
- **Обновление**. В процессе выполнения задачи Kaspersky Endpoint Security обновляет антивирусные базы в соответствии с установленными параметрами обновления.
- **Откат обновлений**. В процессе выполнения задачи Kaspersky Endpoint Security откатывает последнее обновление антивирусных баз.

- **Проверка памяти процессов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет системную память компьютера.
- **Проверка загрузочных секторов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет загрузочные сектора компьютера.

Задачи выполняются, только если на компьютерах запущена программа Kaspersky Endpoint Security.

Вы можете выполнять следующие действия над задачами:

- Создавать новые задачи.
- Изменять параметры задач.
- Управлять задачами.

Права на доступ к параметрам задач Kaspersky Endpoint Security (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через параметры доступа к функциональным областям Kaspersky Endpoint Security. Для настройки прав доступа к параметрам функциональных областей Kaspersky Endpoint Security, перейдите в раздел Безопасность окна свойств Сервера администрирования Kaspersky Security Center.

Общая информация о задачах в Kaspersky Security Center Web Console приводится в документации для Kaspersky Security Center.

Создание задачи

Чтобы создать задачу, выполните следующие действия:

1. На главной странице Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится **Мастер создания задачи**.
3. Настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Security 11 для Linux**.

   b. В раскрывающемся списке **Тип задачи** выберите задачу, которую вы хотите запустить на компьютерах пользователей.

c. В поле **Название задачи** введите короткое описание, например, `Обновление программы для бухгалтерии`.

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 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**). Дополнмительная 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, выполните следующие действия:

1. На главной странице Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Задачи**.

2. В списке задач выберите задачу, параметры которой вы хотите изменить.

3. Измените параметры задачи.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Задача будет сохранена с обновленными параметрами.

Управление задачами

Чтобы запустить, приостановить, возобновить, остановить, удалить, скопировать или переместить задачу, выполните следующие действия:

1. На главной странице Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Задачи**.

2. В списке задач выберите задачи, которые вы хотите запустить, приостановить, возобновить, остановить, удалить, скопировать или переместить, и нажмите на соответствующую кнопку (если она доступна).

Параметры задачи

Для работы с Kaspersky Endpoint Security через Kaspersky Security Center 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.

Антивирусная проверка

Антивирусная проверка – это однократная полная или выборочная проверка файлов на компьютере, выполняемая Kaspersky Endpoint Security. Kaspersky Endpoint Security может выполнять несколько задач антивирусной проверки одновременно.

По умолчанию в Kaspersky Endpoint Security создается одна стандартная задача антивирусной проверки – полная проверка. Программа проверяет все объекты, расположенные на локальных дисках компьютера, а также все смонтированные и разделяемые объекты, доступ к которым предоставляется по протоколам Samba и NFS, с рекомендуемыми параметрами безопасности.

Пользователи могут создавать пользовательские задачи антивирусной проверки.

По умолчанию в Kaspersky Endpoint Security также создается стандартная пользовательская задача антивирусной проверки.

Если программа была перезапущена контрольной службой или вручную пользователем во время антивирусной проверки, выполнение задачи прерывается. В журнале программы сохраняется событие *OnDemandTaskInterrupted*.

Параметр	Описание
Приоритет задачи	В этом разделе можно задать приоритет задачи проверки: • **Фоновая проверка** – задача выполняется с низким приоритетом (выполнение задачи занимает больше времени, но программа выделяет ресурсы на выполнение других задач). • **Нормальный** – задача выполняется с нормальным приоритетом. Выберите этот вариант, если важно время выполнения проверки. По умолчанию выбран вариант **Фоновая проверка**.
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, Kaspersky Endpoint Security проверяет архивы. Программа обнаруживает зараженные объекты в архивах, но не лечит их. Выберите этот вариант для более детальной проверки. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Можно уменьшить продолжительность проверки архивов, включив и настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)**. Если флажок снят, Kaspersky Endpoint Security 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, 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 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, 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.
Прервать проверку, если она длится более (сек.)	Поле, в котором можно 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: `0`
Пропускать объекты размером более (МБ)	Поле, в котором можно указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0` – `999 999`. 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.
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 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** – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов. По умолчанию выбран вариант **Рекомендованный**.

Действия над зараженными объектами	В этом разделе можно выбрать действия, которые Kaspersky Endpoint Security выполняет над обнаруженным зараженным объектом. В первом раскрывающемся списке можно выбрать действие, которое будет выполняться первым: • **Лечить** объект. • **Удалять** объект. • **Пропускать** объект. • **Выполнять рекомендуемое действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. По умолчанию выбран вариант **Выполнять рекомендуемое действие**. Если первое действие выполнить не удалось, программа выполняет второе действие, которое можно выбрать во втором раскрывающемся списке. 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 `Удалить`, программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.
Области проверки	Таблица, содержащая объекты, проверяемые задачей Антивирусная проверка. Области проверки в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.

В разделе **Области исключений** для задачи Антивирусная проверка можно также настроить области исключений, исключения по маске и по названию угрозы.

Контроль целостности системы по требованию

Задача Контроль целостности системы, выполняемая по требованию, доступна только для Kaspersky Security Center Web Console.

В процессе выполнения задачи Контроль целостности системы по требованию изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве *снимка состояния системы*.

Вы можете создать несколько задач ODFIM.

Снимок состояния системы

Снимок состояния системы определяется во время первого выполнения задачи ODFIM на компьютере. 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, Kaspersky Endpoint Security создает событие о нарушении целостности системы.

Вы можете заново создать снимок состояния системы для задачи с помощью соответствующего параметра. Снимок состояния системы создается заново после завершения задачи ODFIM.

Снимок состояния системы также создается при изменении параметров задачи, например, при добавлении новой области мониторинга. При следующем выполнении задачи снимок состояния системы формируется заново.

Задача ODFIM создает хранилище для снимков состояния системы на компьютере с установленным компонентом Контроль целостности системы.

Удалить снимок состояния системы можно, удалив соответствующую задачу ODFIM.

Параметры задачи Контроль целостности системы

Параметр	Описание
Обновлять снимок состояния системы при каждом запуске задачи	Этот флажок включает или выключает обновление снимка состояния системы при каждом запуске задачи Контроль целостности системы. Если флажок установлен, Kaspersky Endpoint Security обновляет снимок состояния системы при каждом запуске задачи Контроль целостности системы. Если флажок снят, Kaspersky Endpoint Security не обновляет снимок состояния системы при каждом запуске задачи Контроль целостности системы.

	По умолчанию флажок снят.
Использовать хеш (SHA-256) для проверки	Флажок включает или выключает использование хеша SHA-256 для задачи Контроль целостности системы. SHA-256 – это криптографическая хеш-функция, которая формирует 256-разрядное хеш-значение. 256-разрядное хеш-значение представляет собой последовательность из 64 шестнадцатеричных цифр. Если флажок установлен, Kaspersky Endpoint Security использует хеш SHA-256 для задачи Контроль целостности системы. Если флажок снят, Kaspersky Endpoint Security не использует хеш SHA-256 для задачи Контроль целостности системы. По умолчанию флажок снят.
Отслеживать директории в областях мониторинга	Флажок включает или выключает контроль указанных директорий во время выполнения задачи Контроль целостности системы. Если флажок установлен, Kaspersky Endpoint Security отслеживает указанные директории во время выполнения задачи Контроль целостности системы. Если флажок снят, Kaspersky Endpoint Security не отслеживает указанные директории во время выполнения задачи Контроль целостности системы. По умолчанию флажок снят.
Проверять время последнего доступа к файлу	Флажок включает или выключает отслеживание времени доступа задачи Контроль целостности системы. Если флажок установлен, Kaspersky Endpoint Security отслеживает время доступа задачи Контроль целостности системы. Если флажок снят, Kaspersky Endpoint Security не отслеживает время доступа задачи Контроль целостности системы. По умолчанию флажок снят.
Области мониторинга	Содержит объекты, контролируемые задачей Контроль целостности системы. По умолчанию таблица содержит область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/). Области проверки в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.

В разделе **Области исключений** для задачи Контроль целостности системы, выполняемой по требованию, можно также настроить исключения из мониторинга и исключения по маске.

Проверка контейнеров

Задача Проверка контейнеров доступна только для Kaspersky Security Center Web Console.

Во время работы пользовательской задачи Сканирование контейнеров программа проверяет Docker-контейнеры и образы на вирусы и вредоносные программы. Можно одновременно запустить несколько пользовательских задач Сканирование контейнеров.

Параметры задачи Проверка контейнеров

Параметр	Описание
Приоритет задачи	В этом разделе можно задать приоритет задачи проверки: • **Фоновая проверка** – задача выполняется с низким приоритетом (выполнение задачи занимает больше времени, но программа выделяет ресурсы на выполнение других задач). • **Нормальный** – задача выполняется с нормальным приоритетом. Выберите этот вариант, если важно время выполнения проверки. По умолчанию выбран вариант **Фоновая проверка**.
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, Kaspersky Endpoint Security проверяет архивы. Программа обнаруживает зараженные объекты в архивах, но не лечит их. Выберите этот вариант для более детальной проверки. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Можно уменьшить продолжительность проверки архивов, включив и настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)**. Если флажок снят, Kaspersky Endpoint Security 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, 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 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, 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.
Прервать проверку, если она длится более (сек.)	Поле, в котором можно 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: `120`
Пропускать объекты размером более (МБ)	Поле, в котором можно указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0` – `999 999`. 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.
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 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** – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов. По умолчанию выбран вариант **Рекомендованный**.
Действия над зараженными объектами	В этом разделе можно выбрать действия, которые Kaspersky Endpoint Security выполняет над обнаруженным зараженным объектом. В первом раскрывающемся списке можно выбрать действие, которое будет выполняться первым: • **Лечить** объект. • **Удалять** объект. • **Пропускать** объект. • **Выполнять рекомендуемое действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. По умолчанию выбран вариант **Выполнять рекомендуемое действие**. Если первое действие выполнить не удалось, программа выполняет второе действие, которое можно выбрать во втором раскрывающемся списке.
Проверить Docker-контейнеры	Флажок включает или выключает проверку Docker-контейнеров. Если флажок установлен, можно указать имя или маску имени проверяемых Docker-контейнеров. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых Docker-контейнеров. По умолчанию указана маска * – выполняется проверка всех Docker-контейнеров.

Действие при обнаружении угрозы	В этом разделе можно выбрать действие, выполняемое при обнаружении зараженного объекта во время поверки: • **Пропустить** и не выполнять никаких действий над Docker-контейнером при обнаружении зараженного объекта. • **Остановить Docker-контейнер** при обнаружении зараженного объекта. • **Остановить Docker-контейнер, если не удалось вылечить объект или устранить угрозу** – если не удалось вылечить зараженный объект, Docker-контейнер останавливается. По умолчанию выбрано действие **Остановить Docker-контейнер, если не удалось вылечить объект или устранить угрозу**.
Проверить Docker-образы	Флажок включает или выключает проверку Docker-образов. Если флажок установлен, можно указать имя или маску имени проверяемых Docker-образов. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых Docker-образов. По умолчанию указана маска * – выполняется проверка всех Docker-образов.
Действие при обнаружении угрозы	В этом разделе можно выбрать действие, выполняемое при обнаружении зараженного объекта во время поверки: • **Пропустить угрозу** и не выполнять никаких действий над Docker-образом при обнаружении зараженного объекта. • **Удалить Docker-образ** при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные Docker-контейнеры будут остановлены, а затем удалены. По умолчанию выбран вариант **Пропустить угрозу**.
Проверять все слои	Флажок включает или выключает проверку всех слоев образов и запущенных Docker-контейнеров. По умолчанию флажок установлен.

В разделе **Области исключений** для задачи Проверка контейнеров можно также настроить исключения по маске и по названию угрозы.

Добавление ключа

Можно добавить ключ активации Kaspersky Endpoint Security, включая дополнительный ключ.

Параметры задачи Добавление ключа

Параметр	Описание
Использовать ключ в качестве дополнительного	Флажок включает или выключает использование ключа в качестве дополнительного. Если флажок установлен, Kaspersky Endpoint Security использует ключ в качестве дополнительного. Если флажок снят, Kaspersky Endpoint Security использует ключ в качестве активного. По умолчанию флажок снят. Флажок недоступен, если вы добавляете ключ для пробной лицензии или ключ по подписке. Невозможно использовать ключ для пробной лицензии и ключ по подписке в качестве дополнительного ключа.
Информация о лицензии	В этом разделе приведены данные о ключе и соответствующей ему лицензии: • **Ключ** – уникальная буквенно-цифровая последовательность. Ключ обеспечивает использование программы в соответствии с условиями Лицензионного соглашения (типом лицензии, сроком действия лицензии, лицензионными ограничениями). Вы можете использовать программу только при наличии в ней ключа. • **Тип лицензии** – пробная, коммерческая или коммерческая (подписка). • **Срок действия лицензии** – срок использования программы, указанный в Лицензионном сертификате (например, 365 дней). Информация не отображается, если вы используете программу по подписке. • **Действует до** – дата окончания срока годности ключа. Активировать программу путем добавления этого ключа и использовать программу по соответствующей лицензии. Если вы используете программу по неограниченной подписке, дата окончания срока годности ключа не указывается. • **Ограничение** – максимальное количество серверов, которые программа может защищать. • **Название программы** – название программы, для которой вы добавляете ключ.

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 Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули программы.

Параметры задач обновления

Параметр	Описание
Источник обновлений баз	В этом разделе можно выбрать источник обновлений: • **Серверы обновлений "Лаборатории Касперского"**, на которых публикуются обновления баз для программ "Лаборатории Касперского". • **Сервер администрирования Kaspersky Security Center** доступен только для Kaspersky Security Center Web Console. • **Точки распространения** доступны 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. По умолчанию выбран вариант **Серверы обновлений "Лаборатории Касперского"**.
Игнорировать параметры прокси для серверов обновлений "Лаборатории Касперского"	Флажок включает или выключает игнорирование параметров прокси для пользовательских источников обновлений. По умолчанию флажок снят.
Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны	Флажок включает или выключает функцию использования 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.
Игнорировать параметры прокси для пользовательских источников обновлений	Флажок включает или выключает игнорирование параметров прокси для пользовательских источников обновлений. Флажок доступен, если выбран вариант **Другие источники в локальной или глобальной сети**. Включите этот вариант, если вы не хотите использовать прокси-сервер для подключения к пользовательским источникам обновлений. По умолчанию флажок снят.
Пользовательские источники обновлений	В таблице содержится список пользовательских источников обновлений баз. В процессе обновления Kaspersky Endpoint Security обращается к источникам обновлений в том порядке, в котором эти ресурсы указаны в списке источников обновлений. Таблица содержит следующие графы: • **Источник обновлений** – HTTP, HTTPS или FTP-серверы или директории на серверах локальной сети. • **Использовать этот источник** – показывает, будет ли источник использоваться в задаче (**Используется** или **Не используется**). Переключатель можно включить в таблице или в окне **Источник обновлений** (открывается при нажатии на кнопку **Добавить** или **Изменить**). 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.

В разделе **Параметры** можно указать время ожидания ответа и параметры загрузки обновлений программы.

Дополнительные параметры задачи обновления

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 обновления программы	В раскрывающемся списке **Режим обновления программы** вы можете выбрать режим обновления Kaspersky Endpoint Security: • **Не загружать** файлы обновлений. Обновить программу невозможно. • **Только загрузить** файлы обновлений, но не устанавливать их на компьютеры пользователей. • **Загрузить и установить** файлы обновлений на компьютеры пользователей. По умолчанию выбрано действие **Только загрузить**.

Откат обновлений

После первого обновления баз программы становится доступна функция отката баз программы к их предыдущей версии.

Каждый раз, когда пользователь запускает процесс обновления, Kaspersky Endpoint Security создает резервную копию текущих баз программы. Это позволяет при необходимости откатить базы программы до предыдущей версии. Откат последних обновлений используется, например, если новая версия баз программы содержит недопустимые сигнатуры, что приводит к блокировке безопасных программ со стороны Kaspersky Endpoint Security.

Задача Откат обновления баз не имеет параметров.

Проверка памяти процессов

Задача Проверка памяти процессов позволяет проверять память процессов и память ядра без указания области проверки.

Параметры задачи Проверка памяти процессов

Параметр	Описание
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 файлах	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.
Действия над зараженными объектами	В этом разделе можно выбрать действия, которые Kaspersky Endpoint Security выполняет над обнаруженным зараженным объектом: • **Лечить** объект. • **Пропускать** объект. По умолчанию выбран вариант **Лечить**.

В разделе **Области исключений** для задачи Проверка памяти процессов можно также настроить исключения по названию угрозы.

Проверка загрузочных секторов

Задача Проверка загрузочных секторов позволяет проверять память процессов и память ядра без указания области проверки.

Параметры задачи Проверка загрузочных секторов

Параметр	Описание
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 файлах	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.
Области проверки	В этом разделе можно настроить области проверки для задачи Проверка загрузочных секторов. При переходе по ссылке **Настроить области проверки** открывается окно **Области проверки**. В этом окне можно указать устройства, загрузочные секторы которых требуется проверять.
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** – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов. По умолчанию выбран вариант **Рекомендованный**.
Действия над зараженными объектами	В этом разделе можно выбрать действия, которые Kaspersky Endpoint Security выполняет над обнаруженным зараженным объектом: • **Лечить** объект. • **Пропускать** объект. По умолчанию выбран вариант **Лечить**.

В разделе **Области исключений** для задачи Проверка загрузочных секторов можно также настроить исключения по маске и по названию угрозы.

Управление политиками

Политика – это набор параметров работы программы, определенный для группы администрирования. В политике задаются не все параметры программы.

Для одной программы можно настроить несколько политик с различными значениями параметров. Однако одновременно для программы может быть только одна активная политика в пределах группы администрирования. При создании новой политики все остальные политики в группе администрирования становятся неактивными. Статус политики можно изменить позже.

При помощи политик вы можете установить одинаковые значения параметров работы программы Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования.

Вы можете локально изменять значения параметров, заданные политикой, для отдельных компьютеров в группе администрирования при помощи Kaspersky Endpoint Security. Вы можете изменять локально только те параметры, изменение которых не запрещено политикой.

Возможность изменять параметр программы на клиентском компьютере определяется статусом "замка" у параметра в политике:

- Если параметр закрыт "замком" ( ), это означает, что вы не можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используется значение параметра, заданное политикой.

- Если параметр не закрыт "замком" ( ), это означает, что вы можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используются значения параметра, установленные локально. Значение параметра, установленное в политике, не применяется.

Локальные параметры программы изменяются в соответствии с параметрами политики после первого применения политики.

Права на доступ к параметрам политики (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, и отдельно для каждой функциональной области Kaspersky Endpoint Security. Для настройки прав доступа к параметрам политики перейдите в раздел Безопасность окна свойств Сервера администрирования Kaspersky Security Center.

Вы можете выполнять следующие действия над политикой:

- Создавать политику.

- Изменять параметры политики.

Если учетная запись пользователя, под которой вы осуществили доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Удалять политику.
- Изменять состояние политики.

Дополнительная информация о политиках приведена в документации Kaspersky Security Center.

Создание политики

Чтобы создать политику, выполните следующие действия:

1. На главной странице Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Политики и профили**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Выбор программы**.
3. Выберите инсталляционный пакет **Kaspersky Endpoint Security 11 для Linux** и нажмите на кнопку **Далее**.
4. Ознакомьтесь с Положением о Kaspersky Security Network и выполните одно из следующих действий:
   - Выберите **Я соглашаюсь использовать Kaspersky Security Network**, чтобы включить Kaspersky Security Network на компьютерах, управляемых созданной политикой.
   - Выберите **Я не соглашаюсь использовать Kaspersky Security Network**, чтобы отключить Kaspersky Security Network на компьютерах, управляемых созданной политикой.

   Отказ от участия в Kaspersky Security Network не прерывает процесс обновления создания политики. В любой момент можно включить, выключить или изменить режим Kaspersky Security Network для управляемых компьютеров в параметрах политики.
5. Нажмите на кнопку **Далее**.

   Откроется окно параметров созданной политики на закладке **Общие**.

6. На закладке **Общие** можно настроить следующие параметры политики:

   - Название политики по умолчанию.
   - 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. По умолчанию выбран этот вариант.
     - **Форсировать наследование параметров дочерними политиками**. Если выбран этот вариант, параметры дочерних политик недоступны для изменения. По умолчанию этот вариант не выбран.

   Дополнительная информация о параметрах политик приведена в документации Kaspersky Security Center.

7. На закладке **Параметры программы** можно изменить параметры Kaspersky Endpoint Security.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить политику.

Политика появится в списке политик. Параметры политики можно изменить позже. Дополнительная информация об управлении политиками приведена в документации Kaspersky Security Center.

Изменение параметров политики

Чтобы изменить параметры политики, выполните следующие действия:

1. На главной странице Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Политики и профили**.
2. В списке политик выберите политику, параметры которой вы хотите изменить.

   Дополнительная информация об общих параметрах политик приведена в документации Kaspersky Security Center .
3. Измените параметры политики.
4. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Политика будет сохранена с обновленными параметрами.

Удаление политики

Чтобы удалить политику, выполните следующие действия:

1. На главной странице Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Политики и профили**.
2. В списке политик установите флажок рядом с названием политики, которую требуется удалить.

   Можно одновременно выбрать несколько политик для удаления.
3. Нажмите на кнопку **Удалить**.
4. Нажмите **ОК**.

Политика будет удалена.

Изменение статуса политики

Чтобы изменить статус политики, выполните следующие действия:

1. На главной странице Kaspersky Security Center Web Console, на закладке **Устройства** выберите **Политики и профили**.
2. В списке политик выберите политику, статус которой вы хотите изменить.
3. На закладке **Общие** в разделе **Статус политики** выберите требуемый 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.

Параметры политики

Политику можно использовать для настройки параметров Kaspersky Endpoint Security. Подробная информация о компонентах программы приведена в соответствующих подразделах.

Набор и значения по умолчанию для параметров политики могут отличаться в зависимости от типа лицензии на программу.

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).

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.

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 "Лаборатории Касперского" (https://www.kaspersky.ru/products-and-services-privacy-policy). Файл с текстом Положения о Kaspersky Security Network входит в комплект поставки программы.

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа 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 .

Настроить параметры KSN Proxy можно в свойствах политики Kaspersky Security Center.

Участие в Kaspersky Security Network является добровольным. Программа предлагает участвовать в KSN во время установки. Начать или прекратить использование KSN можно в любой момент.

Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью	Выбирая этот вариант, вы подтверждаете, что хотите участвовать в Kaspersky Security Network и полностью прочитали, поняли и

прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	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.
Подробнее	При переходе по ссылке открывается веб-сайт "Лаборатории Касперского".
Не участвовать в Kaspersky Security Network	Выбрав этот параметр, вы отказываетесь от участия в Kaspersky Security Network.
Kaspersky Security Network со статистикой	Выбрав этот параметр, 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	Выбрав этот параметр, 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. По умолчанию выбран этот вариант.
Текст Положения о Kaspersky Security Network	При переходе по ссылке открывается окно **Положение о Kaspersky Security Network**. В этом окне вы можете просмотреть текст Положения о Kaspersky Security Network.

Закладка Параметры программы

На закладке **Параметры программы** можно выбрать набор параметров, для которых требуется изменить параметров политики.

Разделы

Раздел	Описание

Базовая защита	Защита от файловых угроз Исключения из проверки Управление сетевым экраном Защита от веб-угроз Защита от сетевых угроз
Продвинутая защита	Kaspersky Security Network Защита от шифрования Контроль целостности системы (только для Kaspersky Security Center Web Console) Контроль устройств Анализ поведения
Локальные задачи	Управление задачами Проверка съемных дисков
Общие параметры	Параметры прокси-сервера Параметры программы Параметры перехватчика Параметры сети Исключенные точки монтирования Хранилища

Защита от файловых угроз

Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. Задача Защита от файловых угроз создается автоматически с параметрами по умолчанию при установке Kaspersky Endpoint Security на компьютер. По умолчанию задача Защита от файловых угроз запускается автоматически при старте Kaspersky Endpoint Security. Задача постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы.

Во время работы задачи Защита от файловых угроз Kaspersky Endpoint Security выполняет проверку всех пространств имен во всех поддерживаемых операционных системах, если в общих параметрах программы для параметра `NamespaceMonitoring` задано значение `Yes` или в Web Console включен параметр **Мониторинг пространств имен и Docker-контейнеров** (**Параметры политики** → **Общие параметры** → **Параметры перехватчика**).

Дополнительно для операционной системы Astra Linux пользовательская задача антивирусной проверки (Scan_File) позволяет проверять файлы из других пространств имен (в рамках обязательной проверки).

Создавать пользовательские задачи Защита от файловых угроз невозможно. Вы можете изменять параметры стандартной задачи Защита от файловых угроз.

Настройка Защиты от файловых угроз

Параметр	Описание
Защита от файловых угроз включена / выключена	Переключатель включает или выключает защиту от файловых угроз на всех управляемых устройствах. По умолчанию переключатель включен.
Режим Защиты от файловых угроз	В раскрывающемся списке можно выбрать режим компонента Защита от файловых угроз: • **Интеллектуальный режим** – 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 доступе** – проверять файл при попытке открытия на чтение, исполнение или изменение. • **При доступе и изменении** – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. По умолчанию выбран вариант **Интеллектуальный режим**.
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 рекомендуемое действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Блокировать** доступ к объекту. По умолчанию выбран вариант **Выполнять рекомендуемое действие**.

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 рекомендуемое действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Блокировать** доступ к объекту. По умолчанию выбран вариант **Блокировать**.
Области проверки	Содержит объекты, которые проверяет компонент Защита от файловых угроз. При переходе по ссылке **Настроить области проверки** открывается окно **Области проверки**. В этом окне можно настраивать области проверки. Области проверки в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз.
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, Kaspersky Endpoint Security проверяет архивы. Программа обнаруживает зараженные объекты в архивах, но не лечит их. Выберите этот вариант для более детальной проверки. Для проверки архива программе требуется сначала распаковать его, что может замедлить проверку. Можно уменьшить продолжительность проверки архивов, включив и настроив параметры **Прервать проверку, если она длится более (сек.)** и **Пропускать объекты размером более (МБ)**. 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.
Прервать проверку, если она длится более (сек.)	Поле, в котором можно 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 можно указать максимальный размер проверяемого архива в мегабайтах. Доступные значения: `0` – `999 999`. 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.
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 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** – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.
  По умолчанию выбран вариант **Рекомендованный**.

Окно Область проверки

Можно настроить области проверки для задачи Защита от файловых угроз. Программа проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все общие директории.

Области проверки для задачи Защита от файловых угроз

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к защищаемой директории.
Статус	Показывает, проверяет ли программа эту область при выполнении задачи. Можно включить или выключить переключатель в таблице для изменения статуса области проверки.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Endpoint Security защищает объекты в указанных областях в том порядке, в каком эти области перечислены в списке. При необходимости поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Название области проверки>

В этом окне можно добавить или настроить области проверки для задачи Защита от файловых угроз.

Параметры области проверки для задачи Защита от файловых угроз

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область в задаче проверки	Флажок включает или выключает проверку этой области во время выполнения задачи. Если флажок установлен, Kaspersky Endpoint Security обрабатывает эту область проверки во время выполнения задачи. Если флажок снят, Kaspersky Endpoint Security 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	В раскрывающемся списке можно выбрать тип файловой системы: • **Локальная** – отображаются локальные директории. • **Смонтированная** – отображаются смонтированные директории. • **Общая** – отображаются ресурсы файловой системы сервера, предоставленные для доступа по протоколу Samba или NFS. • **Все смонтированные** – отображаются все смонтированные директории. • **Все общие** – отображаются все ресурсов файловой системы сервера, предоставленных для доступа по протоколам Samba и NFS. По умолчанию выбран вариант **Локальная**.
Протокол доступа	В раскрывающемся списке можно выбрать протокол удаленного доступа: • **NFS** • **Samba** Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран вариант **Общая** или **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран вариант **Локальная**.

	Если в раскрывающемся списке файловых систем выбран вариант **Локальная** и не указан путь, Kaspersky Endpoint Security проверяет все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые Kaspersky Endpoint Security проверяет во время выполнения задачи Защита от шифрования. По умолчанию список содержит маску * (все объекты). Можно добавлять, изменять и удалять маски.

Исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security не проверяет объект на вирусы и другие угрозы. Можно также исключать объекты из проверки по маскам и названиям угроз.

Параметры исключений из проверки

Параметр	Описание
Области исключений	При переходе по ссылке **Настроить исключения** открывается окно **Области исключений**. Для задач открывается окно **Исключения из проверки**. В этом окне можно задать список исключений из проверки.
Исключения по маске	При переходе по ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**. В этом окне можно настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	При переходе по ссылке **Настроить исключения по названию угрозы** открывается окно **Исключения по названию угрозы**. В этом окне можно задать список исключений из проверки.

Область исключений

Можно настраивать следующие области исключений.

Параметры области исключений

Параметр	Описание
Название области исключения	Поле ввода названия области исключений. Это название будет отображаться в таблице **Исключения из проверки**. Поле ввода не должно быть пустым.
Использовать эту область в	Флажок включает или выключает исключение области во время выполнения задачи проверки по требованию. Если флажок установлен,

задаче проверки	Kaspersky Endpoint Security исключает эту область во время выполнения задачи проверки. Если флажок снят, Kaspersky Endpoint Security включает эту область во время выполнения задачи проверки. В дальнейшем вы можете исключить эту область из проверки, установив флажок. По умолчанию флажок установлен.
Файловая система	В раскрывающемся списке можно выбрать тип файловой системы, исключаемой из проверки: • **Локальная** – выбор локальных директорий. • **Смонтированная** – выбор удаленных директорий, смонтированных на компьютере по протоколу Samba или NFS. • **Все смонтированные** – выбор всех удаленных директорий, смонтированных на компьютере по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке можно выбрать протокол удаленного доступа: • **NFS** • **Samba** Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран элемент **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключений. По умолчанию указан путь **/** – Kaspersky Endpoint Security исключает все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран вариант **Локальная**.
Маски	Список содержит маски имен объектов, которые Kaspersky Endpoint Security исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле **Путь**. Можно добавлять, изменять и удалять маски. По умолчанию список содержит маску * (все объекты).

Исключения по маске

Можно настроить исключение объектов из проверки по маске имени. Программа не будет выполнять поверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Можно добавлять, изменять и удалять маски.

Исключения по названию угрозы

Можно настроить исключение объектов из проверки по названию угрозы. Программа не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Можно добавлять, изменять и удалять названия угроз.

Управление сетевым экраном

Во время работы в локальных сетях и интернете компьютер подвержен не только заражению вирусами и другими вредоносными программами, но и различного рода атакам, использующим уязвимости операционных систем и программного обеспечения.

Сетевой экран операционной системы защищает персональные данные, которые хранятся на компьютере пользователя. Сетевой экран блокирует большую часть потенциальных угроз для операционной системы, когда компьютер подключен к интернету или локальной сети. Управление сетевым экраном позволяет обнаружить все сетевые соединения на компьютере пользователя и предоставить список их IP-адресов с указанием статуса сетевого соединения по умолчанию.

Компонент Управление сетевым экраном фильтрует всю сетевую активность в соответствии с сетевыми пакетными правилами. Настройка сетевых пакетных правил позволяет вам задать нужный уровень защиты компьютера, от полной блокировки доступа в интернет для всех программ до разрешения неограниченного доступа.

Во время работы задачи Управление сетевым экраном Kaspersky Endpoint Security управляет параметрами и правилами сетевого экрана операционной системы. Программа блокирует любую настройку параметров сетевого экрана операционной системы, когда, например, программа или инструмент добавляют или удаляют какое-то правило. Kaspersky Endpoint Security проверяет сетевой экран операционной системы каждые 60 секунд и при необходимости восстанавливает набор правил сетевого экрана. Периодичность проверки изменить невозможно.

> В операционных системах Red Hat Enterprise Linux и CentOS 8 правила сетевого экрана, созданные с помощью Kaspersky Endpoint Security, можно просмотреть только с помощью Kaspersky Endpoint Security (команда `kesl-control -F --query`).

Проверка сетевого экрана операционной системы по-прежнему выполняется, когда задача Управление сетевым экраном остановлена. Это позволяет программе восстанавливать динамические правила.

Все исходящие соединения разрешены по умолчанию (параметр действия по умолчанию) за исключением случаев, когда указаны соответствующие запрещающие правила задачи Управление сетевым экраном. Действие по умолчанию выполняется с самым низким приоритетом: если не сработало никакое другое сетевое пакетное правило или другие сетевые пакетные правила не указаны, соединение разрешается.

Перед включением задачи Управление сетевым экраном мы рекомендуем отключить другие средства управления сетевым экраном операционной системы.

Параметры задачи Управление сетевым экраном

Параметр	Описание
Управление сетевым экраном включено / выключено	Переключатель включает или выключает Управление сетевым экраном. По умолчанию переключатель выключен.
Сетевые пакетные правила	При переходе по ссылке **Настроить сетевые пакетные правила** открывается окно **Сетевые пакетные правила**. В этом окне можно настроить список сетевых пакетных правил, которые будет выполнять компонент Управление сетевым экраном при обнаружении попытки установления сетевого соединения.
Доступные сети	При переходе по ссылке **Настроить доступные сети** открывается окно **Доступные сети**. В этом окне можно настроить список сетей, которые будет контролировать задача Управление сетевым экраном.
Входящие соединения	В этом раскрывающемся списке вы можете указать действие для входящих сетевых соединений: • **Разрешить** сетевые соединения. • **Блокировать** сетевые соединения. По умолчанию выбран вариант **Разрешить**.
Входящие пакеты	В этом раскрывающемся списке вы можете указать действие для входящих пакетов: • **Разрешить** входящие пакеты. • **Блокировать** входящие пакеты. По умолчанию выбран вариант **Разрешить**.
Всегда добавлять разрешающие	Флажок включает или выключает автоматическое добавление разрешающих правил для портов Агента администрирования.

правила для портов Агента администрирования	По умолчанию флажок установлен.

Окно Сетевые пакетные правила

Таблица **Сетевые пакетные правила** содержит сетевые пакетные правилами, используемые в задаче Управление сетевым экраном для контроля сетевой активности. Для сетевых пакетных правил можно настроить параметры, описанные в следующей таблице.

Параметры сетевых пакетных правил

Параметр	Описание
Название	Имя сетевого пакетного правила.
Действие	Действие, выполняемое задачей Управление сетевым экраном при обнаружении сетевой активности. Можно выбрать действие из раскрывающегося списка.
Протокол	Тип протокола передачи данных, для которого необходим мониторинг сетевой активности.
Направление	Направление отслеживаемой сетевой активности.
Удаленный адрес	Сетевые адреса удаленных компьютеров, которые могут передавать и / или получать сетевые пакеты.
Локальный адрес	Сетевые адреса компьютеров с установленной программой Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты.
Удаленные порты	Номера портов удаленных компьютеров, соединение между которыми отслеживается. Отображается, только если выбран протокол передачи данных TCP или UDP.
Локальные порты	Номера портов локальных компьютеров, соединение между которыми отслеживается. Отображается, только если выбран протокол передачи данных TCP или UDP.
ICMP-тип	ICMP-тип пакета – отображается, только если выбран протокол передачи данных ICMP или ICMPv6.
ICMP-код	ICMP-код пакета – отображается, только если выбран протокол передачи данных ICMP или ICMPv6.
Запись в отчет	Переключатель определяет, будут ли действия по сетевому пакетному правилу записываться в отчет.

	Если переключатель включен, программа фиксирует в журнале действия по сетевому пакетному правилу. Если переключатель выключен, программа не фиксирует в журнале действия по сетевому пакетному правилу.

По умолчанию таблица сетевых пакетных правил пуста.

Сетевые пакетные правила в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз. При нажатии на кнопку **Фильтр** открывается окно, в котором можно задать фильтрацию отображаемой информации о сетевых пакетных правилах. Также в этом окне можно выполнить поиск определенных правил.

Окно Сетевое пакетное правило

В окне **Сетевое пакетное правило** можно настроить сетевые пакетные правилами, используемые в задаче Управление сетевым экраном для контроля сетевой активности.

Параметры сетевых пакетных правил

Параметр	Описание
Название правила	Поле ввода названия правила управления сетевым экраном.
Действия	В раскрывающемся списке можно выбрать действие, которое должна выполнять задача Управление сетевым экраном, при обнаружении сетевой активности: • **Блокировать** сетевую активность. • **Разрешить** сетевую активность. По умолчанию выбран вариант **Разрешить**.
Протокол	В раскрывающемся списке выберите тип протокола передачи данных, для которого необходим мониторинг сетевой активности. Доступные значения: • **Любой** • **TCP** • **UDP** • **ICMP** • **ICMPv6** • **IGMP**

	• **GRE** По умолчанию выбран элемент **Любой**.
Указать ICMP-тип	Этот флажок позволяет указать тип ICMP . Задача Управление сетевым экраном контролирует сообщения указанного типа, отправляемые узлом или шлюзом. Если флажок установлен, отображается поле для ввода типа ICMP. Флажок отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **ICMP** или **ICMPv6**. По умолчанию флажок снят.
Указать ICMP-тип	Этот флажок позволяет указать код ICMP. Задача Управление сетевым экраном контролирует сообщения указанного типа (в поле **ICMP-тип**) и с указанным кодом, отправляемые узлом или шлюзом. Если флажок установлен, отображается поле для ввода кода ICMP. Флажок отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **ICMP** или **ICMPv6**, и доступен, если установлен флажок **Указать ICMP-тип**. По умолчанию флажок снят.
Направление	В раскрывающемся списке можно указать направление отслеживаемой сетевой активности: • **Входящее (пакет)**. Если выбран этот вариант, задача Управление сетевым экраном контролирует входящие пакеты. • **Входящее**. Если выбран этот вариант, задача Управление сетевым экраном контролирует входящую сетевую активность. • **Входящее / Исходящее**. Если выбран этот вариант, задача Управление сетевым экраном контролирует входящую и исходящую сетевую активность. • **Входящее / Исходящее (пакет)**. Если выбран этот вариант, задача Управление сетевым экраном контролирует входящие и исходящие пакеты. • **Исходящее (пакет)**. Если выбран этот вариант, задача Управление сетевым экраном контролирует исходящие пакеты. • **Исходящее**. Если выбран этот вариант, задача Управление сетевым экраном контролирует исходящую сетевую активность. По умолчанию выбран элемент **Входящее (пакет)**.

Удаленный адрес	В этом раскрывающемся списке можно указать сетевые адреса удаленных компьютеров, которые могут передавать и получать сетевые пакеты. • **Любой адрес**. Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов удаленными компьютерами с любым IP-адресом. • **Все адреса подсети**. Если выбран этот вариант, сетевое правило контролирует сетевые пакеты, отправляемые и получаемые удаленными компьютерами с IP-адресами, которые относятся к выбранному типу сети: **Публичная**, **Локальная** или **Доверенная**. • **Определенный адрес**. Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов удаленными компьютерами с IP-адресами, указанными в поле ввода **Адрес**. По умолчанию выбран элемент **Любой адрес**.
Указать удаленные порты	Флажок позволяет указать номера портов удаленных компьютеров, между которыми требуется контролировать соединение. Если флажок установлен, отображается поле для ввода номеров портов. Флажок отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **TCP** или **UDP**. По умолчанию флажок снят.
Локальный адрес	В этом раскрывающемся списке можно указать сетевые адреса компьютеров с установленной программой Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты: • **Любой адрес**. Если выбран этот элемент, сетевое правило контролирует отправку и получение сетевых пакетов компьютерами с установленной программой Kaspersky Endpoint Security и любым IP-адресом. • **Определенный адрес**. Если выбран этот вариант, сетевое правило контролирует указанные в поле **Адрес** сетевые адреса компьютеров с установленной программой Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты. По умолчанию выбран элемент **Любой адрес**.
Указать локальные порты	Флажок позволяет указать номера портов локальных компьютеров, между которыми требуется контролировать соединение. Если флажок установлен, отображается поле для ввода номеров портов. Флажок отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **TCP** или **UDP**.

	По умолчанию флажок снят.
Записывать в отчет	Флажок позволяет указать, будут ли действия по сетевому правилу записываться в отчет: Если флажок установлен, Kaspersky Endpoint Security записывает действия сетевого правила. Если флажок снят, Kaspersky Endpoint Security не записывает действия сетевого правила. По умолчанию флажок снят.

Окно Доступные сети

В таблице **Доступные сети** содержатся сети, контролируемые задачей Управление сетевым экраном.

Параметры доступных сетей

Параметр	Описание
IP-адрес	IP-адрес сети.
Тип сети	В раскрывающемся списке можно выбрать тип сети (**Доверенная сеть**, **Локальная сеть** или **Публичная сеть**). Этот параметр можно изменить в раскрывающемся списке в таблице.

По умолчанию таблица доступных сетей пуста.

Можно добавлять, изменять и удалять доступные сети.

Защита от веб-угроз

Во время работы задачи 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.

Kaspersky Endpoint Security проверяет трафик, передаваемый по протоколам HTTP, HTTPS и FTP. Также выполняется проверка веб-сайтов и IP-адресов. Можно указать определенные сетевые порты или диапазоны сетевых портов для проверки.

Для проверки HTTPS-трафика включите проверку зашифрованных соединений.

Для проверки FTP-трафика установите флажок **Отслеживать все сетевые порты**.

При попытке открытия опасного веб-сайта, Kaspersky Endpoint Security выполняет следующие действия:

- Для HTTP- или FTP-трафика программа блокирует доступ и показывает предупреждение.
- Для HTTPS-трафика в браузере отображается страница с ошибкой.

При открытии веб-сайта задача Защита от веб-угроз выполняет следующие действия:

1. Проверяет надежность веб-сайта с помощью загруженных антивирусных баз.
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.

Задача Защита от веб-угроз запускается по умолчанию при запуске Kaspersky Endpoint Security.

Настройка Защиты от веб-угроз

Параметр	Описание
Защита от веб-угроз включена / выключена	Переключатель включает или выключает компонент Защита от веб-угроз. По умолчанию переключатель включен.
Действие при обнаружении угрозы	В этом разделе можно указать действие, выполняемое Kaspersky Endpoint Security над веб-ресурсом, на котором обнаружен опасный объект: • **Информировать** пользователя при обнаружении опасного объекта в веб-трафике. Компонент 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. По умолчанию выбран вариант **Блокировать**.
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 компьютерам 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 считается доверенным. В список доверенных веб-адресов можно добавлять только веб-адреса HTTP/HTTPS. По умолчанию таблица пуста. Можно добавлять, изменять и удалять веб-адреса.

Окно Веб-адрес \ Маска веб-адреса

В список доверенных веб-адресов можно добавлять веб-адреса или маски веб-адресов.

Доверенные веб-адреса

Параметр	Описание
Введите	Поле для ввода веб-адресов и веб-страниц, содержимое которых считается

адрес или маску адреса веб-сайта	доверенным. При создании маски адреса используйте символ звездочка (*) вместо одного или нескольких символов. Например, 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.

Защита от сетевых угроз

Во время работы задачи Защита от сетевых угроз Kaspersky Endpoint Security проверяет входящий сетевой трафик на действия, характерные для сетевых атак. Программа проверяет входящий трафик для TCP-портов 80, 139, 445 и 8080.

При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, программа блокирует сетевую активность со стороны атакующего компьютера и записывает в журнал соответствующее событие.

Kaspersky Endpoint Security блокирует сетевой трафик со стороны атакующего компьютера на один час. Можно изменить параметры блокировки атакующего компьютера.

Задача Защита от сетевых угроз запускается по умолчанию при запуске Kaspersky Endpoint Security.

Настройка 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.
Блокировка атакующих устройств включена / выключена	Переключатель включает или выключает блокировку сетевой активности при обнаружении попытки сетевой атаки. По умолчанию переключатель включен.
Блокировать атакующее	В этом поле можно указать длительность блокировки атакующего устройства в минутах. По истечении указанного времени Kaspersky

устройство на (мин.)	Endpoint Security разрешает сетевую активность со стороны этого устройства. Доступные значения: целые числа от `1` до `32768`. Значение по умолчанию: `60`.
Исключения	В таблице содержится список IP-адресов, сетевые атаки с которых не будут заблокированы. По умолчанию список пуст. IP-адреса в таблице можно добавлять, настраивать и удалять

Окно IP-адрес

Можно добавлять и изменять IP-адреса.

IP-адреса

Параметр	Описание
Укажите IP-адрес (IPv4 или IPv6)	Поле для ввода IP-адреса. IP-адреса можно указывать в форматах IPv4 и IPv6.

Защита от шифрования

Задача Защита от шифрования позволяет защитить ваши файлы в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования.

В 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.

Kaspersky Endpoint Security не расценивает действия как вредоносное шифрование, если активность обнаружена в директориях, которые не входят в область задачи Защита от шифрования.

По умолчанию Kaspersky Endpoint Security блокирует доступ недоверенных устройств к сетевым файловым ресурсам на 30 минут.

Чтобы задача Защита от шифрования работала корректно, необходимо, чтобы в операционной системе была установлена хотя бы одна из служб: Samba или NFS. Для службы NFS необходимо, чтобы был установлен пакет rpcbind.

Задача Защита от шифрования корректно работает с протоколами SMB1, SMB2, SMB3, NFS3, TCP/UDP и IP/IPv6. Работа с протоколами NFS2 и NFS4 не поддерживается. Мы рекомендуем настроить параметры сервера таким образом, чтобы протоколы NFS2 и NFS4 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.

Параметры задачи Защита 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.
Область проверки	При переходе по ссылке **Настроить область проверки** открывается окно Область проверки.
Блокировка недоверенных устройств включена / выключена	Переключатель включает или выключает блокировку недоверенных устройств. По умолчанию переключатель включен.
Блокировать недоверенное устройство на (мин)	В этом поле можно 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	При переходе по ссылке **Настроить исключения** открывается окно Исключения.
Исключения по маске	При переходе по ссылке **Настроить исключения по маске** открывается окно Исключения по маске.

Окно Область проверки

Можно настроить области проверки для задачи Защита от шифрования. Программа проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все общие директории.

Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к защищаемой директории.
Статус	Показывает, проверяет ли программа эту область при выполнении задачи. Можно включить или выключить переключатель в таблице для изменения статуса области проверки.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Endpoint Security защищает объекты в указанных областях в том порядке, в каком эти области перечислены в списке. При необходимости поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Название области проверки>

В этом окне можно добавить или настроить области проверки для задачи Защита от шифрования.

Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область в задаче проверки	Флажок включает или выключает проверку этой области во время выполнения задачи. Если флажок установлен, Kaspersky Endpoint Security обрабатывает эту область проверки во время выполнения задачи. Если флажок снят, Kaspersky Endpoint Security 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	В раскрывающемся списке можно выбрать путь к защищаемым объектам: • **Локальные** – показывает абсолютный путь, доступный по протоколу Samba или NFS. • **Общие** – защищает общие ресурсы, доступные по протоколам Samba и NFS (в зависимости от значения параметра **Протокол доступа**). • **Все общие** – защищает все ресурсы, доступные по протоколам Samba и NFS. По умолчанию выбран вариант **Локальная**.
Протокол доступа	В раскрывающемся списке можно выбрать протокол удаленного доступа: • **NFS** • **Samba** Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран вариант **Общие**.
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран вариант **Локальная**. Поле не должно быть пустым, иначе не удастся сохранить область проверки. По умолчанию указан путь **/** (корневая директория).
Маски	Список содержит маски имен объектов, которые Kaspersky Endpoint Security проверяет во время выполнения задачи Защита от шифрования. По умолчанию список содержит маску * (все объекты). Можно добавлять, изменять и удалять маски.

Окно Исключения

Можно настроить области исключений для задачи Защита от шифрования. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключений

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из защиты.
Статус	Показывает, исключает ли программа эту область из проверки при выполнении задачи.

Элементы в таблице можно добавлять, настраивать и удалять.

Окно <Название области исключений>

В этом окне можно добавить или настроить области исключений для задачи Защита от шифрования.

Параметры области исключений

Параметр	Описание
Название области исключения	Поле ввода названия области исключений. Это название будет отображаться в таблице **Исключения из проверки**. Поле ввода не должно быть пустым.
Использовать эту область в задаче проверки	Флажок включает или выключает исключение области во время выполнения задачи проверки по требованию. Если флажок установлен, Kaspersky Endpoint Security исключает эту область во время выполнения задачи проверки. Если флажок снят, Kaspersky Endpoint Security включает эту область во время выполнения задачи проверки. В дальнейшем вы можете исключить эту область из проверки, установив флажок. По умолчанию флажок установлен.
Файловая система	В раскрывающемся списке можно выбрать путь к объектам, исключаемым из защиты: • **Локальные** – показывает абсолютный путь, доступный по протоколу Samba или NFS. • **Общие** – исключает общие ресурсы, доступные по протоколам Samba и NFS (в зависимости от значения параметра **Протокол доступа**). • **Все общие** – исключает все ресурсы, доступные по протоколам Samba и NFS. По умолчанию выбран вариант **Локальная**.

Протокол доступа	В раскрывающемся списке можно выбрать протокол удаленного доступа: • **NFS** • **Samba** Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран вариант **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите включить в область исключений. Поле доступно, если в раскрывающемся списке файловых систем выбран вариант **Локальная**. Поле не должно быть пустым, иначе не удастся сохранить область исключений.
Маски	Список содержит маски имен объектов, которые Kaspersky Endpoint Security исключает из проверки во время выполнения задачи Защита от шифрования. По умолчанию список содержит маску * (все объекты). Можно добавлять, изменять и удалять маски.

Окно Исключения по маске

Можно настроить исключение объектов из проверки по маске имени. Программа не будет выполнять поверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Можно добавлять, изменять и удалять маски.

Контроль целостности системы

Параметры задачи Контроль целостности системы не доступны при управлении программой с помощью Kaspersky Security Center Cloud Console.

Задача Контроль целостности системы создана для отслеживания действий, выполняемых с файлами и директориями в области мониторинга, указанной в параметрах задачи. Вы можете использовать задачу, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом сервере. Вы также можете настроить отслеживание изменений в файлах в те периоды, когда мониторинг прерывается.

Для использования функции контроля целостности системы необходимо приобрести лицензию, которая включает эту функцию. По умолчанию контроль целостности системы выключен.

Параметры задачи Контроль целостности системы

Параметр	Описание
Контроль целостности системы включен / выключен	Переключатель включает или выключает задачу Контроль целостности системы. По умолчанию переключатель выключен.
Области мониторинга	При переходе по ссылке **Настроить области мониторинга** открывается окно **Области мониторинга**.
Исключения из мониторинга	При переходе по ссылке **Настроить исключения из мониторинга** открывается окно **Исключения из мониторинга**.
Исключения по маске	При переходе по ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**.

Окно Области мониторинга

Можно настроить 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/).

Параметры области проверки

Параметр	Описание
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Показывает, проверяет ли программа эту область при выполнении задачи. Можно включить или выключить переключатель в таблице для изменения статуса области мониторинга.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Endpoint Security защищает объекты в указанных областях в том порядке, в каком эти области перечислены в списке. При необходимости поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Название области проверки>

В этом окне можно добавить или настроить области мониторинга для задачи Контроль целостности системы.

Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице **Области мониторинга**. Поле ввода не должно быть пустым.
Использовать эту область в задаче проверки	Флажок включает или выключает проверку этой области во время выполнения задачи. Если флажок установлен, Kaspersky Endpoint Security обрабатывает эту область мониторинга во время выполнения задачи. Если флажок снят, Kaspersky Endpoint Security не обрабатывает эту область мониторинга во время выполнения задачи. В дальнейшем вы можете включить эту область в параметры задачи, установив флажок. По умолчанию флажок установлен.
Файловая система	Путь к контролируемым объектам: • **Локальные** – показывает абсолютный путь, доступный по протоколу Samba или NFS.
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. Поле не должно быть пустым, иначе не удастся сохранить область проверки.
Маски	Список содержит маски имен объектов, которые Kaspersky Endpoint Security проверяет во время выполнения задачи Защита от шифрования. По умолчанию список содержит маску * (все объекты). Можно добавлять, изменять и удалять маски.

Окно Исключения из мониторинга

Можно настроить области исключений для задачи Контроль целостности системы. Программа не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключений

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из защиты.
Статус	Показывает, исключает ли программа эту область из проверки при выполнении задачи.

Элементы в таблице можно добавлять, настраивать и удалять.

Окно <Название области исключений>

В этом окне можно добавить или настроить области исключений для задачи Контроль целостности системы.

Параметры области исключений

Параметр	Описание
Название области исключения	Поле ввода названия области исключений. Это название будет отображаться в таблице **Исключения из проверки**. Поле ввода не должно быть пустым.
Использовать эту область в задаче проверки	Флажок включает или выключает исключение области во время выполнения задачи проверки по требованию. Если флажок установлен, Kaspersky Endpoint Security исключает эту область во время выполнения задачи проверки. Если флажок снят, Kaspersky Endpoint Security включает эту область во время выполнения задачи проверки. В дальнейшем вы можете исключить эту область из проверки, установив флажок. По умолчанию флажок установлен.
Файловая система	Тип файловой системы: • **Локальная** – отображаются локальные директории.
Путь	Поле ввода пути к директории, которую вы хотите включить в область исключений.
Маски	Список содержит маски имен объектов, которые Kaspersky Endpoint

Security исключает из проверки во время выполнения задачи Защита от шифрования.

По умолчанию список содержит маску * (все объекты).

Можно добавлять, изменять и удалять маски.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно Исключения по маске

Можно настроить исключение объектов из проверки по маске имени. Программа не будет выполнять поверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Можно добавлять, изменять и удалять маски.

Контроль устройств

Во время выполнения задачи Контроль устройств программа Kaspersky Endpoint Security управляет доступом пользователей к устройствам, установленным или подключенным к компьютеру (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. Это позволяет защитить компьютер от заражения при подключении таких устройств, а также предотвратить потерю и утечку данных.

Задача Контроль устройств управляет доступом пользователей к устройствам с помощью правил доступа.

Задача Контроль устройств управляет доступом на следующих уровнях:

- **Класс устройства**. Например, принтеры, съемные диски, CD/DVD-приводы.

  Для каждого типа устройств можно указать следующие правила доступа: *Allow*, *Block* или *DependsOnBus*. Если указано значение *DependsOnBus*, доступ к устройству определяется правилом доступа к шине подключения.

- **Шина подключения**. *Шина подключения* – это интерфейс, используемый для подключения устройств к компьютеру (*USB* или *FireWire*).

  Для каждой шины подключения можно указать следующие правила доступа: *Allow* или *Block*. Например, можно разрешить или запретить подключение всех устройств по USB.

- **Доверенные устройства**. *Доверенные устройства* – это устройства, к которым у пользователей есть полный доступ.

  Можно добавить устройства в список доверенных по идентификатору устройства. У каждого устройства есть уникальный идентификатор.

Если устройство, заблокированное задачей Контроль устройств, подключено к компьютеру, Kaspersky Endpoint Security запрещает пользователям доступ к этому устройству и выводит уведомление.

Параметры задачи Контроль устройств

Параметр	Описание
Контроль подключения съемных дисков включен / выключен	Переключатель включает или выключает компонент Контроль устройств. По умолчанию переключатель включен.
Настроить доверенные устройства	При переходе по ссылке открывается окно **Доверенные устройства**. В этом окне можно добавлять устройства в список доверенных по идентификатору устройства или выбрав их из списка существующих устройств.
Настроить параметры для типов устройств	При переходе по ссылке открывается окно **Типы устройств**. В этом окне можно настроить правила доступа для различных типов устройств.
Настроить параметры для шин подключения устройств	При переходе по ссылке открывается окно **Шины подключения**. В этом окне можно настроить правила доступа к шинам подключения.

Окно Доверенные устройства

На этой странице можно настроить список доверенных устройств. Для доверенного устройства можно настроить параметры, описанные в следующей таблице. По умолчанию не задано ни одного доверенного устройства.

Параметры Доверенного устройства

Параметр	Описание
ID устройства	Идентификатор доверенного устройства.
Имя устройства	Имя доверенного устройства.
Тип устройства	Тип доверенного устройства (например, *Жесткий диск* или *Устройство чтения смарт-карт*).
Имя	Имя компьютера, к которому подключено доверенное устройство.

устройства	
Комментарий	Комментарий, относящийся к доверенному устройству.

Можно добавить устройства в список доверенных по идентификатору устройства, выбрав требуемое устройство из списка существующих устройств. Доверенные устройства в таблице можно изменять и удалять.

Окно Идентификатор устройства

Можно добавить устройства в список доверенных по идентификатору устройства.

Если управление программой Kaspersky Endpoint Security осуществляется с помощью Kaspersky Security Center Cloud Console, список доверенных устройств остается пустым.

Добавление устройства по идентификатору

Параметр	Описание
ID устройства	Поле для ввода идентификатора устройства. Идентификатор устройства можно указать вручную или скопировать идентификатор требуемого устройства из списка **Соответствие устройств и компьютеров**.
Комментарий	Поле ввода комментария (не обязательное). Это поле доступно после ввода идентификатора устройства и нажатия на кнопку **Далее**.

Окно Устройства на компьютере

Можно добавить устройства в список доверенных, выбрав требуемое устройство из списка существующих устройств.

Информация о существующих устройствах доступна, если существует активная политика и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в политике Агента администрирования, по умолчанию – каждые 15 минут). При создании новой политики в отсутствии активной политики, список будет пустым.

Если управление программой Kaspersky Endpoint Security осуществляется с помощью Kaspersky Security Center Cloud Console, список доверенных устройств остается пустым.

Добавление устройства из списка

Параметр	Описание
Тип устройства	В раскрывающемся списке можно выбрать тип устройств, отображающихся в таблице **Устройства на компьютере**.
Маска идентификатора	Поле для ввода маски идентификатора устройства.

устройства	
Комментарий	Поле ввода комментария (не обязательное). Это поле доступно после выбора устройств и нажатия на кнопку **Далее**.

При нажатии на кнопку **Фильтр** открывается окно, в котором можно настроить фильтрацию отображаемой информации об устройствах.

Окно Тип устройства

В этом окне можно настроить правила доступа для различных типов устройств.

Правила подключения для типов устройств

Параметр	Описание
Тип	Типы устройств (например, **Жесткие диски**, **Принтеры**).
Доступ	Правила доступа к устройствам соответствующего типа: • **Разрешить** – предоставить доступ к устройствам соответствующего типа. • **Блокировать** – запретить доступ к устройствам соответствующего типа. Для сетевого адаптера нельзя выбрать правило доступа **Блокировать**. • **Зависит от шины** – разрешает или запрещает доступ к устройствам в зависимости от правила доступа для шины, используемой для подключения устройства к компьютеру. По умолчанию выбран вариант **Зависит от шины**.

Окно Шины подключения

В этом окне можно настроить правила доступа для шин подключения.

Правила доступа для шин подключения

Параметр	Описание
Шина подключения устройства	Шины подключения, используемые для подключения устройств к компьютеру: • **FireWire** • **USB**
Доступ	Переключатель включает или выключает доступ к устройствам, использующим соответствующую шину для подключения к компьютеру:

- **Разрешен** – предоставить доступ к устройствам, подключенным к компьютеру с помощью соответствующей шины подключения.
- **Заблокирован** – запретить доступ к устройствам, подключенным к компьютеру с помощью соответствующей шины подключения.
  По умолчанию переключатель находится в положении **Разрешен**.

Анализ поведения

Задача Анализ поведения контролирует вредоносную активность в операционной системе. При обнаружении вредоносной активности Kaspersky Endpoint Security завершает этот процесс.

По умолчанию задача запускается при старте Kaspersky Endpoint Security. Можно запускать и останавливать задачу Анализ поведения.

Параметры задачи Анализ поведения

Параметр	Описание
Анализ поведения включен / **выключен**	Переключатель включает или выключает задачу Анализ поведения. По умолчанию переключатель включен.

Управление задачами

Для работы с Kaspersky Endpoint Security через Kaspersky Security Center 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.

Параметры управления задачами

Параметр	Описание

Разрешить пользователям просматривать локальные задачи и управлять ими	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в Kaspersky Security Center Web Console, и управление ими из интерфейса Kaspersky Endpoint Security на администрируемых устройствах. По умолчанию флажок снят.
Разрешить пользователям просматривать групповые задачи и управлять ими	Флажок разрешает или запрещает пользователям просмотр групповых задач, созданных в Kaspersky Security Center Web Console, и управление ими из интерфейса Kaspersky Endpoint Security на администрируемых устройствах. По умолчанию флажок снят.

Проверка съемных дисков

Когда запущена задача 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.

Параметры задачи Проверка съемных дисков

Параметр	Описание
Проверка съемных дисков включена / выключена	Переключатель включает или выключает проверку съемных дисков. По умолчанию переключатель выключен.
Действие при подключении съемного диска	В раскрывающемся списке вы можете выбрать действие, выполняемое при подключении съемных дисков: • **Не проверять** съемные диски при подключении. • **Быстрая проверка** – проверять только файлы определенных типов на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков) и не распаковывать составные объекты. При быстрой проверке используются параметры, заданные по умолчанию для задачи Защита от файловых угроз. • **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 по требованию. По умолчанию выбран вариант **Не проверять**.

Действие при подключении CD/DVD-привода	В раскрывающемся списке можно выбрать действие, выполняемое при подключении CD/DVD-приводов и Blu-ray дисков: • **Не проверять** CD/DVD-приводы и Blu-ray диски при подключении. • **Быстрая проверка** – проверять только файлы определенных типов на CD/DVD-приводах и Blu-ray дисках. При быстрой проверке используются параметры, заданные по умолчанию для задачи Защита от файловых угроз. • **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 по требованию. По умолчанию выбран вариант **Не проверять**.
Блокировать доступ к съемному диску во время проверки	Флажок включает или выключает блокировку съемных дисков при выполнении задачи Проверка съемных дисков. По умолчанию флажок снят.

Параметры прокси-сервера

Можно настроить параметры прокси-сервера для доступа пользователей клиентских компьютеров в интернет. Kaspersky Endpoint Security использует эти параметры в работе отдельных компонентов защиты, в том числе для обновления баз и модулей программы.

Параметры прокси-сервера

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, Kaspersky Endpoint Security подключается к службам Kaspersky Security Network, серверам обновлений и серверам активации напрямую, без использования прокси-сервера.
Использовать параметры указанного прокси-сервера	Если выбран этот вариант, Kaspersky Endpoint Security использует пользовательские параметры прокси-сервера для подключения к службам Kaspersky Security Network, серверам обновлений и серверам активации.
Адрес	Поля ввода для IP-адреса или доменного имени прокси-сервера.

	Поле доступно, если выбран вариант **Использовать параметры указанного прокси-сервера**.
Порт	Поля ввода для порта прокси-сервера. Поле доступно, если выбран вариант **Использовать параметры указанного прокси-сервера**. Значение по умолчанию: 3128.
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.
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. Поле ввода доступно, если установлен флажок **Использовать имя пользователя и пароль**. При нажатии на кнопку **Показать** пароль пользователя отображается в поле **Пароль** в открытом виде. Кнопка доступна, если установлен флажок **Использовать имя пользователя и пароль**. По умолчанию пароль пользователя скрыт и отображается в виде точек.
Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы	Флажок включает/выключает использование Kaspersky Security Center в качестве прокси-сервера при активации программы. Если флажок установлен, Kaspersky Endpoint Security использует Kaspersky Security Center в качестве прокси-сервера при активации программы. По умолчанию флажок снят.

Параметры программы

Можно настроить общие параметры Kaspersky Endpoint Security.

Общие параметры программы

Параметр	Описание
Обнаруживать легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда компьютерам 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	При переходе по ссылке **Настроить уведомления о событиях** открывается окно **Параметры уведомлений**. В этом окне вы можете указать события, для которых Kaspersky Endpoint Security будет записывать 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 флажки сняты.

Параметры перехватчика

Можно настроить способ мониторинга пространств имен и Docker-контейнеров в Kaspersky Endpoint Security.

При управлении программой с помощью Kaspersky Security Center Cloud Console доступен только параметр **Блокировать файлы во время проверки**.

Параметры перехватчика

Параметр	Описание
Мониторинг пространств имен и Docker-контейнеров включен / выключен	Переключатель включает или выключает проверку пространств имен и Docker-контейнеров. По умолчанию переключатель включен.
Действие при обнаружении угрозы	В этом разделе можно выбрать действие, выполняемое при обнаружении зараженного объекта во время поверки:

	• **Пропустить угрозу** – при обнаружении зараженного объекта никаких действий с Docker-контейнером не выполняется. • **Остановить Docker-контейнер** – при обнаружении зараженного объекта Docker-контейнер останавливается. • **Остановить Docker-контейнер, если не удалось вылечить объект или устранить угрозу** – если не удалось вылечить зараженный объект, Docker-контейнер останавливается. По умолчанию выбран вариант **Остановить Docker-контейнер, если не удалось вылечить объект или устранить угрозу**.
Docker-сокет	Поле ввода пути к Docker-сокету. Значение по умолчанию – /var/run/docker.sock.
Блокировать файлы во время проверки	Флажок включает или выключает блокировку файлов при проверке для всех задач мониторинга (Защита от файловых угроз, Проверка съемных дисков и Защита от шифрования).

Параметры сети

Можно настроить параметры проверки зашифрованных соединений. Эти параметры используются в задачах Защита от веб-угроз и Защита от сетевых угроз.

Параметры сети

Параметр	Описание
Проверка зашифрованных соединений включена / выключена	Переключатель включает или выключает проверку зашифрованных соединений. По умолчанию переключатель включен.
Действие при обнаружении недоверенного сертификата	В этом разделе можно выбрать действие, выполняемое при обнаружении недоверенного сертификата: • **Разрешить** подключение к домену с недоваренным сертификатом. • **Запретить** подключение к домену с недоваренным сертификатом. По умолчанию выбран вариант **Разрешить**.

Действие при ошибках во время проверки зашифрованных соединений	В этом разделе можно выбрать действие, выполняемое при возникновении ошибки во время проверки зашифрованных соединений: • **Добавить веб-сайт в исключения** – 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. По умолчанию выбран вариант **Добавить веб-сайт в исключения**.
Исключения	В этом разделе можно настроить список доверенных доменных имен. При переходе по ссылке **Настроить исключения** открывается окно **Исключения**. По умолчанию список имен доверенных доменов пуст.
Сетевые порты	В этом разделе можно настроить контролируемые сетевые порты. При переходе по ссылке **Изменить конфигурацию сетевых портов** открывается окно **Сетевые порты**.
Отслеживать все сетевые порты	Если выбран этот вариант, Kaspersky Endpoint Security проверяет все сетевые порты.
Отслеживать только указанные порты	Если выбран этот вариант, Kaspersky Endpoint Security проверяет только сетевые порты, указанные в таблице. Это действие выбрано по умолчанию.

Окно Исключения

Таблица содержит доменные имена и маски доменных имен, которые будут исключены из проверки зашифрованных соединений.

По умолчанию таблица пустая.

Домены в списке доверенных доменов можно добавлять, изменять и удалять.

Окно Сетевые порты

В окне **Сетевые порты**, в таблице отображаются сетевые порты, контролируемые Kaspersky Endpoint Security, если выбран вариант **Отслеживать только указанные порты**.

Таблица содержит два столбца:

- **Описание** указанного порта.

- Контролируемый **порт**.

По умолчанию в таблице отображается список сетевых портов, обычно используемых для передачи почтового и сетевого трафика. Список сетевых портов входит в пакет Kaspersky Endpoint Security.

Элементы в таблице можно добавлять, настраивать и удалять.

Исключенные точки монтирования

В таблице **Исключенные точки монтирования** содержатся точки монтирования, исключенные из проверки для задач, использующих перехват 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, настраивать и удалять.

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. Резервные копии могут содержать персональные данные. По умолчанию Хранилище расположено в директории /var/opt/kaspersky/kesl/common/objects-backup/.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, пользователь может попытаться восстановить файл из его вылеченной копии в директорию исходного размещения файла.

Параметры хранилища

Параметр	Описание
Информирование о необработанных файлах включено / выключено	Переключатель включает или выключает отправку уведомлений о необработанных файлах на Сервер администрирования. Если переключатель включен, Kaspersky Endpoint Security отправляет уведомление на Сервер администрирования, если файл не удалось обработать во время проверки.

	Если переключатель выключен, Kaspersky Endpoint Security не отправляет уведомление на Сервер администрирования, если файл не удалось обработать во время проверки. По умолчанию переключатель включен.
Информирование о файлах в хранилище включено / выключено	Переключатель включает или выключает отправку уведомлений о файлах в хранилище на Сервер администрирования. Если переключатель включен, Kaspersky Endpoint Security отправляет уведомления о файлах в хранилище на Сервер администрирования. Если переключатель выключен, Kaspersky Endpoint Security не отправляет уведомления 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).

Использование графического пользовательского интерфейса Kaspersky Endpoint Security

В этом разделе описана работа в Kaspersky Endpoint Security с использованием графического пользовательского интерфейса.

Локальное включение и выключение графического пользовательского интерфейса

Вы можете включить или выключить графический пользовательский интерфейс Kaspersky Endpoint Security локально с помощью командной строки.

Для включения и выключения графического пользовательского интерфейса требуются root-права.

Если отключен графический пользовательский интерфейс, пользователи, не обладающие root-правами, не смогут запустить графический пользовательский интерфейс на своих локальных компьютерах.

Чтобы включить или выключить графический пользовательский интерфейс, выполните следующие действия:

1. Запустите конфигурационный скрипт программы:

   `/opt/kaspersky/kesl/bin/kesl-setup.pl -G`

   Отображается запрос.

2. Выполните одно из следующих действий:

   - Если вы хотите включить графический пользовательский интерфейс, нажмите `Y`, а затем, при необходимости, укажите пользователя которому необходимо назначить роль администратора.

     Если вы включите графический пользовательский интерфейс, пользователи без root-прав смогут запускать до пяти задачи антивирусной проверки одновременно.

     Если пользователь вошел в систему, для него будет запущен графический пользовательский интерфейс, если доступны все необходимые библиотеки. Значок программы появляется в области уведомлений панели задач, и создается ярлык.

   - Если вы хотите отключить графический пользовательский интерфейс, введите `N`.

     Программа запрещает пользователям запускать графический пользовательский интерфейс локально. Значок программы и ярлык удаляются.

Интерфейс программы

Этот раздел содержит информацию об основных элементах графического пользовательского интерфейса программы.

Значок программы в области уведомлений

После включения графического пользовательского интерфейса Kaspersky Endpoint Security значок программы появляется в области уведомлений справа на панели задач.

Значок обеспечивает доступ к контекстному меню и главному окну программы.

Контекстное меню значка программы содержит следующие пункты:

- **Kaspersky Endpoint Security 11 для Linux**. Открывает главное окно программы. В главном окне программы отображается состояние защиты вашего компьютера, а также состояние задач антивирусной проверки и обновлений. Вы также можете перейти в окно **Отчеты**, **Хранилище**, **Параметры** или **Поддержка**.

- **Выход**. Выход из графического пользовательского интерфейса Kaspersky Endpoint Security.

Вы можете открыть контекстное меню значка программы, щелкнув правой кнопкой мыши по значку программы в области уведомлений.

Главное окно программы

В главном окне Kaspersky Endpoint Security находятся элементы интерфейса, предоставляющие вам доступ к функциям программы.

Главное окно программы разделено на несколько частей:

- В центральной части окна отображается статус защиты вашего компьютера. При щелчке мышью в этой части окна откроется окно **Центр защиты**.

- На закладке **Проверка** отображается состояние задачи антивирусной проверки и количество обнаруженных угроз. При щелчке по этой закладке открывается окно **Проверка**. В этом окне можно запустить и остановить задачи антивирусной проверки, проверки загрузочных секторов и проверки памяти процессов. Вы также можете просмотреть отчеты для этих задач.

- На закладке **Обновление** отображается состояние задачи Обновление и антивирусных баз. При щелчке по этой закладке открывается окно **Обновление**. В этом окне можно запустить или остановить задачи обновления или копирования обновлений. Вы также можете просмотреть отчеты для этих задач.

- В нижней части главного окна программы находятся следующие элементы:

    - Кнопка **Отчеты**. При нажатии на эту кнопку открывается окно **Отчеты**, в котором можно просмотреть статистику задач и различные отчеты.

    - Кнопка **Хранилище**. При нажатии на эту кнопку открывается окно **Хранилище**, в котором содержится информация об объектах в хранилище.

- Кнопка **Параметры**. При нажатии на эту кнопку открывается окно **Параметры**, в котором можно включить или отключить участие в Kaspersky Security Network, а также задачи Защита от файловых угроз, Контроль целостности системы, Управление сетевым экраном, Защита от шифрования, Защита от веб-угроз, Контроль устройств, Проверка съемных дисков, Защита от сетевых угроз и Анализ поведения.

- Кнопка **Поддержка**. При нажатии этой кнопки открывается окно **Поддержка**, в котором содержится информация о текущей версии Kaspersky Endpoint Security, лицензиях, статусе ключа, статусе баз, операционной системе, а также ссылки на информационные ресурсы "Лаборатории Касперского".

Открыть главное окно Kaspersky Endpoint Security можно одним из следующих способов:

- Дважды щелкните или щелкните правой кнопкой мыши значок программы в области уведомлений панели задач.

- Щелкните правой кнопкой мыши программу и выберите **Kaspersky Endpoint Security 11 для Linux**.

Управление задачами и компонентами

По умолчанию графический пользовательский интерфейс Kaspersky Endpoint Security позволяет вам запускать и останавливать следующие задачи:

- Задача полной проверки (Scan_My_Computer)

- Задачи антивирусной проверки (Scan_File, Boot_Scan, Memory_Scan)

- Задачи обновления (Обновление, Откат обновления баз)

Графический пользовательский интерфейс Kaspersky Endpoint Security также позволяет вам включать и выключать следующие компоненты:

- Защита от файловых угроз

- Контроль целостности системы

- Управление сетевым экраном

- Защита от шифрования

- Защита от веб-угроз

- Контроль устройств

- Проверка съемных дисков

- Защита от сетевых угроз
- Анализ поведения

Кроме того, вы можете управлять своим участием в Kaspersky Security Network.

Запуск и остановка задач проверки

С помощью графического пользовательского интерфейса Kaspersky Endpoint Security вы можете запускать и останавливать задачи полной проверки, антивирусной проверки, проверки загрузочных секторов и проверки памяти процессов.

Чтобы запустить или остановить задачу проверки, выполните следующие действия:

1. Откройте главное окно программы.
2. Кнопкой **Проверка**, расположенной в главном окне программы, откройте окно **Проверка**.
3. Выполните одно из следующих действий:
   - Если вы хотите запустить задачу, нажмите на кнопку **Запустить** под той задачей, которую вы хотите запустить.

     Отображается ход выполнения задачи.
   - Если вы хотите остановить задачу, нажмите на кнопку **Остановить** под той задачей проверки, которую вы хотите остановить.

     Задача проверки останавливается, и отображается информация о проверенных объектах и обнаруженных угрозах.
4. При необходимости вы можете нажать на кнопку **Показать отчет**, чтобы просмотреть отчет по задаче.

При обнаружении зараженного объекта или при завершении задачи проверки отображается всплывающее окно в области уведомлений рядом со значком программы в правой части панели задач.

Запуск и остановка задач обновления

С помощью графического пользовательского интерфейса Kaspersky Endpoint Security можно запускать и останавливать задачи **Обновление**, **Откат обновления баз** и **Копирование обновлений**.

Чтобы запустить или остановить задачу обновления или копирования обновления, выполните следующие действия:

1. Откройте главное окно программы.
2. Кнопкой **Обновить**, расположенной в главном окне программы, откройте окно **Обновление**.
3. Выполните одно из следующих действий:

   - Если вы хотите запустить задачу, нажмите на кнопку **Запустить** под той задачей, которую вы хотите запустить.

     Отображается ход выполнения задачи.

     При успешном завершении задачи обновления становится доступна ссылка **Откат обновления**, с помощью которой вы можете откатить последнее обновление.

   - Если вы хотите остановить задачу, нажмите на кнопку **Остановить** под той задачей, которую вы хотите остановить.

     Задача будет остановлена.

4. При необходимости вы можете нажать на кнопку **Показать отчет**, чтобы просмотреть отчет по задаче.

Чтобы запустить задачу отката обновления, выполните следующие действия:

1. Откройте главное окно программы.
2. Кнопкой **Обновить**, расположенной в главном окне программы, откройте окно **Обновление**.
3. В разделе **Обновление** перейдите по ссылке **Откат обновления**, чтобы откатить последнее успешное обновление баз.

Включение и выключение компонентов программы

С помощью графического пользовательского интерфейса Kaspersky Endpoint Security вы можете в любой момент включить или выключить следующие компоненты программы: Защита от файловых угроз, Управление сетевым экраном, Защита от шифрования и Контроль целостности системы.

Если компонент включен, доступна кнопка **Отключить**. По умолчанию включен только компонент Защита от файловых угроз.

Если компонент выключен, доступна кнопка **Включить**.

Чтобы включить или выключить компонент, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части главного окна программы нажмите на кнопку **Параметры**.

Откроется окно **Параметры**.

3. В окне **Параметры** выполните следующие действия для требуемого компонента:

   - Чтобы включить компонент, нажмите на кнопку **Включить**.
   - Чтобы отключить компонент, нажмите на кнопку **Отключить**.

Управление участием в Kaspersky Security Network

Вы можете управлять своим участием в Kaspersky Security Network в любой момент.

Чтобы включить Kaspersky Security Network, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части главного окна программы нажмите на кнопку **Параметры**.

   Откроется окно **Параметры**.
3. В окне **Параметры** выберите один из следующих вариантов:

   - **Kaspersky Security Network со статистикой** – чтобы включить Kaspersky Security Network, получать информацию из базы знаний и отправлять анонимную статистику и данные о типах и источниках угроз.
   - **Kaspersky Security Network без статистики** – чтобы 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, понимаю и принимаю положения и условия настоящего Положения о KSN** – чтобы включить Kaspersky Security Network.
   - **Я не принимаю положения и условия настоящего Положения о KSN** – чтобы отказаться от использования Kaspersky Security Network.
6. Нажмите **ОК**.

   Кнопка **ОК** недоступна, если выбран вариант **Не выбрано**.

Чтобы выключить Kaspersky Security Network, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части главного окна программы нажмите на кнопку **Параметры**.

   Откроется окно **Параметры**.

3. В окне **Параметры** нажмите на кнопку **Отключить**.

4. В открывшемся окне выполните одно из следующих действий:

   - Нажмите на кнопку **Да**, чтобы подтвердить отключение Kaspersky Security Network.
   - Нажмите **Отмена**, чтобы продолжать участвовать в Kaspersky Security Network.

Отчеты

В этом разделе содержится информация о том, как просматривать отчеты в графическом пользовательском интерфейсе Kaspersky Endpoint Security.

Об отчетах

Информация о работе каждого компонента Kaspersky Endpoint Security, результаты выполнения каждой задачи и работы всей программы в целом записываются в отчеты.

Способы формирования отчетов различаются и зависят от параметров программы и использования Kaspersky Security Center.

- Все отчеты хранятся в локальном хранилище событий программы. Хранилище событий расположено в директории, указанной общим параметром программы `EventsStoragePath`. По умолчанию, файл базы данных, в которой Kaspersky Endpoint Security сохраняет данные о событиях – /var/opt/kaspersky/kesl/events.db. Для доступа к базе данных событий требуются root-права.

- Если управление программой Kaspersky Endpoint Security осуществляется с помощью Kaspersky Security Center, данные о событиях могут передаваться на Сервер администрирования Kaspersky Security Center. Дополнительная информация об управлении отчетами в Kaspersky Security Center приведена в документации Kaspersky Security Center.

- Если для общего параметра программы задано значение `UseSysLog=Yes`, данные о событиях также записываются в syslog. Для доступа к syslog требуются root-права.

В отчетах могут содержаться следующие данные пользователей:

- имя и идентификатор пользователя в операционной системе;
- путь к файлам пользователя;

- IP-адреса удаленных компьютеров, проверяемых задачей Защита от шифрования;
- IP-адреса отправителей и получателей сетевых пакетов, проверяемых задачей Управление сетевым экраном;
- веб-адреса источников обновлений;
- Общие параметры программы;
- Названия и параметры задач.

Принципы работы с отчетами

Информация о производительности задач Kaspersky Endpoint Security регистрируется в отчетах.

Данные в отчете представлены в виде таблицы, которая содержит список событий. Каждая строка в таблице содержит информацию об отдельном событии. Атрибуты события расположены в графах таблицы. События, зарегистрированные в работе разных задач, имеют разный набор атрибутов.

Доступны следующие отчеты, перечисленные в меню слева:

- **Статистика**. Содержит статистические данные о задаче Защита от файловых угроз и задачах антивирусной проверки. Вы можете обновить отображаемый отчет, нажав на кнопку **Обновить**.

  При остановке задачи Защита от файловых угроз происходит сброс статистики. Сброса статистики для задач антивирусной проверки не происходит. Вместо этого статистика накапливается за время, пока программа установлена на компьютере.

- **Системный аудит**. Этот отчет содержит информацию о событиях, которые произошли во время взаимодействия пользователя с программой. Он также содержит информацию о событиях, которые произошли во время обычной работы программы.

- **Защита от угроз**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы следующих компонентов Kaspersky Endpoint Security:

  - Защита от шифрования
  - Контроль целостности системы
  - Управление сетевым экраном
  - Защита от веб-угроз
  - 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 Kaspersky Endpoint Security:
    - Задачи проверки
    - Обновление
    - Проверка целостности

В отчетах применяются следующие уровни важности событий:

- **Информационные события**. События справочного характера, как правило, не содержащие важной информации.
- **Важные события**. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе Kaspersky Endpoint Security.
- **Критические события**. События критической важности, указывающие на проблемы в работе Kaspersky Endpoint Security или на уязвимости в защите компьютера пользователя.

Для удобства работы с отчетами вы можете изменять представление данных на экране следующими способами:

- отфильтровать список событий по времени;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке.

Просмотр отчетов

Чтобы просмотреть отчеты, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части главного окна программы нажмите на кнопку **Отчеты**.

   Откроется окно **Отчеты**.

3. Чтобы просмотреть конкретный отчет, в левой части окна **Отчеты** выберите нужную задачу из списка задач.

   В правой части окна отобразится отчет, содержащий список событий о работе выбранной задачи Kaspersky Endpoint Security.

   По умолчанию события в отчете отсортированы по возрастанию значений графы **Дата**. Вы можете выбрать другой порядок, щелкнув заголовок нужной графы.

4. Чтобы просмотреть в отчете подробную сводную информацию о каждом событии, выберите соответствующее событие в отчете.

   Сводная информация о событии отображается в нижней части окна.

Просмотр объектов в хранилище

Чтобы просмотреть объекты, которые Kaspersky Endpoint Security переместил в хранилище, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Хранилище**.

   В открывшемся окне отображается информация об объектах в хранилище.

Вы можете просмотреть следующую информацию об объектах в хранилище:

- название угрозы;
- полный путь к объекту;
- дата перемещения объекта в хранилище;
- дата удаления объекта из хранилища. Это поле отображается, если указан параметр `DaysToLive`;
- размер объекта.

Вы можете восстановить объекты из хранилища в их оригинальные директории. Вы также можете удалить объекты из хранилища. Удаленные объекты восстановить невозможно. Информация об этих действиях записывается в журнал событий.

Создание файла трассировки

Чтобы создать файл трассировки, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Поддержка**.

3. В окне **Поддержка** нажмите на кнопку **Трассировка**.

4. В раскрывающемся списке **Уровень** выберите уровень трассировки.

   Рекомендуется уточнить необходимый уровень трассировки у специалиста из Службы технической поддержки "Лаборатории Касперского". По умолчанию для уровня трассировки установлено значение **Диагностический (300)**.

5. Чтобы запустить процесс трассировки, нажмите на кнопку **Включить**.

6. Чтобы остановить процесс трассировки, нажмите на кнопку **Отключить**.

Созданные файлы трассировки хранятся в директории /var/log/kaspersky/kesl/. В файлах трассировки содержится информация об операционной системе, а также могут содержаться персональные данные.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского". Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки .

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить по телефону. Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной или интернациональной Службы технической поддержки.

- Отправить запрос с портала My Kaspersky. Этот метод позволяет вам связаться с нашими специалистами с помощью формы запроса.

Техническая поддержка доступна только пользователям, которые приобрели лицензию на использование программы. Техническая поддержка не предоставляется пользователям, использующим пробные версии.

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки Лаборатории Касперского. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского".

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. Вы можете использовать Kaspersky CompanyAccount для отслеживания статуса ваших онлайн-запросов и хранения их истории.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки .

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.

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 Kaspersky Endpoint Security 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 антивирусных баз).

Содержимой файлов дампа и их хранение

> Сохраненные файлы дампа могут содержать персональные данные. Чтобы обеспечить контроль и ограничение доступа к данным, необходимо самостоятельно позаботься о безопасности файлов дампа.

Файлы дампа формируются автоматически при сбое программы и хранятся на компьютере в течение всего времени использования программы. Файлы дампа удаляются без возможности восстановления при удалении программы.

Файлы дампа хранятся в директории /var/opt/kaspersky/kesl.

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security на момент создания файла дампа. Файл дампа может также содержать персональные данные.

Для доступа к файлам дампа требуются root-права.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Конфигурационные файлы задачи по умолчанию

Этот раздел содержит информацию о конфигурационных файлах по умолчанию для задач Kaspersky Endpoint Security.

Конфигурационные файлы можно изменить в любой момент. Вы также можете изменить значения параметров из командной строки.

Правила редактирования конфигурационных файлов Kaspersky Endpoint Security

При редактировании конфигурационного файла соблюдайте следующие правила:

- В конфигурационном файле необходимо указать все обязательные параметры. Отдельные параметры задачи можно указать без файла, с помощью командной строки.
- Если параметр принадлежит к какой-либо секции, помещайте его только в этой секции. В пределах одной секции вы можете помещать параметры в любом порядке.
- Заключайте имена секций в квадратные скобки [ ].
- Вводите значения параметров в формате имя параметра=значение (пробелы между именем параметра и его значением не обрабатываются).

  Пример:

  ```
  [ScanScope.item_0000]
  AreaDesc=Home
  AreaMask.item_0000=*doc
  Path=/home
  ```

  Символы "пробел" и "табуляция" игнорируются перед первой кавычкой и после последней кавычки строкового значения, а также в начале и в конце строкового значения, не заключенного в кавычки.
- Если вам нужно указать несколько значений параметра, повторите параметр столько раз, сколько значений вы хотите указать.

  Пример:

  ```
  AreaMask.item_0000=*xml
  AreaMask.item_0001=*doc
  ```

- Соблюдайте регистр при вводе значений параметров следующих типов:
  - имена (маски) проверяемых объектов и объектов исключения;
  - названия (маски) угроз;

При вводе остальных значений параметров соблюдать регистр не требуется.

- Указывайте значения параметров булевского типа следующим образом: `Yes – No`.
- Заключайте в кавычки строковые значения, содержащие символ "пробел" (например, имена файлов и директорий, пути к ним; выражения, содержащие дату и время в формате "ГГГГ-ММ-ДД ЧЧ:ММ:СС").

  Остальные значения вы можете вводить как в кавычках, так и без них.

  Пример:

  ```
  AreaDesc="Проверка почтовых баз"
  ```

Одиночная кавычка в начале или в конце строки считается ошибкой.

Конфигурационный файл задачи Защита от файловых угроз

```
ScanArchived=No

ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

TimeLimit=60

SizeLimit=0

FirstAction=Recommended

SecondAction=Block

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No
```

```
ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanByAccessType=SmartCheck

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Конфигурационный файл задачи Антивирусная проверка

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

ScanPriority=Idle

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No
```

```
ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Конфигурационный файл задачи Выборочная проверка

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

ScanPriority=Normal

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No
```

```
ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Конфигурационный файл задачи Проверка загрузочных секторов

```
UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

Action=Disinfect
```

Конфигурационный файл задачи Проверка памяти процессов

```
UseExcludeThreats=No

ReportCleanObjects=No

ReportUnprocessedObjects=No
```

```
Action=Disinfect
```

Конфигурационный файл задачи Обновление

```
SourceType="KLServers"

UseKLServersWhenUnavailable=Yes

IgnoreProxySettingsForKLServers=No

IgnoreProxySettingsForCustomSources=No

ApplicationUpdateMode=DownloadOnly

ConnectionTimeout=10
```

Конфигурационный файл задачи Управление Хранилищем

```
DaysToLive=90

BackupSizeLimit=0

BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

Конфигурационный файл задачи Управление сетевым экраном

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

[NetworkZonesTrusted]

[NetworkZonesLocal]

[NetworkZonesPublic]
```

Конфигурационный файл задачи 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 folders

UseScanArea=Yes

Path=AllShared

AreaMask.item_0000=*
```

Конфигурационный файл задачи Защита от веб-угроз

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Конфигурационный файл задачи Контроль устройств

```
[DeviceClass]
HardDrive=DependsOnBus
RemovableDrive=DependsOnBus
Printer=DependsOnBus
FloppyDrive=DependsOnBus
OpticalDrive=DependsOnBus
Modem=DependsOnBus
TapeDrive=DependsOnBus
MultifuncDevice=DependsOnBus
SmartCardReader=DependsOnBus
PortableDevice=DependsOnBus
WiFiAdapter=DependsOnBus
NetworkAdapter=DependsOnBus
BluetoothDevice=DependsOnBus
ImagingDevice=DependsOnBus
SerialPortDevice=DependsOnBus
ParallelPortDevice=DependsOnBus
InputDevice=DependsOnBus
SoundAdapter=DependsOnBus
[DeviceBus]
USB=Allow
FireWire=Allow
```

Конфигурационный файл задачи Проверка съемных дисков

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Конфигурационный файл задачи Защита от сетевых угроз

```
BlockAttackingHosts=Yes

BlockDurationMinutes=60

UseExcludeIPs=No
```

Конфигурационный файл задачи Сканирование контейнеров

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=120

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=Idle

ContainerScanAction=StopContainerIfFailed

ImageAction=Skip
```

Для пользовательской задачи Сканирование контейнеров можно использовать этот же конфигурационный файл.

Настройка совместной работы: Антивирус Касперского для Linux Mail Server

Чтобы настроить совместную работу Kaspersky Endpoint Security с Антивирусом Касперского для Linux Mail Server, выполните следующие действия:

1. Сохраните параметры задачи Защита от файловых угроз в конфигурационном файле с помощью следующей команды:

   ```
   kesl-control --get-settings 1 --file <полный путь к файлу>
   ```

2. Откройте созданный конфигурационный файл для редактирования.

3. Добавьте в созданный файл следующий раздел:

   ```
   [ExcludedFromScanScope.item_<номер элемента>]
   Path=/var/opt/kaspersky/klms
   ```

4. Повторите указанный выше раздел для всех почтовых агентов, интегрированных с Антивирусом Касперского для Linux Mail Server.

5. Для исключения из проверки временной директории фильтров и служб Антивируса Касперского для Linux Mail Server добавьте в созданный файл следующую секцию:

```
[ExcludedFromScanScope.item_<номер элемента>]
Path=/tmp/klmstmp
```

6. Сохраните изменения в конфигурационном файле.
7. Импортируйте параметры из конфигурационного файла в задачу Защита от файловых угроз с помощью следующей команды:

   ```
   kesl-control --set-settings 1 --file <полный путь к файлу>
   ```

Коды возврата командной строки

В этом разделе приведено описание кодов возврата командной строки.

0 – команда / задача выполнена успешно;

1 – общая ошибка в аргументах команды;

2 – ошибка в переданных настройках программы;

64 – Kaspersky Endpoint Security не запущен;

66 – антивирусные базы не загружены (используется только командой `kesl-control --app-info`);

67 – активация 2.0 завершилась с ошибкой из-за сетевых проблем;

68 – выполнение команды невозможно, так как программа работает под политикой;

128 – неизвестная ошибка;

65 – все остальные ошибки.

Источники информации о программе

Страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security, расположенной на веб-сайте Лаборатории Касперского, вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Endpoint Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Endpoint Security в Базе знаний приведены статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и другими пользователями в нашем сообществе.

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

> Для доступа к ресурсам веб-сайта требуется подключение к интернету.

Если вы не нашли решения своей проблемы, обратитесь в Службу технической поддержки.

Глоссарий

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать вредоносный код в проверяемых объектах. Антивирусные базы создаются специалистами "Лаборатории Касперского" и обновляются каждый час.

Группа администрирования

Набор устройств, сгруппированный по функциям и установленным программам "Лаборатории Касперского". Устройства объединены в одну группу для удобства управления. В состав группы могут входить другие группы. Групповые политики и групповые задачи можно создавать для каждой из программ, установленных в рамках одной группы.

Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех клиентских устройствах, входящих в состав этой группы администрирования.

Задача

Операции в программе "Лаборатории Касперского" реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз программы.

Задача для набора устройств

Задача, назначенная набору клиентских устройств из произвольной группы администрирования и выполняемая на этих устройствах.

Зараженный объект

Объект, часть кода которого полностью совпадает с частью кода известной вредоносной программы. "Лаборатория Касперского" не рекомендует открывать такие объекты.

Защита от файловых угроз (Файловый антивирус)

Компонент программы безопасности, расположенный в оперативной памяти устройства и выполняющий проверку всех открытых, сохраненных и исполняемых файлов. По умолчанию, для этого компонента настроены параметры, рекомендованные специалистами "Лаборатории Касперского".

Исключение

Исключение – это объект, исключенный из проверки программой "Лаборатории Касперского". Вы можете исключить из проверки файлы определенных форматов, маски файлов, определенную область (например, папку или программу), процесс программы или объект по типу угрозы, согласно классификации Вирусной энциклопедии. Для каждой задачи можно назначить набор исключений.

Код активации

Код, который вы получаете при приобретении лицензии Kaspersky Endpoint Security. Этот код необходим для активации программы.

Код активации представляет собой последовательность из 20 букв и цифр в формате xxxxx-xxxxx-xxxxx-xxxxx.

Лечение

Способ обработки зараженных объектов, в результате которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, предоставляемый "Лабораторией Касперского" вместе с файлом ключа или кодом активации. Этот документ содержит информацию о предоставляемой лицензии.

Лицензия

Ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Маска файла

Представление имени файла с подстановочными знаками. Стандартными подстановочными символами в масках файлов являются * и ?, где * – любое количество символов, а ? – любой отдельный символ.

Обновление

Функция программы "Лаборатории Касперского", позволяющая ей поддерживать защиту компьютера в актуальном состоянии. Во время обновления программа загружает обновления для своих баз и модулей с серверов обновлений "Лаборатории Касперского", а затем автоматически устанавливает и применяет их.

Параметры задачи

Параметры программы, специфические для каждого типа задачи.

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

Плагин управления

Специализированный компонент, который обеспечивает интерфейс для управления программой через Консоль администрирования. У каждой программы есть собственный плагин. Он включен во все программы "Лаборатории Касперского", которыми можно управлять через Kaspersky Endpoint Security.

Подписка

Позволяет эксплуатировать программу согласно выбранным характеристикам (таким как дата окончания срока действия или количество устройств). Подписку можно приостановить или возобновить, автоматически продлить или отменить.

Политика

Политика определяет параметры программы и управляет доступом к настройке программы, установленной на компьютерах в рамках группы администрирования. Для каждой программы необходимо создавать отдельную политику. Вы можете создать неограниченное количество различных политик для программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

Потенциально заражаемый объект

Объект, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например с расширением .com, .exe или .dll. Риск проникновения вредоносного кода в такие файлы весьма высок.

Прокси-сервер

Служба в компьютерных сетях, через которую пользователи могут выполнять косвенные запросы к другим сетевым службам. Сначала пользователь подключается к прокси-серверу и запрашивает ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос пользователя или ответ сервера может быть изменен прокси-сервером в определенных целях.

Резервное хранилище

Специальное хранилище для резервных копий файлов, которые создаются перед попыткой лечения или удаления.

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского". Его также можно использовать для управления этими программами.

Серверы обновлений "Лаборатории Касперского"

Список HTTP- и FTP-серверов "Лаборатории Касперского", с которых программа загружает обновления баз на мобильные устройства.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в директории установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Amazon – товарный знак или зарегистрированные в США и / или других странах товарный знак, принадлежащий Amazon.com, Inc. или аффилированным компаниям.

FireWire – товарный знак Apple Inc., зарегистрированный в США и других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Core – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Active Directory, Microsoft, Outlook, Outlook Express и Windows – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Novell – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

JavaScript и Oracle – зарегистрированные товарные знаки Oracle Corporation и (или) ее аффилированных компаний.

CentOS, Red Hat и Red Hat Enterprise Linux – товарные знаки Red Hat Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.