kaspersky

Kaspersky Endpoint Security для Linux

Содержание

О Kaspersky Endpoint Security 12.1 для Linux

Приложение Kaspersky Endpoint Security 12.1 для Linux (далее также Kaspersky Endpoint Security, приложение) предназначено для защиты устройств под управлением операционных систем Linux® от различного вида угроз, сетевых и мошеннических атак.

Приложение позволяет защищать как физические устройства, так и виртуальные машины. Вы можете использовать приложение Kaspersky Endpoint Security в составе решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.

Основные функции защиты и контроля устройств обеспечиваются следующими функциональными компонентами и задачами приложения:

- **Защита от файловых угроз** позволяет избежать заражения файловой системы устройства пользователя. Компонент *Защита от файловых угроз* запускается автоматически при запуске Kaspersky Endpoint Security и в реальном времени проверяет все открываемые, сохраняемые и запускаемые файлы.

  Вы также можете выполнять проверку защищаемых устройств по требованию с помощью следующих задач проверки:

  - **Поиск вредоносного ПО**. Приложение проверяет на наличие вредоносного ПО объекты файловой системы, расположенные на локальных дисках устройства, а также смонтированные и разделяемые ресурсы, доступ к которым предоставляется по протоколам SMB и NFS. Вы можете использовать эту задачу для полной или выборочной проверки устройства.

  - **Проверка важных областей**. Приложение проверяет загрузочные секторы, объекты автозапуска, память процессов и память ядра.

- **Проверка съемных дисков**. Компонент *Проверка съемных дисков* позволяет в реальном времени контролировать подключение съемных дисков к устройству и проверять съемный диск и его загрузочные секторы на наличие вредоносного ПО. Kaspersky Endpoint Security может проверять следующие съемные диски: CD/DVD-приводы, Blu-ray диски, флеш-накопители (включая USB-модемы), внешние жесткие диски и дискеты.

- **Проверка контейнеров**. Компонент *Мониторинг контейнеров* позволяет в реальном времени проверять пространства имен и запущенные контейнеры на наличие вредоносного ПО. Поддерживается интеграция с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc. С помощью задачи *Проверка контейнеров* вы можете выполнять проверку контейнеров и образов по требованию.

- **Защита от веб-угроз**. Компонент *Защита от веб-угроз* позволяет проверять входящий трафик, не допускать загрузки вредоносных файлов из интернета, а также блокировать фишинговые, рекламные и прочие опасные веб-сайты. Kaspersky Endpoint Security может проверять защищенные соединения.

- **Защита от сетевых угроз**. Компонент *Защита от сетевых угроз* позволяет проверять входящий сетевой трафик на действия, характерные для сетевых атак.

- **Управление сетевым экраном**. Компонент *Управление сетевым экраном* позволяет контролировать параметры сетевого экрана операционной системы и фильтровать всю сетевую активность в соответствии с сетевыми пакетными правилами, которые вы настроили.

- **Защита от шифрования**. Компонент *Защита от шифрования* позволяет проверять обращения удаленных устройств к файлам, расположенным в локальных директориях с сетевым доступом по протоколам SMB/NFS, и защищать файлы от удаленного вредоносного шифрования.

- **Контроль устройств**. Компонент *Контроль устройств* позволяет управлять доступом пользователей к устройствам, которые установлены на клиентском устройстве или подключены к нему (например, жестким дискам, камерам или модулям Wi-Fi). Это позволяет защитить клиентское устройство от

заражения при подключении внешних устройств и предотвратить потерю или утечку данных. Доступ пользователей к устройствам регулируется с помощью режимов доступа и правил доступа, которые вы настроили.

- **Контроль приложений**. Компонент *Контроль приложений* позволяет управлять запуском приложений на устройствах пользователей. Это снижает риск заражения устройства за счет ограничения доступа к приложениям. Запуск приложений регулируется с помощью правил контроля приложений, которые вы настроили.

- **Инвентаризация**. Задача *Инвентаризация* позволяет получить информацию обо всех исполняемых файлах приложений, хранящихся на клиентских устройствах. Эта информация может быть полезна, например, для создания правил контроля приложений.

- **Веб-Контроль**. Компонент *Веб-Контроль* управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть веб-сайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security заблокирует доступ или покажет предупреждение.

- **Анализ поведения**. Компонент *Анализ поведения* позволяет контролировать вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности Kaspersky Endpoint Security может завершать процесс приложения, осуществляющего вредоносную активность.

- **Контроль целостности системы** позволяет отслеживать изменения файлов и директорий операционной системы. Компонент *Контроль целостности системы* в реальном времени отслеживает действия, выполняемые с объектами из области мониторинга, указанной в параметрах компонента. С помощью задачи *Проверка целостности системы* вы можете выполнять проверку целостности системы по требованию. Проверка осуществляется путем сравнения текущего состояния объектов, включенных в область мониторинга, с исходным состоянием этих объектов, зафиксированным предварительно в виде снимка состояния системы.

Kaspersky Endpoint Security позволяет обнаруживать зараженные объекты и обезвреживать обнаруженные в них угрозы. При этом приложение может использовать:

- Базы приложения для поиска и лечения зараженных файлов. Во время процесса проверки приложение анализирует каждый файл на наличие угрозы: сравнивает код файла с кодом конкретной угрозы и ищет возможные совпадения.

- Kaspersky Security Network. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложения Kaspersky Endpoint Security на различные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Перед лечением или удалением Kaspersky Endpoint Security сохраняет резервные копии файлов в резервном хранилище, расположенном на устройстве. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете восстановить файл из его копии.

Во время выполнения задач проверки Kaspersky Endpoint Security может лечить и удалять файлы, защищенные от изменения: файлы с атрибутами immutable и append-only и файлы в директориях с атрибутами immutable и append-only. В резервном хранилище сохраняются копии этих файлов, созданные до лечения или удаления. Вы можете восстанавливать файлы из резервных копий, если требуется. После выполнения задач проверки атрибуты immutable и append-only вылеченных файлов сбрасываются.

Приложение Kaspersky Endpoint Security может работать в информирующем режиме. *Информирующий режим* – это такой режим работы приложения, при котором в случае обнаружения угрозы компоненты и задачи приложения не пытаются лечить или удалять вредоносные объекты, запрещать доступ или блокировать активность приложений, а только информируют пользователя об обнаружении угрозы.

Kaspersky Endpoint Security поддерживает возможность интеграции с другими решениями "Лаборатории Касперского" для расширения возможностей использования приложения:

- Интеграция с Kaspersky Managed Detection and Response обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.
- Интеграция с Kaspersky Endpoint Detection and Response (KATA), компонентом решения Kaspersky Anti Targeted Attack Platform обеспечивает защиту IT-инфраструктуры организации и своевременное обнаружение таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats.
- Интеграция с Kaspersky Endpoint Detection and Response Optimum обеспечивает защиту IT-инфраструктуры организации от таких угроз, как эксплойты (англ. exploits), программы-вымогатели (англ. ransomware), бесфайловые атаки (англ. fileless attacks) и использование злоумышленниками законных системных инструментов для нанесения вреда устройствам или данным.

Вы можете использовать Kaspersky Endpoint Security как контейнерное приложение (далее KESL-контейнер) для встраивания во внешние системы с целью проверки образов контейнеров из репозиториев.

Функционал KESL-контейнера не поддерживается, если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Для поддержки приложения в актуальном состоянии предусмотрены дополнительные функции приложения:

- Активация приложения с помощью файла ключа или кода активации.

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент).

- Обновление баз и модулей приложения с серверов обновлений "Лаборатории Касперского", через Сервер администрирования или из указанного пользователем источника по расписанию и по требованию.

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, приложение получает обновление баз и программных модулей от Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент).

- Разграничение доступа пользователей к функциям приложения в соответствии с ролями пользователей.
- Уведомление администратора о событиях, произошедших во время работы приложения.
- Проверка целостности компонентов приложения с помощью утилиты проверки целостности.

Вы можете управлять приложением Kaspersky Endpoint Security следующими способами:

- С помощью Kaspersky Security Center через Kaspersky Security Center Web Console, Kaspersky Security Center Cloud Console или Консоль администрирования.
- С помощью команд управления из командной строки.
- С помощью графического пользовательского интерфейса.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, управление приложением с помощью Kaspersky Security Center Cloud Console и графического пользовательского интерфейса недоступно.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN будут недоступны в приложении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

О режимах использования приложения Kaspersky Endpoint Security

Вы можете использовать Kaspersky Endpoint Security в одном из следующих режимов:

- В стандартном режиме для защиты рабочих станций и серверов (далее также "Стандартный режим"). Kaspersky Endpoint Security используется как автономное приложение для защиты устройств под управлением операционных систем Linux.
- В режиме Легкого агента для защиты виртуальных сред в составе решения Kaspersky Security для виртуальных сред Легкий агент (далее также "Режим Легкого агента"). Kaspersky Endpoint Security используется как компонент Легкий агент решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.

По умолчанию приложение используется в стандартном режиме.

Если вы хотите использовать приложение в режиме Легкого агента, вам нужно выполнить следующие действия:

1. Установить Kaspersky Endpoint Security на каждой виртуальной машине, которую требуется защищать с помощью решения Kaspersky Security для виртуальных сред Легкий агент. Вы также можете установить приложение на шаблоне виртуальных машин.

   В ходе установки вам нужно указать, что приложение будет использоваться в режиме Легкого агента, одним из следующих способов:

   - во время первоначальной настройки приложения в интерактивном или автоматическом режиме (в случае установки с помощью командной строки);
   - в свойствах инсталляционного пакета приложения или в конфигурационном файле autoinstall.ini, который включен в инсталляционный пакет (в случае установки с помощью Kaspersky Security Center).

   После установки Kaspersky Endpoint Security изменить режим использования приложения невозможно.

   При выборе режима Легкого агента вы также можете настроить следующие параметры работы Kaspersky Endpoint Security в режиме Легкого агента:

   - Роль виртуальной машины, которую вы хотите защищать, в виртуальной инфраструктуре: сервер или рабочая станция. Роль виртуальной машины определяет, по какой лицензии будет использоваться приложение на этой виртуальной машине, и объем доступной функциональности.
   - Режим защиты инфраструктуры VDI. Рекомендуется включить этот режим, если вы устанавливаете приложение на шаблон виртуальных машин, из которого будут создаваться временные виртуальные

машины. Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах.

2. Настроить параметры подключения Легкого агента к SVM и параметры подключения Легкого агента к Серверу интеграции.

   Kaspersky Endpoint Security в режиме Легкого агента взаимодействует с другими компонентами решения Kaspersky Security для виртуальных сред Легкий агент: Сервером интеграции и Сервером защиты, установленным на SVM (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент). Для взаимодействия с Сервером защиты Kaspersky Endpoint Security устанавливает и поддерживает подключение к SVM, на которой установлен этот Сервер защиты.

   Подключение к Серверу интеграции требуется, если вы хотите, чтобы Легкие агенты получали информацию об SVM через Сервер интеграции, или если вы хотите защищать соединение между Сервером защиты и Легким агентом.

   Вы можете настроить параметры подключения в свойствах политики Kaspersky Endpoint Security с помощью Консоли администрирования Kaspersky Security Center или с помощью Kaspersky Security Center Web Console.

Информацию о параметрах работы приложения в режиме Легкого агента, о подключении к Серверу интеграции и к SVM вы можете получить с помощью команд приложения: `kesl-control --ksvla-info`, `kesl-control --viis-info` и `kesl-control --svm-info`.

Информация о режиме использования приложения отображается в Kaspersky Security Center в свойствах приложения Kaspersky Endpoint Security на управляемом устройстве в разделе **Компоненты**. Информация отображается в строке **Режим Легкого агента для защиты виртуальных сред** следующим образом:

- статус *выполняется* означает, что приложение используется в режиме Легкого агента;
- статус *не установлено* означает, что приложение используется в стандартном режиме.

Об активации приложения в режиме Легкого агента

Если Kaspersky Endpoint Security используется в режиме Легкого агента, отдельно активировать приложение не требуется. Вы активируете решение Kaspersky Security для виртуальных сред Легкий агент. Активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионного ключа на SVM. См. подробнее в справке Kaspersky Security для виртуальных сред Легкий агент.

> Для активации функциональности Kaspersky Endpoint Detection and Response Optimum дополнительно требуется добавить на SVM лицензионный ключ EDR Optimum. Лицензии, предназначенные для активации компонентов решения Kaspersky Security для виртуальных сред Легкий агент, не включают эту функциональность.

После активации решения и подключения Легкого агента к SVM компонент Сервер защиты передает информацию о лицензии Легкому агенту. При выборе SVM для подключения Легкий агент учитывает среди прочих параметров тип лицензионного ключа, добавленного на SVM. Легкий агент не подключается к SVM, если тип ключа, добавленного на SVM, не соответствует роли защищенной виртуальной машины в виртуальной инфраструктуре (сервер или рабочая станция). См. подробнее в справке Kaspersky Security для виртуальных сред Легкий агент.

Информацию о лицензии, по которой используется Легкий агент для Linux, вы можете посмотреть на защищенной виртуальной машине с Легким агентом с помощью команды `kesl-control -L --query`.

Не поддерживается управление лицензионными ключами с помощью задачи Kaspersky Endpoint Security *Добавление ключа* и с помощью команд Kaspersky Endpoint Security для добавления и удаления лицензионных ключей.

Об обновлении баз и модулей приложения в режиме Легкого агента

Kaspersky Endpoint Security в режиме Легкого агента использует специальные базы вредоносного ПО, необходимые для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Kaspersky Endpoint Security получает от Сервера защиты обновления баз и программных модулей. См. подробнее в справке Kaspersky Security для виртуальных сред Легкий агент.

Обновление баз и модулей на защищенных виртуальных машинах выполняется с помощью специальной локальной задачи приложения Kaspersky Endpoint Security *Обновление*, в которой в качестве источника обновлений указана папка на SVM. Задача обновления запускается автоматически. Вы не можете удалять эту задачу и изменять ее параметры.

Не поддерживается обновление из источников, отличных от папки на SVM, и использование групповых задач обновления.

Откат последнего обновления баз вредоносного ПО также выполняется на стороне Сервера защиты. После отката обновления баз и программных модулей на SVM на защищенной виртуальной машине автоматически запускается специальная локальная задача *Обновление*. В результате выполнения задачи Легкий агент возвращается к использованию предыдущего набора баз вредоносного ПО.

Не поддерживается использование локальной и групповой задачи приложения Kaspersky Endpoint Security *Откат обновления баз*.

Другие особенности использования приложения в режиме Легкого агента

Если Kaspersky Endpoint Security используется в режиме Легкого агента:

- Не поддерживается функциональность KESL-контейнера.
- Недоступно управление приложением с помощью Kaspersky Security Center Cloud Console и графического пользовательского интерфейса.
- Не поддерживается использование облачных баз.
- Kaspersky Endpoint Security взаимодействует с серверами KSN с помощью прокси-сервера KSN. Взаимодействие с KSN напрямую не поддерживается.
- Использование прокси-сервера приложения не поддерживается при подключении к Серверу интеграции, к SVM и к серверам KSN.
- Не поддерживается возможность интеграции с Kaspersky Symphony XDR.

Комплект поставки

На веб-сайте "Лаборатории Касперского" вы можете скачать файлы, которые входят в комплект поставки приложения Kaspersky Endpoint Security, а также файлы, используемые в процедуре удаленной установки приложения с помощью Kaspersky Security Center.

В комплект поставки приложения Kaspersky Endpoint Security входят следующие файлы:

- kesl-12.1.0-<номер сборки>.i386.rpm, kesl_12.1.0-<номер сборки>_i386.deb

  Содержат основные файлы приложения. Пакеты могут быть установлены на 32-битные операционные системы в соответствии с типом менеджера пакетов.

- kesl-12.1.0-<номер сборки>.x86_64.rpm, kesl_12.1.0-<номер сборки>_amd64.deb

  Содержат основные файлы приложения. Пакеты могут быть установлены на 64-битные операционные системы в соответствии с типом менеджера пакетов.

- kesl-12.1.0-<номер сборки>.aarch64.rpm, kesl_12.1.0-<номер сборки>_arm64.deb

  Содержат основные файлы приложения. Пакеты могут быть установлены на 64-битные операционные системы для архитектуры Arm® в соответствии с типом менеджера пакетов.

- kesl-gui-12.1.0-<номер сборки>.i386.rpm, kesl-gui_12.1.0-<номер сборки>_i386.deb

  Содержат файлы графического интерфейса приложения. Пакеты могут быть установлены на 32-битные операционные системы в соответствии с типом менеджера пакетов.

- kesl-gui-12.1.0-<номер сборки>.x86_64.rpm, kesl-gui_12.1.0-<номер сборки>_amd64.deb

  Содержат файлы графического интерфейса приложения. Пакеты могут быть установлены на 64-битные операционные системы в соответствии с типом менеджера пакетов.

- kesl-gui-12.1.0-<номер сборки>.aarch64.rpm, kesl-gui_12.1.0-<номер сборки>_arm64.deb

  Содержат файлы графического интерфейса приложения. Пакеты могут быть установлены на 64-битные операционные системы для архитектуры Arm в соответствии с типом менеджера пакетов.

- kesl-12.1.0.<номер сборки>.zip

  Содержит файлы, используемые в процедуре удаленной установки приложения с помощью Kaspersky Security Center, включая файлы license.<идентификатор языка> и ksn_license.<идентификатор языка>.

  > Агент администрирования Kaspersky Security Center не входит в комплект поставки. Вы можете скачать его на странице загрузки приложений в разделе **Kaspersky Security Center**.

- docker-service-kesl64-12.1.0-<номер сборки>.tgz

  Содержит файлы для создания образа контейнерного приложения KESL-контейнер.

- ksn_license.<идентификатор языка>

  Содержит текст Положения о Kaspersky Security Network.

- license.<идентификатор языка>

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

Самостоятельное изменение файлов приложения способами, не описанными в документации к приложению или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе приложения и операционной системы, снижению уровня защиты вашего устройства, к нарушению доступности и целостности обрабатываемой информации, а также включению отсылки дополнительных статистик KSN.

Аппаратные и программные требования

Этот раздел содержит аппаратные и программные требования приложения Kaspersky Endpoint Security.

Аппаратные требования

Приложение Kaspersky Endpoint Security имеет следующие аппаратные требования:

Минимальные аппаратные требования:

- процессор Core™ 2 Duo 1.86 ГГц или выше;
- раздел подкачки не менее 1 ГБ;
- 1 ГБ оперативной памяти для 32-битных операционных систем, 2 ГБ оперативной памяти для 64-битных операционных систем;
- 4 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов;
- при использовании графического пользовательского интерфейса монитор должен обеспечивать отображение окон шириной 1000 пикселей и высотой 600 пикселей (если применяется масштабирование экрана, то эти размеры также масштабируются);
- если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.

Минимальные аппаратные требования для архитектуры Arm:

- процессор Armv8.2-A Kunpeng 920 или Armv8-A Baikal-M (BE-M1000) или платформа m-TrusT Терминал;
- раздел подкачки не менее 1 ГБ;
- 2 ГБ оперативной памяти;
- 3 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов;
- при использовании графического пользовательского интерфейса монитор должен обеспечивать отображение окон шириной 1000 пикселей и высотой 600 пикселей (если применяется масштабирование экрана, то эти размеры также масштабируются).

Использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред не поддерживается на операционных системах для архитектуры Arm.

Программные требования

Для установки Kaspersky Endpoint Security на устройстве должна быть установлена одна из следующих операционных систем:

- 32-битные операционные системы:
  - Debian GNU/Linux 11.0 и выше.
  - Debian GNU/Linux 12.0 и выше.
  - Mageia™ 4.

    На устройствах с операционной системой Mageia 4 не поддерживается интеграция приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA).
  - Альт 8 СП Рабочая Станция (8.4).
  - Альт 8 СП Сервер (8.4).
  - Альт СП Рабочая Станция релиз 10.
  - Альт СП Сервер релиз 10.
- 64-битные операционные системы:
  - AlmaLinux OS 8 и выше.
  - AlmaLinux OS 9 и выше.
  - AlterOS® 7.5 и выше.
  - Amazon™ Linux 2.
  - Astra Linux Common Edition 2.12.
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
  - Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).

На устройствах с операционными системами Astra Linux в режимах мандатного разграничения доступа и замкнутой программной среды не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

Работа операционной системы Astra на планшетном компьютере (планшете) в режиме "Мобильный" поддерживается только в десктопном виде.

- CentOS 7.2 и выше.
- CentOS Stream 8.
- CentOS Stream 9.
- Debian GNU/Linux 11.0 и выше.
- Debian GNU/Linux 12.0 и выше.
- EMIAS 1.0 и выше.
- EulerOS 2.0 SP10.
- Kylin 10.
- Linux Mint 20.3 и выше.
- Linux Mint 21.1 и выше.
- openSUSE Leap 15.0 и выше.
- Oracle Linux 7.3 и выше.
- Oracle Linux 8.0 и выше.
- Oracle Linux 9.0 и выше.
- Red Hat Enterprise Linux 7.2 и выше.
- Red Hat Enterprise Linux 8.0 и выше.
- Red Hat Enterprise Linux 9.0 и выше.
- Rocky Linux 8.5 и выше.
- Rocky Linux 9.1.
- SberLinux 8.8 (Dykhtau).
- SberOS 3.2.0.
- SUSE Linux Enterprise Server 12.5 и выше.
- SUSE Linux Enterprise Server 15 и выше.

- Ubuntu® 20.04 LTS.
- Ubuntu 22.04 LTS.
- Ubuntu 24.04 LTS.
- Альт 8 СП Рабочая станция (8.4).
- Альт 8 СП Сервер (8.4).
- Альт Образование 10.1.
- Альт Рабочая Станция 10.1.
- Альт Сервер 10.1.
- Альт СП Рабочая Станция релиз 10.
- Альт СП Сервер релиз 10.
- Атлант, сборка Alcyone, версия 2022.02.
- Гослинукс 7.17.
- Гослинукс 7.2.
- МСВСФЕРА 9.2 АРМ.
- МСВСФЕРА 9.2 СЕРВЕР.
- РЕД ОС® 7.3.
- РЕД ОС 8.0.
- РОСА "Кобальт" 7.9.
- РОСА "Хром" 12.
- СинтезМ-Клиент 8.6.
- СинтезМ-Сервер 8.6.

- 64-битные операционные системы для архитектуры Arm:
  - Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
  - CentOS Stream 9.
  - EulerOS 2.0 SP10.
  - SUSE Linux Enterprise Server 15.
  - Ubuntu 22.04 LTS.
  - Альт 8 СП Рабочая Станция (8.4).

- Альт 8 СП Сервер (8.4).
- Альт СП Рабочая Станция релиз 10.
- Альт СП Сервер релиз 10.
- РЕД ОС 7.3.

На устройствах с операционными системами для архитектуры Arm не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

Из-за ограничений технологии fanotify приложение не поддерживает работу со следующими файловыми системами: autofs, binfmt_misc, cgroup, configfs, debugfs, devpts, devtmpfs, fuse, fuse.gvfsd-fuse, gfs2, gvfs, hugetlbfs, mqueue, nfsd, proc, parsecfs, pipefs, pstore, usbfs, rpc_pipefs, securityfs, selinuxfs, sysfs, tracefs.

Поддерживаемые версии Kaspersky Security Center

Приложение Kaspersky Endpoint Security совместимо с приложением Kaspersky Security Center следующих версий:

- Kaspersky Security Center 13.2. Поддерживается управление приложением Kaspersky Endpoint Security через Консоль администрирования с помощью mmc-плагина управления.
- Kaspersky Security Center 14. Поддерживается управление приложением Kaspersky Endpoint Security через Консоль администрирования с помощью mmc-плагина управления и через Kaspersky Security Center Web Console с помощью веб-плагина управления.
- Kaspersky Security Center 14.2 Windows. Поддерживается управление приложением Kaspersky Endpoint Security через Консоль администрирования с помощью mmc-плагина управления и через Kaspersky Security Center Web Console с помощью веб-плагина управления.
- Kaspersky Security Center 14.2 Linux. Поддерживается управление приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console с помощью веб-плагина управления.
- Kaspersky Security Center 15 Linux. Поддерживается управление приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console с помощью веб-плагина управления.
- Kaspersky Security Center 15.1 Linux. Поддерживается управление приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console с помощью веб-плагина управления.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент), для управления приложением рекомендуется использовать Kaspersky Security Center следующих версий:

- Kaspersky Security Center 14.2 Windows.
- Kaspersky Security Center 15 Linux.
- Kaspersky Security Center 15.1 Linux.

Для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center требуется Агент администрирования Kaspersky Security Center.

Агент администрирования Kaspersky Security Center не входит в комплект поставки Kaspersky Endpoint Security. Вы можете скачать его на странице загрузки приложений в разделе **Kaspersky Security Center**.

Если вы используете интеграцию приложения с компонентом Kaspersky Endpoint Detection and Response (KATA), для управления приложением рекомендуется использовать Kaspersky Security Center следующих версий:

- Kaspersky Security Center 14.2 Windows.
- Kaspersky Security Center 15 Linux.
- Kaspersky Security Center 15.1 Linux.

Поддерживаемые версии Kaspersky Anti Targeted Attack Platform

Приложение Kaspersky Endpoint Security совместимо с решением Kaspersky Anti Targeted Attack Platform следующих версий:

- Kaspersky Anti Targeted Attack Platform 5.1. Поддерживается с ограничениями.
- Kaspersky Anti Targeted Attack Platform 6.0.
- Kaspersky Anti Targeted Attack Platform 6.1.

Подробнее о решении Kaspersky Anti Targeted Attack Platform см. в справке Kaspersky Anti Targeted Attack Platform.

Что нового

В приложении Kaspersky Endpoint Security появились следующие возможности и доработки:

- Реализована возможность интеграции с Kaspersky Endpoint Detection and Response Optimum, что обеспечивает защиту IT-инфраструктуры организации от таких угроз, как эксплойты (англ. exploits), программы-вымогатели (англ. ransomware), бесфайловые атаки (англ. fileless attacks) и использование злоумышленниками законных системных инструментов для нанесения вреда устройствам или данным.

- Реализована возможность добавлять в приложение два активных лицензионных ключа: основной ключ для активации приложения и дополнительный ключ для активации функциональности Kaspersky Endpoint Detection and Response Optimum. Дополнительный ключ требуется, если ваша основная лицензия не включает функциональность Kaspersky Endpoint Detection and Response Optimum.

- Добавлен новый функциональный компонент *Веб-Контроль*, который управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть веб-сайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security заблокирует доступ или покажет предупреждение.

- Реализована функция мониторинга стабильности работы Kaspersky Endpoint Security, которая позволяет отслеживать количество нештатных остановок приложения и уведомлять администратора о нестабильной работе приложения.

- Доработана процедура установки Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console: в свойствах инсталляционного пакета приложения теперь можно задавать параметры первоначальной настройки приложения, ранее доступные только в конфигурационном файле autoinstall.ini.

- Расширены возможности управления дополнительными параметрами приложения через Kaspersky Security Center Web Console и Консоль администрирования Kaspersky Security Center: вы можете настраивать параметры, которые ранее можно было настраивать только путем редактирования конфигурационного файла kesl.ini.

- Добавлена возможность включать и выключать использование глобальных исключений и исключений Защиты от файловых угроз при выполнении задач проверки.

- Реализована возможность интеграции с Kaspersky Symphony XDR: если приложение Kaspersky Endpoint Security используется в стандартном режиме, приложение может выполнять действия по реагированию "Запуск поиска вредоносного ПО" и "Обновление баз". Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, интеграция с Kaspersky Symphony XDR не поддерживается.

- Реализована передача на Сервер администрирования информации обо всех устройствах, установленных на клиентских устройствах или подключенных к ним (в том числе установленных и подключенных ранее и уже отключенных) при управлении приложением с помощью Kaspersky Security Center.

- Доработаны правила перехвата трафика для поддержки взаимодействия контейнеров в одной сети.

- Обновлен список поддерживаемых операционных систем.

Подготовка к установке приложения Kaspersky Endpoint Security

Общие действия

Перед началом установки приложения Kaspersky Endpoint Security вам нужно выполнить следующие действия:

- Проверить соответствие вашего устройства аппаратным и программным требованиям приложения.
- Убедиться в том, что на вашем устройстве не установлено стороннее антивирусное программное обеспечение.
- Убедиться в том, что на вашем устройстве не установлено приложение Kaspersky Endpoint Agent для Linux. Если приложение Kaspersky Endpoint Agent для Linux установлено, во время установки отобразится сообщение о необходимости удалить его вручную.
- Убедиться в том, что на вашем устройстве установлен интерпретатор языка Perl версии 5.10 или выше.
- Убедиться в том, что в системе установлена утилита semanage. Если утилита не установлена, установите пакет policycoreutils-python или policycoreutils-python-utils в зависимости от типа менеджера пакетов.
- На устройствах с операционными системами, не поддерживающими технологию fanotify, убедиться в том, что установлены:
  - пакеты для компиляции программ и запуска задач (gcc, binutils, glibc, glibc-devel, make);
  - пакет с заголовочными файлами ядра операционной системы для компиляции модулей Kaspersky Endpoint Security.
- В зависимости от операционной системы на вашем устройстве установить один из следующих пакетов:
  - На устройстве с операционной системой SUSE Linux Enterprise Server 15 установить пакет insserv-compat.
  - На устройстве с операционной системой Red Hat Enterprise Linux 8 или РЕД ОС установить пакет perl-Getopt-Long.
  - На устройстве с операционной системой Red Hat Enterprise Linux или РЕД ОС установить пакет perl-File-Copy. Этот пакет требуется для работы скрипта первоначальной настройки приложения, но по умолчанию может отсутствовать.
- В операционных системах Astra Linux по умолчанию включен запрет трассировки ptrace (Disable ptrace capability), который может влиять на работу приложения Kaspersky Endpoint Security. Для корректной работы Kaspersky Endpoint Security рекомендуется отключить запрет трассировки ptrace при установке Astra Linux. Если Astra Linux уже установлена, инструкцию по включению и выключению этого режима см. на сайте Справочного центра Astra Linux (**Настройка механизмов защиты и блокировок**, раздел **Блокировка трассировки ptrace**).
- Если на вашем устройстве используется ядро Linux ниже 3.16, то для интеграции с Kaspersky Endpoint Detection and Response (KATA) нужно убедиться, что служба auditd не запущена или не установлена.
- Для работы компонентов Управление сетевым экраном, Защита от веб-угроз и Защита от сетевых угроз требуется установить на вашем устройстве пакет утилит iptables.

- Для работы плагина управления Kaspersky Endpoint Security на устройстве, где установлен Сервер администрирования Kaspersky Security Center, требуется установить Microsoft® Visual C++® 2015 Redistributable Update 3 RC (см. https://www.microsoft.com/ru-ru/download/details.aspx?id=52685).

- Для запуска и корректной работы приложения требуется убедиться, что учетная запись root является владельцем следующих директорий и только владелец имеет право на запись в них: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

Дополнительные действия перед установкой Kaspersky Endpoint Security в режиме Легкого агента

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент), вам нужно выполнить дополнительно следующие действия перед началом установки приложения Kaspersky Endpoint Security:

- Убедиться в том, что на виртуальных машинах, которые вы хотите защищать, установлены следующие пакеты, в зависимости от виртуальной инфраструктуры, в которой развернуто решение Kaspersky Security для виртуальных сред Легкий агент:

  - В инфраструктуре Microsoft Hyper-V на виртуальных машинах должен быть установлен пакет служб интеграции (Integration Services).

  - В инфраструктуре VMware vSphere на виртуальных машинах должен быть установлен пакет VMware Tools.

  - В инфраструктуре XenServer на виртуальных машинах должна быть установлена программа XenTools.

  - В инфраструктуре HUAWEI FusionSphere на виртуальных машинах должен быть установлен пакет HUAWEI Tools.

  - В инфраструктуре KVM, OpenStack, Облачная платформа VK Cloud, Облачная платформа ТИОНИКС, Astra Linux и Альт Сервер Виртуализации на виртуальных машинах должен быть установлен QEMU Guest Agent.

- Убедиться в том, что в настройках сетевого оборудования или программного обеспечения, обеспечивающего контроль трафика между виртуальными машинами, разрешено прохождение сетевого трафика через порты, которые используются для взаимодействия приложения Kaspersky Endpoint Security в режиме Легкого агента с другими компонентами решения Kaspersky Security для виртуальных сред Легкий агент. Подробнее о компонентах решения см. в справке Kaspersky Security для виртуальных сред Легкий агент .

Порты, используемые в работе Легкого агента

Порт и протокол	Направление	Назначение и описание
7271 TCP	От Легкого агента к Серверу интеграции.	Для взаимодействия Легкого агента и Сервера интеграции.
8000 UDP	От SVM к Легкому агенту.	Для передачи Легким агентам информации о доступных SVM с использованием списка адресов SVM.
8000 UDP	От Легкого агента к SVM.	Для получения Легким агентом информации о состоянии SVM.
11111 TCP	От Легкого агента к SVM.	Для передачи служебных запросов (например, на получение информации о лицензии) от Легкого агента Серверу защиты при

		незащищенном соединении.
11112 TCP	От Легкого агента к SVM.	Для передачи служебных запросов (например, на получение информации о лицензии) от Легкого агента Серверу защиты при защищенном соединении.
9876 TCP	От Легкого агента к SVM.	Для передачи запросов на проверку файлов от Легкого агента Серверу защиты при незащищенном соединении.
9877 TCP	От Легкого агента к SVM.	Для передачи запросов на проверку файлов от Легкого агента Серверу защиты при защищенном соединении.
80 TCP	От Легкого агента к SVM.	Для обновления баз и программных модулей решения на Легком агенте.
15000 UDP	От Kaspersky Security Center к SVM.	Для управления Сервером защиты через Kaspersky Security Center.
15000 UDP	От Kaspersky Security Center к Легким агентам.	Для управления Легким агентом через Kaspersky Security Center.
13000 TCP	От Легкого агента к Kaspersky Security Center.	Для управления Легким агентом через Kaspersky Security Center при защищенном соединении.
14000 TCP	От Легкого агента к Kaspersky Security Center.	Для управления Легким агентом через Kaspersky Security Center при незащищенном соединении.

Установка и первоначальная настройка приложения Kaspersky Endpoint Security

Перед началом установки приложения Kaspersky Endpoint Security требуется выполнить подготовку к установке.

Сценарии ниже описывают установку и первоначальную настройку приложения Kaspersky Endpoint Security, а также установку и настройку Агента администрирования Kaspersky Security Center и установку плагинов управления Kaspersky Endpoint Security. Сценарий установки зависит от режима, в котором вы планируете использовать приложение Kaspersky Endpoint Security.

Стандартный режим

Если вы планируете использовать приложение Kaspersky Endpoint Security в стандартном режиме, процедура установки приложения состоит из следующих этапов:

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

   Если вы планируете управлять приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, установите на защищаемом устройстве Агент администрирования Kaspersky Security Center и настройте его параметры.

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

   Если вы планируете управлять приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, установите плагин управления Kaspersky Endpoint Security. В зависимости от консоли управления Kaspersky Security Center используются следующие плагины управления:

   - Веб-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console. Веб-плагин устанавливается на устройстве с установленным приложением Kaspersky Security Center Web Console.
   - Mmc-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Консоль администрирования Kaspersky Security Center. Mmc-плагин устанавливается на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

3. **Установка пакетов приложения и графического пользовательского интерфейса**

   Приложение Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM. Предусмотрены отдельные пакеты для приложения и графического пользовательского интерфейса. Установите Kaspersky Endpoint Security и, если требуется, графический пользовательский интерфейс из пакетов нужного формата.

   Вы можете выполнить установку одним из следующих способов:

   - С помощью Kaspersky Security Center.
   - С помощью командной строки.

4. **Первоначальная настройка Kaspersky Endpoint Security**

   Выполнение первоначальной настройки требуется для включения защиты клиентского устройства.

   Если вы установили приложение Kaspersky Endpoint Security с помощью Kaspersky Security Center, после завершения установки выполните подготовку приложения к работе.

   Если вы установили приложение Kaspersky Endpoint Security с помощью командной строки, после завершения установки запустите скрипт первоначальной настройки или выполните первоначальную настройку в автоматическом режиме.

Режим Легкого агента

Не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред на операционных системах для архитектуры Arm.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, процедура установки приложения состоит из следующих этапов:

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

   Установите на виртуальные машины и шаблоны виртуальных машин Агент администрирования Kaspersky Security Center и настройте его параметры.

   Если вы устанавливаете Агент администрирования на шаблон, из которого будут создаваться временные виртуальные машины, рекомендуется настроить параметры, которые позволяют оптимизировать работу на временных виртуальных машинах. Подробнее об установке на шаблон виртуальных машин см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

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

   Установите плагин управления Kaspersky Endpoint Security. В зависимости от консоли управления Kaspersky Security Center используются следующие плагины управления:

   - Веб-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console. Веб-плагин устанавливается на устройство с установленным приложением Kaspersky Security Center Web Console.
   - Mmc-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Консоль администрирования Kaspersky Security Center. Mmc-плагин устанавливается на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

3. **Установка пакетов приложения и первоначальная настройка Kaspersky Endpoint Security**

   Приложение Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM. Установите Kaspersky Endpoint Security из пакета нужного формата. Предусмотрены отдельные пакеты для приложения и графического пользовательского интерфейса.

   Графический пользовательский интерфейс не поддерживается, если Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

   Вы можете выполнить установку приложения одним из следующих способов:

   - С помощью Kaspersky Security Center.

     Перед началом установки вам нужно настроить параметры первоначальной настройки приложения одним из следующих способов:

     - В свойствах инсталляционного пакета на закладке **Параметры** (этот способ доступен только в Kaspersky Security Center Web Console).
     - С помощью конфигурационного файла, который включен в инсталляционный пакет.

     Вам нужно выбрать режим Легкого агента (в конфигурационном файле – параметр `KSVLA_MODE=yes`). Если вы устанавливаете Kaspersky Endpoint Security на шаблон, из которого будут создаваться временные виртуальные машины, рекомендуется также включить режим защиты инфраструктуры VDI для оптимизации работы приложения на временных виртуальных машинах (в конфигурационном файле – параметр `VDI_MODE=yes`).

- С помощью командной строки. В случае установки с помощью командной строки выбор режима использования приложения выполняется во время первоначальной настройки.

4. **Первоначальная настройка Kaspersky Endpoint Security**

   Выполнение первоначальной настройки требуется для включения защиты клиентского устройства.

   Если вы установили приложение Kaspersky Endpoint Security с помощью Kaspersky Security Center, после завершения установки выполните подготовку приложения к работе.

   Если вы установили приложение Kaspersky Endpoint Security с помощью командной строки, после завершения установки запустите скрипт первоначальной настройки или выполните первоначальную настройку в автоматическом режиме. Во время первоначальной настройки вам нужно выбрать режим Легкого агента одним из следующих способов:

   - Ввести `yes` на шаге `Specifying the application usage` скрипта первоначальной настройки.
   - Задать в конфигурационном файле первоначальной настройки параметр `KSVLA_MODE=yes`.

   Если вы устанавливаете приложение Kaspersky Endpoint Security на шаблон, из которого будут создаваться временные виртуальные машины, рекомендуется также настроить параметр, который позволяет оптимизировать работу на временных виртуальных машинах. Подробнее об установке на шаблон виртуальных машин см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Установка и первоначальная настройка Агента администрирования Kaspersky Security Center

Установка Агента администрирования требуется для управления приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center.

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

Вы можете выполнить установку и первоначальную настройку Агента администрирования:

- удаленно с рабочего места администратора с помощью Kaspersky Security Center Web Console или Консоли администрирования;
- с помощью командной строки.

Об установке Агента администрирования с помощью Kaspersky Security Center

Перед началом удаленной установки Агента администрирования с помощью Kaspersky Security Center требуется подготовить устройство к удаленной установке (см. в справке Kaspersky Security Center, раздел "Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux").

Для удаленной установки используется инсталляционный пакет Агента администрирования. Файлы, необходимые для создания инсталляционного пакета Агента администрирования, вы можете скачать на веб-сайте "Лаборатории Касперского" в разделе **Kaspersky Security Center**.

Чтобы удаленно установить Агент администрирования:

1. Создайте инсталляционный пакет Агента администрирования.

   Во время создания инсталляционного пакета вам нужно принять условия Лицензионного соглашения для Агента администрирования. Вы можете ознакомиться с текстом Лицензионного соглашения, прочитав документ license.txt из комплекта поставки Агента администрирования.

   В параметрах инсталляционного пакета укажите адрес Сервера администрирования, к которому должен подключаться Агент администрирования, и порт для подключения.

2. Выполните установку Агента администрирования с помощью задачи удаленной установки приложений.

Подробнее об установке Агента администрирования, см. в справке Kaspersky Security Center.

Об установке Агента администрирования с помощью командной строки

Вы можете установить Агент администрирования с помощью командной строки одним из следующих способов:

- Выполнить установку и первоначальную настройку в тихом режиме с файлом ответов. Файл ответов – это текстовый файл, который содержит пользовательский набор параметров установки и первоначальной настройки Агента администрирования.
- Выполнить установку Агента администрирования из пакета формата RPM или DEB в соответствии с типом менеджера пакетов, затем выполнить первоначальную настройку Агента администрирования с помощью скрипта в интерактивном режиме. Скрипт запускается по команде:
  - 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
    ```

Установку Агента администрирования требуется запускать с root-правами.

Чтобы выполнить установку Агента администрирования в тихом режиме:

1. Создайте файл ответов. Добавьте в файл ответов список параметров установки и первоначальной настройки Агента администрирования в формате `< параметр >=< значение >`, каждый параметр в отдельной строке.

   Для правильного использования файла ответов вам нужно включить в него следующие обязательные параметры:

   - KLNAGENT_SERVER – полное доменное имя (FQDN) или IP-адрес Сервера администрирования.
   - KLNAGENT_AUTOINSTALL – параметр определяет, включен ли тихий режим установки. Укажите значение `1`.
   - EULA_ACCEPTED – согласие с условиями Лицензионного соглашения для Агента администрирования. Вам нужно принять условия Лицензионного соглашения, чтобы продолжить процедуру установки. Ознакомьтесь с текстом Лицензионного соглашения, прочитав документ license.txt из комплекта поставки Агента администрирования. Если вы понимаете и принимаете условия Лицензионного соглашения, укажите значение `1`.

Вы также можете добавить другие параметры установки и первоначальной настройки Агента администрирования. Полный список возможных параметров см. в справке Kaspersky Security Center (раздел "Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)").

2. Задайте значение переменной среды KLAUTOANSWERS, введя полное имя файла ответов (включая путь), например, следующим образом:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

3. Установите Агент администрирования:

   - 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 RPM на 64-битную операционную систему для архитектуры Arm, выполните следующую команду:

     ```
     # rpm -i klnagent64-<номер сборки>.aarch64.rpm
     ```

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

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

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

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

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

     ```
     # apt-get install ./klnagent64_<номер сборки>_arm64.deb
     ```

Установка плагинов управления Kaspersky Endpoint Security

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

- веб-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console;

- mmc-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Консоль администрирования Kaspersky Security Center.

Вы можете одновременно установить плагины управления для разных версий приложения Kaspersky Endpoint Security. Таким образом вы сможете управлять приложением, используя политики, созданные с помощью разных версий плагина управления.

Вы можете также конвертировать политики и задачи, созданные с помощью предыдущих версий плагина управления, в новые версии.

Установка веб-плагина Kaspersky Endpoint Security

Веб-плагин управления Kaspersky Endpoint Security требуется установить на клиентское устройство с установленным приложением Kaspersky Security Center Web Console. При этом функции веб-плагина доступны всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console в браузере.

Вы можете установить веб-плагин следующими способами:

- С помощью мастера первоначальной настройки Kaspersky Security Center Web Console.

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

- Вручную, используя дистрибутив из списка веб-плагинов "Лаборатории Касперского" или из стороннего источника.

Чтобы установить веб-плагин Kaspersky Endpoint Security вручную:

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры → Веб-плагины**.

   Откроется список установленных веб-плагинов.

2. Запустите установку веб-плагина Kaspersky Endpoint Security одним из следующих способов:

   - Установка из списка веб-плагинов "Лаборатории Касперского":

     a. Нажмите на кнопку **Добавить**.

     Откроется список всех доступных веб-плагинов "Лаборатории Касперского". Список обновляется автоматически после выпуска новых версий веб-плагинов.

     b. Найдите в списке веб-плагин **Kaspersky Endpoint Security <номер версии> для Linux** и нажмите на его название.

     c. В открывшемся окне с описанием веб-плагина нажмите на кнопку **Установить плагин**.

     d. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

   - Установка веб-плагина из стороннего источника (архивы, необходимые для установки веб-плагинов, входят в комплект поставки):

     a. Нажмите на кнопку **Добавить из файла**.

     b. В открывшемся окне укажите путь к ZIP-архиву с дистрибутивом веб-плагина и путь к файлу с подписью в формате TXT. Этот файл находится в архиве с веб-плагином.

     c. Нажмите на кнопку **Добавить**.

     d. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отображается в списке установленных веб-плагинов (**Параметры** → **Веб-плагины**).

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

Установка mmc-плагина Kaspersky Endpoint Security

Mmc-плагин управления Kaspersky Endpoint Security требуется установить на том же клиентском устройстве, на котором установлена Консоль администрирования Kaspersky Security Center.

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

Чтобы установить mmc-плагин,

на устройстве, где установлена Консоль администрирования Kaspersky Security Center, запустите исполняемый файл klcfginst.msi.

Файл входит в комплект поставки приложения Kaspersky Endpoint Security.

После установки mmc-плагин управления отображается в списке установленных mmc-плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

Чтобы посмотреть список установленных mmc-плагинов управления:

1. В дереве Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования <имя сервера>** и откройте окно свойств Сервера администрирования одним из следующих способов:

   - с помощью пункта **Свойства** контекстного меню узла **Сервер администрирования <имя сервера>**;
   - по ссылке **Свойства сервера администрирования**, расположенной в рабочей области узла **Сервер администрирования <имя сервера>** в блоке **Сервер администрирования**.

2. В списке слева в разделе **Дополнительно** выберите раздел **Информация об установленных плагинах управления программами**.

   В правой части окна в списке установленных плагинов управления отображается mmc-плагин управления Kaspersky Endpoint Security: **Kaspersky Endpoint Security <номер версии> для Linux**.

Установка и первоначальная настройка приложения с помощью Kaspersky Security Center

Вы можете установить приложение Kaspersky Endpoint Security на клиентское устройство удаленно с рабочего места администратора с помощью Kaspersky Security Center Web Console или с помощью Консоли администрирования.

Для удаленной установки используется инсталляционный пакет приложения Kaspersky Endpoint Security. Инсталляционный пакет Kaspersky Endpoint Security является общим для всех поддерживаемых операционных систем и типов архитектуры процессора. Вы можете создать инсталляционный пакет с помощью Kaspersky Security Center Web Console или с помощью Консоли администрирования.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент), вам нужно настроить параметры первоначальной настройки приложения в свойствах инсталляционного пакета (этот способ доступен только в Web Console) или в конфигурационном файле autoinstall.ini, который включен в инсталляционный пакет.

Вы можете развернуть приложение Kaspersky Endpoint Security на устройствах в сети организации несколькими способами.

Kaspersky Security Center Web Console поддерживает следующие основные способы развертывания:

- Установка приложения с помощью мастера развертывания защиты.
- Установка приложения с помощью задачи удаленной установки приложений.

Консоль администрирования Kaspersky Security Center поддерживает следующие основные способы развертывания:

- Установка приложения с помощью мастера удаленной установки.
- Установка приложения с помощью задачи удаленной установки приложений.

Описание процедур развертывания см. в справке Kaspersky Security Center.

При необходимости вы можете просмотреть журнал удаленной установки приложения с помощью удаленной диагностики клиентского устройства Kaspersky Security Center.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается активация приложения во время установки и автоматическое распространение лицензионных ключей. Kaspersky Endpoint Security получает информацию о лицензии от Сервера защиты после подключения к SVM, отдельно активировать Kaspersky Endpoint Security не требуется.

После завершения установки приложения с помощью Kaspersky Security Center требуется выполнить подготовку приложения к работе.

Чтобы управлять с помощью Kaspersky Security Center работой приложения Kaspersky Endpoint Security, установленного на клиентских устройствах, вам нужно поместить эти устройства в группы администрирования. Перед началом установки приложения Kaspersky Endpoint Security вы можете создать в Kaspersky Security Center группы администрирования, в которые вы хотите поместить устройства с установленным приложением, и настроить правила автоматического перемещения устройств в группы администрирования. Если правила перемещения устройств в группы администрирования не настроены, Kaspersky Security Center помещает все устройства с установленным Агентом администрирования, подключенным к Серверу администрирования, в список **Нераспределенные устройства**. В этом случае вам нужно вручную переместить устройства в группы администрирования (см. подробнее в справке Kaspersky Security Center).

Создание инсталляционного пакета в Web Console

В Kaspersky Security Center Web Console вы можете создать инсталляционный пакет одним из следующих способов:

- Из архивного файла, который вы подготовили предварительно.
- Из дистрибутива, размещенного на серверах "Лаборатории Касперского".

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, вам нужно настроить параметры первоначальной настройки приложения в свойствах созданного инсталляционного пакета на закладке **Параметры**. Вы также можете настраивать параметры первоначальной настройки приложения с помощью конфигурационного файла, который включен в инсталляционный пакет.

Чтобы подготовить архивный файл для создания инсталляционного пакета:

1. Скачайте архив kesl.zip на странице загрузки приложений в разделе **Kaspersky Endpoint Security для Linux** (**Дополнительный дистрибутив** → **Files for Product remote installation**).
2. Распакуйте архив kesl.zip в папку, доступную для Сервера администрирования Kaspersky Security Center. В ту же папку поместите файлы дистрибутива, соответствующие типу операционной системы, на которую вы хотите установить приложение, и типу менеджера пакетов на ней:
   - для установки Kaspersky Endpoint Security:
     - kesl-12.1.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
     - kesl_12.1.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
     - kesl-12.1.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
     - kesl_12.1.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
     - kesl-12.1.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
     - kesl_12.1.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)
   - для установки графического интерфейса:
     - kesl-gui-12.1.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
     - kesl-gui_12.1.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
     - kesl-gui-12.1.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
     - kesl-gui_12.1.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
     - kesl-gui-12.1.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)

- kesl-gui_12.1.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)

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

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, графический пользовательский интерфейс не поддерживается.

Обратите внимание, что если графический пользовательский интерфейс не будет использоваться, то вам нужно установить значение параметра `USE_GUI=No` в свойствах созданного инсталляционного пакета или в конфигурационном файле autoinstall.ini. В противном случае установка завершается с ошибкой.

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

3. Если вы хотите настроить параметры первоначальной настройки приложения с помощью конфигурационного файла, откройте конфигурационный файл autoinstall.ini и внесите необходимые изменения. Файл autoinstall.ini находится в папке, в которую вы распаковали архив kesl.zip.

   Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, в конфигурационном файле autoinstall.ini вам нужно установить значение параметра `KSVLA_MODE=yes`.

   Вы также можете настроить параметры первоначальной настройки приложения в свойствах созданного инсталляционного пакета на закладке **Параметры**.

4. Если вы планируете использовать приложение Kaspersky Endpoint Security в стандартном режиме и хотите использовать предварительно скачанные базы, поместите в папку подготовленные архивы с базами для всех необходимых типов операционных систем, откройте конфигурационный файл autoinstall.ini и установите значение параметра `UPDATE_EXECUTE=no`. Файл autoinstall.ini находится в папке, в которую вы распаковали архив kesl.zip.

5. Поместите все подготовленные файлы в архив формата ZIP, CAB, TAR или TAR.GZ с произвольным именем.

Чтобы создать инсталляционный пакет Kaspersky Endpoint Security в Kaspersky Security Center Web Console:

1. В главном окне Web Console выберите один из следующих разделов:

   - **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.
   - **Операции → Хранилища → Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

3. На первой странице мастера выберите способ создания инсталляционного пакета:

   - **Создать инсталляционный пакет из файла**. Инсталляционный пакет будет создан из архивного файла, который вы подготовили предварительно. Вам нужно выбрать этот вариант, если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

   - **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**. Инсталляционный пакет будет создан из дистрибутива, размещенного на серверах "Лаборатории Касперского".

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

4. В зависимости от выбранного способа создания пакета:

   - Укажите имя пакета, нажмите на кнопку **Обзор** и укажите путь к архиву, который вы подготовили для создания инсталляционного пакета.

   - Выберите дистрибутив приложения Kaspersky Endpoint Security. В окне справа ознакомьтесь с информацией о дистрибутиве и нажмите на кнопку **Загрузить и создать инсталляционный пакет**. Запустится процесс создания инсталляционного пакета.

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

Инсталляционный пакет будет создан и добавлен в список инсталляционных пакетов. С помощью инсталляционного пакета вы можете установить приложение на устройства сети организации или обновить версию приложения.

В свойствах инсталляционного пакета на закладке **Параметры** вы можете настроить параметры первоначальной настройки приложения (см. таблицу ниже).

Настройка инсталляционного пакета Kaspersky Endpoint Security в версии Kaspersky Security Center Web Console ниже 14.2 не поддерживается. Для настройки параметров используйте конфигурационный файл autoinstall.ini.

Параметры инсталляционного пакета

Раздел	Описание
Указать языковой стандарт	Установите флажок, чтобы указать языковой стандарт, используемый при работе приложения. Языковой стандарт в формате, определенном в RFC 3066. Если этот параметр не указан, используется языковой стандарт по умолчанию.
Активировать приложение	Установите флажок, чтобы активировать приложение. Вы также можете активировать приложение после установки. Параметр применяется, только если приложение используется в стандартном режиме.

Выберите источник обновлений	Укажите источник обновлений: • **Серверы обновлений "Лаборатории Касперского"**. • **Kaspersky Security Center**. • **Другие источники в локальной или глобальной сети**. Параметр применяется, только если приложение используется в стандартном режиме.
Запустить задачу обновления баз после установки	Установите флажок, чтобы запустить задачу обновления после установки приложения. Параметр применяется, только если приложение используется в стандартном режиме.
Указать параметры прокси-сервера	Установите флажок, чтобы указать адрес прокси-сервера, используемого для подключения к интернету. Параметр применяется, только если приложение используется в стандартном режиме.
Установить исходный код ядра	Установите флажок, чтобы автоматически начать компиляцию модулей ядра.
Использовать графический пользовательский интерфейс	Установите флажок, чтобы включить использование графического пользовательского интерфейса. Параметр применяется, только если приложение используется в стандартном режиме.
Указать пользователя с ролью Администратор (admin)	Установите флажок, чтобы указать пользователя, которому назначается роль администратора (admin).
Выполнить автоматическую настройку SELinux	Установите флажок, чтобы выполнить автоматическую настройку SELinux для работы с Kaspersky Endpoint Security.
Удалить пользователей из привилегированных групп	Установите флажок, чтобы перед установкой приложения удалить пользователей из привилегированных групп kesladmin и keslaudit. Если флажок установлен и группа nogroup отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную.
Выключить компоненты защиты и задачи проверки при первом запуске приложения после установки	Установите флажок, чтобы после установки приложение запустилось с выключенными компонентами защиты и задачами проверки.

	Установка с выключенными компонентами защиты может быть удобна, например, для воспроизведения проблемы в работе приложения с целью создания файла трассировки. Если вы включите нужные компоненты и задачи, то после перезапуска приложения включенные компоненты и задачи продолжат работу.
Использовать приложение в режиме Легкого агента	Установите флажок, если вы хотите использовать приложение в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент). Если флажок снят, приложение используется в стандартном режиме.
Включить режим защиты инфраструктуры VDI	Установите флажок, чтобы включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки приложения на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. Параметр применяется, только если приложение используется в режиме Легкого агента.
Защищаемая виртуальная машина используется как сервер	Установите флажок, если виртуальная машина, на которую будет установлено приложение, используется в виртуальной инфраструктуре как сервер. Параметр применяется, только если приложение используется в режиме Легкого агента.

Создание инсталляционного пакета в Консоли администрирования

Перед тем, как создать инсталляционный пакет приложения Kaspersky Endpoint Security, вам нужно подготовить файлы, которые будут включены в пакет.

Чтобы подготовить файлы для создания инсталляционного пакета:

1. Скачайте архив kesl.zip на странице загрузки приложений в разделе **Kaspersky Endpoint Security для Linux** (**Дополнительный дистрибутив** → **Files for Product remote installation**).

2. Распакуйте архив kesl.zip в папку, доступную для Сервера администрирования Kaspersky Security Center. В ту же папку поместите файлы дистрибутива, соответствующие типу операционной системы, на которую вы хотите установить приложение, и типу менеджера пакетов на ней:

   - для установки Kaspersky Endpoint Security:

     - kesl-12.1.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
     - kesl_12.1.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
     - kesl-12.1.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
     - kesl_12.1.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)

- kesl-12.1.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
- kesl_12.1.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)

- для установки графического интерфейса:
  - kesl-gui-12.1.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
  - kesl-gui_12.1.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
  - kesl-gui-12.1.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
  - kesl-gui_12.1.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
  - kesl-gui-12.1.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
  - kesl-gui_12.1.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)

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

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, графический пользовательский интерфейс не поддерживается.

Обратите внимание, что если графический пользовательский интерфейс не будет использоваться, то вам нужно установить значение параметра `USE_GUI=No` в свойствах созданного инсталляционного пакета или в конфигурационном файле autoinstall.ini. В противном случае установка завершается с ошибкой.

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

3. Если вы хотите настроить параметры первоначальной настройки приложения с помощью конфигурационного файла, откройте конфигурационный файл autoinstall.ini и внесите необходимые изменения. Файл autoinstall.ini находится в папке, в которую вы распаковали архив kesl.zip.

   Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, в конфигурационном файле autoinstall.ini вам нужно установить значение параметра `KSVLA_MODE=yes`.

4. Если вы планируете использовать приложение Kaspersky Endpoint Security в стандартном режиме и хотите использовать предварительно скачанные базы, поместите в папку подготовленные архивы с базами для всех необходимых типов операционных систем, откройте конфигурационный файл autoinstall.ini и установите значение параметра `UPDATE_EXECUTE=no`. Файл autoinstall.ini находится в папке, в которую вы распаковали архив kesl.zip.

Чтобы создать инсталляционный пакет Kaspersky Endpoint Security в Консоли администрирования Kaspersky Security Center:

1. В дереве консоли выберите **Дополнительно → Удаленная установка → Инсталляционные пакеты**.
2. Нажмите на кнопку **Создать инсталляционный пакет**.

   Запустится мастер создания инсталляционного пакета.
3. В открывшемся окне мастера нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
4. Введите имя нового инсталляционного пакета и перейдите к следующему шагу.
5. Выберите дистрибутив приложения Kaspersky Endpoint Security. Для этого откройте стандартное окно Windows с помощью кнопки **Обзор** и укажите путь к файлу kesl.kud. Файл находится в папке, в которую вы распаковали архив kesl.zip.

   В окне отобразится название приложения.

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

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

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

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

Подготовка архива с базами приложения для создания инсталляционного пакета с интегрированными базами

В некоторых случаях может потребоваться создать пакет удаленной установки с предварительно скачанными базами приложения. Например, если вы устанавливаете приложение на устройство с операционной системой Astra Linux Special Edition или хотите установить приложение сразу с готовыми рабочими базами (чтобы дополнительно не обновлять базы позднее).

Чтобы создать инсталляционный пакет с интегрированными базами для установки приложения:

1. Выполните установку и первоначальную настройку приложения Kaspersky Endpoint Security на устройстве с помощью командной строки или с помощью Kaspersky Security Center.
2. Выполните обновление баз приложения. Вы можете обновить базы в ходе первоначальной настройки приложения или после установки, запустив задачу типа Update в командной строке или задачу *Обновление* в Консоли администрирования Kaspersky Security Center или в Kaspersky Security Center Web Console.

3. Скопируйте содержимое директории /var/opt/kaspersky/kesl/private/updates/ в одну из следующих поддиректорий в зависимости от архитектуры операционной системы, для которой вы создаете инсталляционный пакет с интегрированными базами: /i386/, /x86_64/ или /arm64/.

4. Поместите директории с базами в архив kesl-bases.tgz, сохраняя структуру вложенных директорий. Вы можете поместить в архив только одну поддиректорию с базами для нужной архитектуры операционной системы или все поддиректории с базами (/i386/, /x86_64/ или /arm64/) в один архив под разные архитектуры, если вы планируете создать инсталляционный пакет для установки на несколько операционных систем с разной архитектурой.

5. Созданный архив с базами приложения вы можете использовать при создании инсталляционного пакета в Консоли администрирования Kaspersky Security Center или в Kaspersky Security Center Web Console.

Параметры конфигурационного файла autoinstall.ini

В конфигурационном файле autoinstall.ini вы можете задавать параметры, приведенные в таблице ниже. Набор применимых параметров зависит от режима использования приложения.

Параметры конфигурационного файла autoinstall.ini

Параметр	Описание	Значения
KSVLA_MODE	Режим использования Kaspersky Endpoint Security.	yes – Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент). no (значение по умолчанию) – Kaspersky Endpoint Security используется в стандартном режиме.
SERVER_MODE	Роль защищаемой виртуальной машины (сервер или рабочая станция). Параметр применяется, только если приложение используется в режиме Легкого агента.	yes (значение по умолчанию) – защищаемая виртуальная машина используется как сервер. no – защищаемая виртуальная машина используется как рабочая станция.
VDI_MODE	Включение режима защиты инфраструктуры VDI для оптимизации работы приложения на временных виртуальных машинах. Параметр применяется, только если приложение используется в режиме Легкого агента.	yes – включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки Kaspersky Endpoint Security на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. no (значение по умолчанию) – не включать режим защиты инфраструктуры VDI.

EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения.	yes (значение по умолчанию) – принять условия Лицензионного соглашения, чтобы продолжить процедуру установки приложения. no – не принимать условия Лицензионного соглашения. Установка приложения будет прервана.
PRIVACY_POLICY_AGREED	Обязательный параметр. Согласие с условиями Политики конфиденциальности.	yes (значение по умолчанию) – принять условия Политики конфиденциальности, чтобы продолжить процедуру установки приложения. no – не принимать условия Политики конфиденциальности. Установка приложения будет прервана.
USE_KSN	Обязательный параметр. Включение использования Kaspersky Security Network. Для включения использования KSN требуется принять условия Положения о Kaspersky Security Network.	yes – принять условия Положения о Kaspersky Security Network и включить использование KSN. no (значение по умолчанию) – не принимать условия Положения о Kaspersky Security Network. Если приложение Kaspersky Endpoint Security используется в стандартном режиме и вы включили использование KSN, автоматически включается облачный режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО.
GROUP_CLEAN	Обязательный параметр. Удаление пользователей из привилегированных групп kesladmin и keslaudit.	yes – удалять пользователей из привилегированных групп. Если указано значение yes и группа nogroup отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную. no – не удалять пользователей из привилегированных групп.
LOCALE	Дополнительный параметр. Языковой стандарт, используемый для локализации событий приложения, отправляемых в Kaspersky Security Center.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр LOCALE не указан, устанавливается язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию en_US.utf8.

		Локализация графического интерфейса и командной строки приложения зависит от локализации, указанной в переменной окружения `LANG`. Если в переменной окружения `LANG` указана локализация, которую приложение Kaspersky Endpoint Security не поддерживает, то графический интерфейс и командная строка отображаются в английской локализации.
INSTALL_LICENSE	Код активации или файл ключа. Параметр применяется, только если приложение используется в стандартном режиме.	
UPDATER_SOURCE	Источник обновлений. Параметр применяется, только если приложение используется в стандартном режиме.	`SCServer` – использовать в качестве источника обновлений Сервер администрирования Kaspersky Security Center. `KLServers` – использовать в качестве источника обновлений серверы "Лаборатории Касперского". Это значение используется по умолчанию. Адрес источника обновлений.
PROXY_SERVER	Адрес прокси-сервера, используемого для подключения к интернету. Параметр применяется, только если приложение используется в стандартном режиме.	Адрес прокси-сервера.
UPDATE_EXECUTE	Запуск задачи обновления баз приложения во время процедуры настройки. Параметр применяется, только если приложение используется в стандартном режиме.	`yes` (значение по умолчанию) – запускать задачу обновления. `no` – не запускать задачу обновления.
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра.	`yes` (значение по умолчанию) – компилировать модуль ядра.

		no – не компилировать модуль ядра.
USE_GUI	Использование графического пользовательского интерфейса. Параметр применяется, только если приложение используется в стандартном режиме.	yes – включить использование графического пользовательского интерфейса. no (значение по умолчанию) – выключить использование графического пользовательского интерфейса.
ADMIN_USER	Пользователь, которому назначается роль администратора (admin).	Нет
CONFIGURE_SELINUX	Автоматическая настройка SELinux для работы с приложением Kaspersky Endpoint Security.	yes (значение по умолчанию) – выполнить автоматическую настройку SELinux для работы с Kaspersky Endpoint Security. no – не выполнять автоматическую настройку SELinux для работы с Kaspersky Endpoint Security.
DISABLE_PROTECTION	Выключение функциональных компонентов приложения после его установки. Установка с выключенными компонентами может быть удобна, например, для воспроизведения проблемы в работе приложения с целью создания файла трассировки. Если после установки приложения с параметром `DISABLE_PROTECTION=yes` вы включите нужные компоненты, то после перезапуска приложения включенные компоненты продолжат работу.	yes – выключить компоненты защиты и задачи проверки при запуске приложения после установки. no – не выключать компоненты защиты и задачи проверки при запуске приложения после установки.
DISABLE_FILEAV_ACTIONS	Выключение функций лечения и удаления файлов для компонентов приложения после его установки.	yes – выключить функции лечения и удаления файлов при запуске приложения после установки. no (значение по умолчанию) – не выключать функции лечения и удаления файлов при запуске приложения после установки.

	Если функции лечения и удаления файлов выключены, в случае обнаружения угрозы приложение не пытается лечить или удалять файлы, в которых обнаружена угроза, а только информирует пользователя об обнаружении угрозы в файлах. После установки приложения вы можете включить функции лечения и удаления файлов с помощью параметра `DisableFileAvActions` в конфигурационном файле kesl.ini.	

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

Подготовка приложения к работе с помощью Kaspersky Security Center

После развертывания приложения Kaspersky Endpoint Security через Kaspersky Security Center требуется подготовить приложение к работе. Действия, которые необходимо выполнить, зависят от режима, в котором вы планируете использовать приложение Kaspersky Endpoint Security.

Стандартный режим

Если вы планируете использовать приложение Kaspersky Endpoint Security в стандартном режиме, после развертывания приложения вам нужно выполнить следующие действия:

- Активировать приложение. Вы можете создать и выполнить задачу активации через Консоль администрирования или через Kaspersky Security Center Web Console, а также распространить на устройства лицензионный ключ из хранилища ключей Kaspersky Security Center.
- Обновить базы и модули приложения через Консоль администрирования или через Kaspersky Security Center Web Console. Вы можете использовать задачу *Обновление*, которая создана автоматически мастером первоначальной настройки Kaspersky Security Center после установки mmc-плагина управления или веб-плагина управления Kaspersky Endpoint Security.

  Kaspersky Endpoint Security обеспечивает защиту устройства только после обновления баз приложения.

- Настроить политику для централизованного управления работой приложения с помощью Консоли администрирования Kaspersky Security Center или Web Console. Вы можете использовать политику,

которая создана автоматически мастером первоначальной настройки Kaspersky Security Center после установки mmc-плагина управления или веб-плагина управления Kaspersky Endpoint Security.

Также вы можете настроить задачи управления приложением с помощью Консоли администрирования или Web Console.

Режим Легкого агента

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, после развертывания приложения вам нужно выполнить следующие действия:

1. Настроить параметры обнаружения SVM Легкими агентами. Для этого вам нужно создать и настроить политику для централизованного управления работой приложения на клиентских устройствах. Для работы с политиками вы можете использовать Консоль администрирования или Web Console.

   В свойствах политики вам нужно настроить следующие параметры:

   - Параметры подключения Легких агентов к Серверу интеграции.
   - Параметры подключения Легких агентов к SVM.

2. Убедиться в том, что установлено подключение Легких агентов к SVM и к Серверу интеграции.

   Вы можете получить информацию о подключении с помощью команд Kaspersky Endpoint Security на защищенной виртуальной машине:

   - Информацию о подключении к SVM вы можете посмотреть с помощью команды `kesl-control [-V] --svm-info`.
   - Информацию о подключении к Серверу интеграции вы можете посмотреть с помощью команды `kesl-control [-V] --viis-info`.

3. Убедиться в том, что приложение Kaspersky Endpoint Security, используемое в качестве Легкого агента, получает информацию о лицензии, по которой активировано решение Kaspersky Security для виртуальных сред Легкий агент.

   После активации решения на SVM и подключения Легких агентов к SVM компонент Сервер защиты передает информацию о лицензии Легким агентам. Информацию о лицензии, которую использует приложение Kaspersky Endpoint Security в составе решения, вы можете посмотреть на защищенной виртуальной машине с помощью команды `kesl-control -L --query`.

4. Убедиться в том, что на защищенных виртуальных машинах установлены обновления баз, необходимых для работы Легкого агента.

   Обновление баз на защищенных виртуальных машинах выполняется с помощью специальной задачи *Обновление*, в которой в качестве источника обновлений указана папка на SVM. Задача обновления запускается автоматически.

   Вы можете проверить актуальность баз на защищенной виртуальной машине с Легким агентом с помощью команды `kesl-control --app-info`.

   Также вы можете настроить задачи управления приложением с помощью Консоли администрирования или Web Console.

Активация приложения с помощью Kaspersky Security Center

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии приложения в течение срока действия лицензии.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, активировать приложение после установки не требуется. Вы активируете решение Kaspersky Security для виртуальных сред Легкий агент, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент). См. подробнее в справке Kaspersky Security для виртуальных сред Легкий агент.

Процедура активации приложения Kaspersky Endpoint Security заключается в добавлении лицензионного ключа приложения.

Вы можете добавлять лицензионные ключи в приложение через Kaspersky Security Center следующими способами:

- Путем добавления ключа в инсталляционный пакет Kaspersky Endpoint Security.

  Этот способ позволяет добавить ключ приложения в свойствах инсталляционного пакета при развертывании Kaspersky Endpoint Security. Приложение будет активировано автоматически после установки.

- С помощью задачи добавления ключа в приложение.

  Этот способ позволяет добавить лицензионный ключ на конкретное устройство или устройства, входящие в группу администрирования. Вы можете создать и выполнить задачу добавления ключа через Kaspersky Security Center Web Console или через Консоль администрирования.

- Путем распространения на клиентские устройства лицензионного ключа, размещенного на Сервере администрирования Kaspersky Security Center.

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

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

Если вы используете приложение по лицензии, которая не включает функциональность Kaspersky Endpoint Detection and Response Optimum, после активации приложения вам нужно добавить ключ EDR Optimum.

Активация в Kaspersky Security Center Web Console

Перед созданием задачи добавления ключа в приложение или распространением ключа требуется добавить ключ в хранилище Сервера администрирования Kaspersky Security Center.

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

1. В главном окне Web Console выберите **Операции** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне выберите способ добавления ключа в хранилище:
   - **Ввести код активации**, если вы хотите добавить ключ с помощью кода активации.

- **Добавить файл ключа**, если вы хотите добавить ключ с помощью файла ключа.

4. В зависимости от выбранного вами на предыдущем шаге способа добавления ключа, выполните одно из следующих действий:

   - Введите код активации и нажмите на кнопку **Отправить**.
   - Нажмите на кнопку **Выберите файл ключа** и в открывшемся окне выберите файл с расширением key.

5. Нажмите на кнопку **Закрыть**.

Добавленный ключ отобразится в списке ключей.

Чтобы добавить ключ в приложение через Web Console с помощью задачи Добавление ключа:

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите название приложения Kaspersky Endpoint Security.

   b. В раскрывающемся списке **Тип задачи** выберите **Добавление ключа**.

   c. В поле **Название задачи** введите короткое описание, например, `Активация Kaspersky Endpoint Security`.

   d. В разделе **Устройства, которым будет назначена задача** выберите область действия задачи. Нажмите на кнопку **Далее**.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

   Откроется окно **Хранилище ключей Kaspersky Security Center**.

5. Если вы добавили ключ в хранилище ключей Kaspersky Security Center предварительно, выберите ключ в списке и нажмите на кнопку **Далее**.

6. Если нужный ключ в хранилище ключей отсутствует, нажмите на кнопку **Добавить ключ**.

   a. В открывшемся окне выберите способ добавления ключа в хранилище:

      - **Ввести код активации**, если вы хотите добавить ключ с помощью кода активации.
      - **Добавить файл ключа**, если вы хотите добавить ключ с помощью файла ключа.

   b. В зависимости от выбранного вами на предыдущем шаге способа добавления ключа, выполните одно из следующих действий:

      - Введите код активации и нажмите на кнопку **Отправить**.
      - Нажмите на кнопку **Выберите файл ключа** и в открывшемся окне выберите файл с расширением key.

c. Ознакомьтесь с информацией о ключе и нажмите на кнопку **Закрыть**.

d. Добавленный ключ отобразится в списке ключей. Выберите его в списке и нажмите на кнопку **Далее**.

7. Ознакомьтесь с информацией о лицензии и нажмите на кнопку **Далее**.

8. Завершите работу мастера.

   В списке задач отобразится новая задача.

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

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

Если вы добавляете резервный ключ, но активный ключ еще не добавлен в приложение, задача завершается с ошибкой.

Чтобы добавить ключ в приложение через Web Console путем распространения на устройства ключа, размещенного на Сервере администрирования:

1. В главном окне Web Console выберите **Операции** → **Лицензии "Лаборатории Касперского"**.

2. Откройте свойства ключа по ссылке с названием приложения, для активации которого предназначен ключ.

3. На закладке **Общие** установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.

4. Нажмите на кнопку **Сохранить**.

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

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

- Просмотреть Отчет об использовании лицензионных ключей (**Мониторинг и отчеты** → **Отчеты**).
- Просмотреть статусы управляемых устройств (**Активы (Устройства)** → **Управляемые устройства**). Если приложение не активировано, то для устройства будет отображаться статус и описание статуса **Защита выключена**.
- Просмотреть свойства ключа (**Операции** → **Лицензии "Лаборатории Касперского"**).

Особенности активации в Kaspersky Security Center Cloud Console

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

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

Установка и первоначальная настройка приложения с помощью командной строки

Вы можете выполнить следующие действия при установке приложения с помощью командной строки:

- Установить приложение с графическим пользовательским интерфейсом.

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент), графический пользовательский интерфейс не поддерживается. Вам нужно установить пакет приложения без графического пользовательского интерфейса.

- Установить приложение без графического пользовательского интерфейса.
- Установить графический пользовательский интерфейс на устройстве, где установлено приложение.

  Невозможно установить графический пользовательский интерфейс на устройство, на котором не установлено приложение.

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

После завершения установки приложения требуется выполнить первоначальную настройку приложения в интерактивном режиме или в автоматическом режиме.

Установка приложения с помощью командной строки

Установка приложения без графического пользовательского интерфейса

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

```
# rpm -i kesl-12.1.0-<номер сборки>.i386.rpm
```

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

```
# rpm -i kesl-12.1.0-<номер сборки>.x86_64.rpm
```

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

```
# rpm -i kesl-12.1.0-<номер сборки>.aarch64.rpm
```

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

```
# apt-get install ./kesl_12.1.0-<номер сборки>_i386.deb
```

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

```
# apt-get install ./kesl_12.1.0-<номер сборки>_amd64.deb
```

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

```
# apt-get install ./kesl_12.1.0-<номер сборки>_arm64.deb
```

Установка графического пользовательского интерфейса

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

```
# rpm -i kesl-gui-12.1.0-<номер сборки>.i386.rpm
```

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

```
# rpm -i kesl-gui-12.1.0-<номер сборки>.x86_64.rpm
```

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

```
# rpm -i kesl-gui-12.1.0-<номер сборки>.aarch64.rpm
```

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

```
# apt-get install ./kesl-gui_12.1.0-<номер сборки>_i386.deb
```

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

```
# apt-get install ./kesl-gui_12.1.0-<номер сборки>_amd64.deb
```

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

```
# apt-get install ./kesl-gui_12.1.0-<номер сборки>_arm64.deb
```

Первоначальная настройка приложения в интерактивном режиме

После установки приложения Kaspersky Endpoint Security с помощью командной строки требуется выполнить первоначальную настройку приложения, запустив скрипт первоначальной настройки. Скрипт первоначальной настройки входит в комплект поставки Kaspersky Endpoint Security.

Выполнение первоначальной настройки после установки приложения с помощью командной строки требуется для включения защиты клиентского устройства.

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

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

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

Чтобы проверить код возврата, выполните следующую команду:

```
echo $?
```

Если команда вернула код 0, первоначальная настройка приложения успешно завершена.

Kaspersky Endpoint Security обеспечивает защиту устройства только после обновления баз приложения.

Выбор режима использования приложения

На этом шаге выберите режим использования приложения Kaspersky Endpoint Security:

- Введите `yes`, если вы хотите использовать Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.
- Введите `no`, если вы хотите использовать Kaspersky Endpoint Security в стандартном режиме.

После завершения первоначальной настройки изменить режим использования приложения невозможно.

Определение роли виртуальной машины

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

На этом шаге укажите роль виртуальной машины (сервер или рабочая станция), на которую вы устанавливаете приложение Kaspersky Endpoint Security:

- Введите `yes`, если вы используете виртуальную машину как сервер.
- Введите `no`, если вы используете виртуальную машину как рабочую станцию.

Включение режима защиты инфраструктуры VDI

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

На этом шаге вы можете включить режим защиты инфраструктуры VDI. Этот режим позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. Если режим защиты инфраструктуры VDI включен, то обновления, требующие перезагрузки виртуальной машины, не устанавливаются. При получении обновлений, требующих перезагрузки, Легкий агент, установленный на виртуальной машине, отправляет в Kaspersky Security Center сообщение о необходимости обновить шаблон защищенных виртуальных машин.

Введите `yes`, если вы хотите включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки Kaspersky Endpoint Security на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины.

Введите `no`, если не требуется включать режим защиты инфраструктуры VDI. Рекомендуется в случае установки Kaspersky Endpoint Security на постоянную виртуальную машину или на шаблон виртуальных машин, из которого будут создаваться постоянные виртуальные машины.

Выбор языкового стандарта

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

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

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

Просмотр Лицензионного соглашения и Политики конфиденциальности

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

Принятие Лицензионного соглашения

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

После выхода из режима просмотра введите одно из следующих значений:

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

Если вы не согласны с условиями Лицензионного соглашения, процесс настройки приложения Kaspersky Endpoint Security прерывается.

Принятие Политики конфиденциальности

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

После выхода из режима просмотра введите одно из следующих значений:

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

Если вы не согласны с условиями Политики конфиденциальности, процесс настройки приложения Kaspersky Endpoint Security прерывается.

Использование Kaspersky Security Network

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

Введите одно из следующих значений:

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

Отказ от использования Kaspersky Security Network не прерывает процесс первоначальной настройки приложения Kaspersky Endpoint Security. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме и вы включили использование Kaspersky Security Network, автоматически включается облачный режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО. В режиме Легкого агента для защиты виртуальных сред работа с облегченными базами вредоносного ПО не поддерживается.

Удаление пользователей из привилегированных групп

Этот шаг отображается, только если обнаружены пользователи в группе kesladmin и/или в группе keslaudit.

На этом шаге укажите, следует ли удалить пользователей из привилегированных групп kesladmin и keslaudit. Пользователи, включенные в группы kesladmin и keslaudit, получают привилегированный доступ к функциям приложения.

Введите `yes`, чтобы удалить всех обнаруженных пользователей из группы kesladmin и/или keslaudit. Пользователи, для которых группа kesladmin или keslaudit является первичной, будут перемещены в группу nogroup. Если группа nogroup отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную.

Введите `no`, если вы не хотите, чтобы приложение удаляло пользователей из привилегированных групп.

Назначение пользователю роли администратора

На этом шаге вы можете назначить пользователю роль администратора (admin).

Введите имя пользователя, которому вы хотите назначить роль администратора.

Вы можете назначить пользователю роль администратора позже в любой момент.

Определение типа перехватчика файловых операций

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

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

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

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

Включение автоматической настройки SELinux

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

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

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

Введите `no`, если вы не хотите, чтобы приложение автоматически настроило систему SELinux.

По умолчанию приложение предлагает значение `yes`.

Если требуется, вы можете вручную настроить систему SELinux для работы с приложением позже, после завершения первоначальной настройки приложения Kaspersky Endpoint Security.

Настройка источника обновлений

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в стандартном режиме. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает обновления баз и программных модулей Легкого агента от Сервера защиты.

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

Введите одно из следующих значений:

- `KLServers` – приложение получает обновления с одного из серверов обновлений "Лаборатории Касперского".
- `SCServer` – приложение загружает обновления на защищаемое устройство с установленного в вашей организации Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновлений, если вы используете приложение Kaspersky Security Center для централизованного управления защитой устройств в вашей организации.

- < веб-адрес > – приложение загружает обновления из пользовательского источника. Вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.
- < путь > – приложение получает обновления из указанной директории.

Настройка параметров прокси-сервера

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в стандартном режиме.

На этом шаге вам нужно указать параметры прокси-сервера, если вы используете прокси-сервер для доступа в интернет. Для загрузки баз приложения с серверов обновлений требуется подключение к интернету.

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

- Если при подключении к интернету вы используете прокси-сервер, укажите адрес прокси-сервера в одном из следующих форматов:
  - < IP-адрес прокси-сервера >:< номер порта >, если для подключения к прокси-серверу не требуется аутентификация;
  - < имя пользователя >:< пароль >@< IP-адрес прокси-сервера >:< номер порта >, если для подключения к прокси-серверу требуется аутентификация.

    Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.
- Если для подключения к интернету не используется прокси-сервер, введите значение no.

По умолчанию приложение предлагает значение no.

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

Запуск обновления баз приложения

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в стандартном режиме. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает обновления баз и программных модулей Легкого агента от Сервера защиты.

На этом шаге вы можете запустить задачу обновления баз приложения на клиентском устройстве. Базы приложения содержат описания сигнатур угроз и методов борьбы с ними. Приложение использует эти записи при поиске и нейтрализации угроз. Вирусные аналитики "Лаборатории Касперского" регулярно добавляют записи о новых угрозах.

Если вы хотите отказаться от запуска обновления баз приложения, введите `no`.

Если вы хотите запустить задачу обновления баз на устройстве, введите `yes`.

По умолчанию приложение предлагает значение `yes`.

Если выбрано значение `yes`, приложение будет автоматически перезапущено после обновления баз.

Kaspersky Endpoint Security обеспечивает защиту устройства только после обновления баз приложения.

Вы можете запустить задачу обновления позже без использования скрипта первоначальной настройки.

Включение автоматического обновления баз приложения

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в стандартном режиме. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает обновления баз и программных модулей Легкого агента от Сервера защиты.

На этом шаге вы можете включить автоматическое обновление баз приложения.

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

Введите `no`, если вы не хотите, чтобы приложение автоматически обновляло базы.

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

Активация приложения

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в стандартном режиме. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает информацию о лицензии от Сервера защиты, отдельно активировать Kaspersky Endpoint Security не требуется.

На этом шаге вы можете активировать приложение с помощью кода активации или файла ключа.

Чтобы активировать приложение с помощью кода активации, требуется ввести код активации.

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

Если вы не указали код активации или файл ключа, приложение будет активировано с помощью пробного ключа на один месяц.

Вы можете активировать приложение позже без использования скрипта первоначальной настройки.

Первоначальная настройка приложения в автоматическом режиме

Вы можете выполнить первоначальную настройку приложения в автоматическом режиме.

Чтобы запустить первоначальную настройку приложения в автоматическом режиме, выполните следующую команду:

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

где < `конфигурационный файл первоначальной настройки` > – путь к конфигурационному файлу, который содержит параметры первоначальной настройки. Вы можете создать этот файл или скопировать структуру для него из конфигурационного файла autoinstall.ini, который используется для удаленной установки приложения с помощью Kaspersky Security Center.

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

Чтобы проверить код возврата, выполните следующую команду:

```
echo $?
```

Если команда вернула код 0, первоначальная настройка приложения успешно завершена.

Kaspersky Endpoint Security обеспечивает защиту устройства только после обновления баз приложения.

Для корректного обновления модулей приложения после завершения работы скрипта может потребоваться перезапустить приложение. Проверьте состояние обновлений для приложения с помощью команды `kesl-control --app-info`.

Параметры конфигурационного файла первоначальной настройки

В конфигурационном файле первоначальной настройки вы можете задавать параметры, приведенные в таблице ниже. Набор применимых параметров зависит от режима использования приложения.

Параметры конфигурационного файла первоначальной настройки

Параметр	Описание	Значения
KSVLA_MODE	Режим использования Kaspersky Endpoint Security.	`yes` – Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент). `no` – Kaspersky Endpoint Security используется в стандартном режиме.
SERVER_MODE	Роль защищаемой виртуальной машины (сервер или рабочая станция).	`yes` – защищаемая виртуальная машина используется как сервер. `no` – защищаемая виртуальная машина используется как рабочая станция.

	Параметр применяется, только если приложение используется в режиме Легкого агента.	
VDI_MODE	Включение режима защиты инфраструктуры VDI для оптимизации работы приложения на временных виртуальных машинах. Параметр применяется, только если приложение используется в режиме Легкого агента.	yes – включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки Kaspersky Endpoint Security на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. no – не включать режим защиты инфраструктуры VDI.
EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения.	yes – принять условия Лицензионного соглашения, чтобы продолжить процедуру установки приложения. no – не принимать условия Лицензионного соглашения. Установка приложения будет прервана.
PRIVACY_POLICY_AGREED	Обязательный параметр. Согласие с условиями Политики конфиденциальности.	yes – принять условия Политики конфиденциальности, чтобы продолжить процедуру установки приложения. no – не принимать условия Политики конфиденциальности. Установка приложения будет прервана.
USE_KSN	Обязательный параметр. Включение использования Kaspersky Security Network. Для включения использования KSN требуется принять условия Положения о Kaspersky Security Network.	yes – принять условия Положения о Kaspersky Security Network и включить использование KSN. no – не принимать условия Положения о Kaspersky Security Network. Если приложение Kaspersky Endpoint Security используется в стандартном режиме и вы включили использование KSN, автоматически включается облачный режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО.
GROUP_CLEAN	Обязательный параметр. Удаление пользователей из привилегированных групп kesladmin и keslaudit.	yes – удалять пользователей из привилегированных групп. Если указано значение yes и группа nogroup отсутствует, то установка будет прервана

		и вам будет предложено удалить пользователей из привилегированных групп вручную. `no` – не удалять пользователей из привилегированных групп.
LOCALE	Дополнительный параметр. Языковой стандарт, используемый для локализации событий приложения, отправляемых в Kaspersky Security Center.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр `LOCALE` не указан, устанавливается язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию `en_US.utf8`. Локализация графического интерфейса и командной строки приложения зависит от локализации, указанной в переменной окружения `LANG`. Если в переменной окружения `LANG` указана локализация, которую приложение Kaspersky Endpoint Security не поддерживает, то графический интерфейс и командная строка отображаются в английской локализации.
INSTALL_LICENSE	Код активации или файл ключа. Параметр применяется, только если приложение используется в стандартном режиме.	
UPDATER_SOURCE	Источник обновлений. Параметр применяется, только если приложение используется в стандартном режиме.	`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. Параметр применяется, только если приложение используется в стандартном режиме.	Адрес прокси-сервера.

UPDATE_EXECUTE	Запуск задачи обновления баз приложения во время процедуры настройки. Параметр применяется, только если приложение используется в стандартном режиме.	`yes` – запускать задачу обновления. `no` – не запускать задачу обновления.
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра.	`yes` – компилировать модуль ядра. `no` – не компилировать модуль ядра.
ADMIN_USER	Пользователь, которому назначается роль администратора (admin).	
CONFIGURE_SELINUX	Автоматическая настройка SELinux для работы с приложением Kaspersky Endpoint Security.	`yes` – выполнить автоматическую настройку SELinux для работы с Kaspersky Endpoint Security. `no` – не выполнять автоматическую настройку SELinux для работы с Kaspersky Endpoint Security.
DISABLE_PROTECTION	Выключение компонентов защиты и задач проверки приложения после его установки. Установка с выключенными компонентами защиты может быть удобна, например, для воспроизведения проблемы в работе приложения с целью создания файла трассировки. Если после установки приложения с параметром `DISABLE_PROTECTION=yes` вы включите нужные компоненты и задачи, то после перезапуска приложения включенные компоненты и задачи продолжат работу.	`yes` – выключить компоненты защиты и задачи проверки при запуске приложения после установки. `no` – не выключать компоненты защиты и задачи проверки при запуске приложения после установки.
DISABLE_FILEAV_ACTIONS	Выключение функций лечения и удаления файлов для компонентов приложения после его установки.	`yes` – выключить функции лечения и удаления файлов при запуске приложения после установки. `no` (значение по умолчанию) – не выключать функции лечения и удаления файлов при запуске приложения после установки.

	Если функции лечения и удаления файлов выключены, в случае обнаружения угрозы приложение не пытается лечить или удалять файлы, в которых обнаружена угроза, а только информирует пользователя об обнаружении угрозы. После установки приложения вы можете включить функции лечения и удаления файлов с помощью параметра `DisableFileAvActions` в конфигурационном файле kesl.ini.	

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

Настройка разрешающих правил в системе SELinux

Настройка SELinux для работы с приложением вручную

Если во время первоначальной настройки приложению Kaspersky Endpoint Security не удалось настроить систему SELinux автоматически или вы отказались от автоматической настройки, вы можете вручную настроить систему SELinux для работы с приложением Kaspersky Endpoint Security.

Чтобы вручную настроить SELinux для работы с приложением:

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

     ```
     # setenforce Permissive
     ```

   - Если SELinux был выключен, в конфигурационном файле /etc/selinux/config задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.
2. Убедитесь, что в системе установлена утилита semanage. Если утилита не установлена, установите пакет policycoreutils-python или policycoreutils-python-utils в зависимости от типа менеджера пакетов.
3. Если вы используете пользовательскую политику SELinux, то есть отличную от заданной по умолчанию targeted policy, назначьте метку для каждого исходного исполняемого файла приложения Kaspersky Endpoint Security в соответствии с используемой политикой SELinux, выполнив следующие команды:

   ```
   # semanage fcontext -a -t bin_t <исполняемый файл>
   # restorecon -v <исполняемый файл>
   ```

   где `<исполняемый файл>`:

- /var/opt/kaspersky/kesl/12.1.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/libexec/kesl
- /var/opt/kaspersky/kesl/12.1.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/bin/kesl-control
- /var/opt/kaspersky/kesl/12.1.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/libexec/kesl-gui
- /var/opt/kaspersky/kesl/12.1.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/shared/kesl

4. Запустите следующие задачи:
   - задачу Защита от файловых угроз:
     ```
     kesl-control --start-task 1
     ```
   - задачу Проверка важных областей:
     ```
     kesl-control --start-task 4 -W
     ```

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

5. Запустите графический пользовательский интерфейс, если вы планируете его использовать.
6. Убедитесь, что в файле audit.log нет ошибок:
   ```
   # grep kesl /var/log/audit/audit.log
   ```
7. Если в файле audit.log присутствуют ошибки, создайте и загрузите новый модуль правил на основе блокирующих записей, чтобы устранить ошибки, и снова запустите задачи, которые вы планируете запускать при использовании приложения Kaspersky Endpoint Security, выполнив следующие команды:
   ```
   # grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   # semodule -i kesl.pp
   ```

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

8. Переведите SELinux в блокирующий режим:
   ```
   # setenforce Enforcing
   ```

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

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

Настройка SELinux для запуска задачи Запуск процесса

Если в вашей операционной системе установлена система SELinux в режиме `Enforcing`, то для запуска задачи Запуск процесса вам нужно дополнительно настроить систему SELinux.

Чтобы настроить SELinux для запуска задачи Запуск процесса:

1. Переведите SELinux в неблокирующий режим:

   - Если SELinux был активирован, выполните следующую команду:

     ```
     # setenforce Permissive
     ```

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

2. Убедитесь, что в системе установлена утилита semanage. Если утилита не установлена, установите пакет policycoreutils-python или policycoreutils-python-utils в зависимости от типа менеджера пакетов.

3. Запустите задачу Запуск процесса.

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

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

5. Если в файле audit.log присутствуют ошибки, создайте и загрузите новый модуль правил на основе блокирующих записей, чтобы устранить ошибки, и снова запустите задачу Запуск процесса.

   ```
   # grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   # semodule -i kesl.pp
   ```

6. Переведите SELinux в блокирующий режим:

   ```
   # setenforce Enforcing
   ```

Запуск приложения в ОС Astra Linux в режиме замкнутой программной среды

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

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

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

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

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Установите пакет совместимости:

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

3. Создайте директорию для ключа приложения:

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

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

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

5. Обновите образ initramfs:

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

Для Astra Linux Special Edition (очередное обновление 1.5)

Чтобы запустить приложение в операционной системе Astra Linux Special Edition (очередное обновление 1.5):

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

   ```
   DIGSIG_LOAD_KEYS=1
   DIGSIG_ENFORCE=1
   ```

2. Создайте директорию для ключа приложения:

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

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

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

4. Обновите образ initramfs:

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

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

Обновление предыдущей версии приложения

Вы можете обновить до версии Kaspersky Endpoint Security 12.1 для Linux только версию Kaspersky Endpoint Security 12.0 для Linux.

Обновление Kaspersky Endpoint Security более ранних версий до версии 12.1 не предусмотрено. Если у вас установлена более ранняя версия Kaspersky Endpoint Security, вам нужно сначала удалить ее, а затем установить Kaspersky Endpoint Security 12.1 для Linux.

Перед началом обновления приложения Kaspersky Endpoint Security требуется выполнить подготовку к установке.

Процедура обновления приложения состоит из следующих этапов:

1. **Обновление Агента администрирования Kaspersky Security Center**

   Если вы управляете приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, вам нужно обновить Агент администрирования на защищаемых устройствах. Обновление выполняется путем установки новой версии Агента администрирования.

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

   > На устройстве с операционной системой Astra Linux Special Edition рекомендуется обновлять Агент администрирования удаленно с помощью Kaspersky Security Center, так как при обновлении с помощью командной строки в консоли управления Kaspersky Security Center создается новый экземпляр того же управляемого устройства, а старый становится недоступным.

   Во время обновления Агента администрирования приложение продолжает корректно работать.

2. **Обновление плагина управления Kaspersky Endpoint Security**

   Если вы управляете приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, вам нужно обновить веб-плагин или mmc-плагин управления Kaspersky Endpoint Security, в зависимости от консоли управления Kaspersky Security Center, которую вы используете.

3. **Обновление приложения и графического пользовательского интерфейса на защищаемых устройствах**

   Вам нужно обновить приложение, установленное на защищаемых устройствах. Для обновленного приложения сохраняется тот режим использования приложения, который был выбран во время установки. Если вы хотите использовать приложение в другом режиме, вам нужно удалить приложение и затем выполнить процедуру установки и первоначальной настройки приложения.

   Если Kaspersky Endpoint Security используется в стандартном режиме и вы используете графический пользовательский интерфейс приложения, вам также нужно обновить графический пользовательский интерфейс.

   Вы можете обновлять приложение и графический пользовательский интерфейс приложения следующими способами:

   - Удаленно с помощью Kaspersky Security Center.
   - Локально из командной строки.

> Если во время обновления приложения произошла ошибка, обновление откатывается и запускается предыдущая версия приложения. В этом случае отображается сообщение об ошибке, но в менеджере пакетов указывается новая версия (rpm/dpkg).

Независимо от того, было ли приложение Kaspersky Endpoint Security запущено до начала процесса обновления, если обновление завершено успешно, то запустится новая версия приложения.

При обновлении версии приложения файлы дампов предыдущей версии удаляются.

Если Kaspersky Endpoint Security используется в стандартном режиме, после обновления приложения рекомендуется запустить задачу обновления баз.

Об обновлении плагинов управления Kaspersky Endpoint Security

Обновление плагина управления Kaspersky Endpoint Security выполняется путем установки новой версии плагина управления. В зависимости от консоли управления Kaspersky Security Center, которую вы используете, вам нужно установить:

- веб-плагин управления Kaspersky Endpoint Security;
- mmc-плагин управления Kaspersky Endpoint Security.

Политики и задачи, настроенные для версии приложения Kaspersky Endpoint Security 12.0 для Linux не совместимы с обновленной версией приложения. Если для управления приложением вы используете Консоль администрирования Kaspersky Security Center, после обновления mmc-плагина управления вы можете сконвертировать политики и задачи с помощью мастера массовой конвертации политик и задач Kaspersky Security Center (см. подробнее в справке Kaspersky Security Center).

В сконвертированных политиках и задачах для большинства параметров используются значения, настроенные для предыдущей версии приложения. Для некоторых параметров устанавливаются особые значения. Параметры, которые отсутствовали в политиках и задачах предыдущей версии, в сконвертированных политиках и задачах принимают значения по умолчанию.

В Kaspersky Security Center Web Console процедура конвертации политик и задач недоступна. Если для управления приложением вы используете Web Console, вам нужно создать новые политики и задачи для приложения в Kaspersky Security Center. Некоторые значения параметров политик и задач вы можете переносить из предыдущей версии политики или задачи в новую путем экспорта и импорта параметров.

Плагины управления предыдущей версии продолжают работать после установки новой версии плагинов управления Kaspersky Endpoint Security. С их помощью вы можете управлять приложением Kaspersky Endpoint Security предыдущей версии.

Если вы обновили приложение на всех клиентских устройствах, вы можете удалить плагины управления Kaspersky Endpoint Security предыдущей версии.

Обновление приложения с помощью Kaspersky Security Center

Обновление приложения и графического пользовательского интерфейса выполняется путем удаленной установки новой версии пакетов приложения и графического пользовательского интерфейса на защищаемом устройстве.

Графический пользовательский интерфейс не поддерживается, если Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Для удаленной установки используется инсталляционный пакет приложения Kaspersky Endpoint Security. Вы можете создать инсталляционный пакет с помощью Kaspersky Security Center Web Console или с помощью Консоли администрирования.

Kaspersky Security Center Web Console поддерживает следующие основные способы развертывания:

- Установка приложения с помощью мастера развертывания защиты.
- Установка приложения с помощью задачи удаленной установки приложений.

Консоль администрирования Kaspersky Security Center поддерживает следующие основные способы развертывания:

- Установка приложения с помощью мастера удаленной установки.
- Установка приложения с помощью задачи удаленной установки приложений.

Описание процедур развертывания см. в справке Kaspersky Security Center.

Обновление приложения с помощью командной строки

Обновление приложения с помощью командной строки выполняется путем установки на устройство новой версии приложения из пакета формата RPM или DEB в соответствии с типом менеджера пакетов.

Если вы используете графический пользовательский интерфейс, для его обновления вам нужно сначала удалить пакет графического пользовательского интерфейса предыдущей версии с помощью команды `rpm -e --nodeps kesl-gui`, а затем установить пакет, содержащий файлы графического интерфейса версии 12.1.

> Графический пользовательский интерфейс не поддерживается, если Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Если в новой версии приложения изменились условия Лицензионного соглашения и/или Политики конфиденциальности, вам нужно принять новые условия в ходе обновления приложения. Ознакомьтесь с новой версией Лицензионного соглашения и/или Политики конфиденциальности:

- новая версия Лицензионного соглашения расположена в директории (~/.kesl/<версия приложения>/license.<идентификатор языка>);
- новая версия Политики конфиденциальности расположена в директории (~/.kesl/<версия приложения>/license.<идентификатор языка>).

Если вы не согласитесь с условиями Лицензионного соглашения и/или Политики конфиденциальности, приложение не будет обновлено.

Если в новой версии приложения изменились условия Положения о Kaspersky Security Network, вам нужно принять или отклонить новые условия использования Kaspersky Security Network. Ознакомьтесь с новой версией документа, расположенной в директории (~/.kesl/<версия приложения>/ksn_license.<ID языка>). Отказ от использования Kaspersky Security Network не прерывает процесс обновления приложения Kaspersky Endpoint Security. Вы можете включить, выключить или изменить режим Kaspersky Security Network позже.

Если в прошлой версии приложения вы использовали KSN и приняли условия Положения о Kaspersky Security Network, при обновлении версии приложения вам нужно принять условия Положения о Kaspersky Security Network, в противном случае использование KSN будет выключено.

Чтобы принять условия новых соглашений в ходе обновления, используйте переменные окружения `KESL_EULA_AGREED=yes`, `KESL_PRIVACY_POLICY_AGREED=yes` и `KESL_USE_KSN=yes/no`.

Чтобы обновить приложение:

1. Установите пакет приложения с помощью следующей команды в соответствии с типом менеджера пакетов. Если у вас установлен графический пользовательский интерфейс приложения предыдущей версии, вам также нужно установить пакет, содержащий файлы графического интерфейса приложения.

   - для пакета в формате RPM:

     `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kesl-12.1.0-<номер сборки>.<arch>.rpm [kesl-gui-12.1.0-<номер сборки>.<arch>.rpm]`

     где `<arch>` – тип архитектуры:

     - i386 – для 32-битных операционных систем;
     - x86_64 – для 64-битных операционных систем;
     - aarch64 – для 64-битных операционных систем для архитектуры Arm.

     > Если на операционной системе с rpm установлены пакет приложения и пакет графического интерфейса, не рекомендуется обновлять только один из пакетов.

   - для пакета в формате DEB:

     `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] apt-get install ./kesl_12.1.0-<номер сборки>_<arch>.deb [./kesl-gui_12.1.0-<номер сборки>_<arch>.deb]`

     где `<arch>` – тип архитектуры:

     - i386 – для 32-битных операционных систем;
     - amd64 – для 64-битных операционных систем;
     - arm64 – для 64-битных операционных систем для архитектуры Arm.

     > Если на операционной системе с dpkg установлены пакет приложения и пакет графического интерфейса, невозможно обновить только один из пакетов.

2. Приложение Kaspersky Endpoint Security будет автоматически перезапущено.

3. На некоторых операционных системах может потребоваться перезагрузка операционной системы, приложение отобразит сообщение об этом.

Если для управления приложением вы используете командную строку, после обновления для большинства параметров приложения используются значения, настроенные для предыдущей версии приложения. Для некоторых параметров устанавливаются особые значения. Параметры, которые отсутствовали в предыдущей версии приложения, в новой версии приложения принимают значения по умолчанию.

> Изменения параметров приложения, сделанные после завершения обновления и до перезапуска приложения, не сохраняются.

Особенности установки значений параметров при обновлении приложения

Если для управления приложением вы используете Консоль администрирования Kaspersky Security Center и после обновления приложения вы хотите использовать значения параметров политик и задач, настроенных в Kaspersky Security Center для предыдущей версии приложения, вам нужно выполнить конвертацию политик и задач (см. подробнее в справке Kaspersky Security Center).

В Kaspersky Security Center Web Console процедура конвертации политик и задач недоступна. Если для управления приложением вы используете Web Console, вам нужно создать новые политики и задачи для обновленной версией приложения. Некоторые параметры политик и задач вы можете переносить из предыдущей версии политики или задачи в новую путем экспорта и импорта параметров.

В командной строке для большинства параметров значения переносятся из предыдущей версии приложения. Вы также можете перенести параметры приложения путем экспорта параметров в файл и импорта из файла.

Параметры, которые отсутствовали в предыдущей версии приложения, принимают значения по умолчанию. Для некоторых параметров устанавливаются особые значения.

Параметры исключений

После конвертации задач в mmc-плагине в задачах проверки (типа ODS) и задачах проверки контейнеров флажки **Использовать глобальные исключения** и **Использовать исключения Защиты от файловых угроз** будут сняты. Конвертация задач в веб-плагине не поддерживается.

После обновления приложения с помощью командной строки для параметров `UseOASExclusions` и `UseGlobalExclusions` устанавливается значение `No`.

Параметры использования Kaspersky Security Network

После конвертации политики в mmc-плагине в свойствах политики будет выбран вариант **Не использовать Kaspersky Endpoint Security**. Конвертация политик в веб-плагине не поддерживается.

После обновления приложения с помощью командной строки для параметра `UseKSN` устанавливается значение `No`, если при обновлении вы установили значение параметра `KESL_USE_KSN=No`, и устанавливается значение `UseKSN=Extended`, если вы установили значение параметра `KESL_USE_KSN=Yes`. В остальных случаях значение параметра `UseKSN` после обновления не меняется.

Чтобы начать или возобновить использование Kaspersky Security Network, требуется:

- при использовании mmc- или веб-плагина выбрать вариант **Стандартный режим KSN** или **Расширенный режим KSN**;
- при использовании командной строки задать для параметра `UseKSN` значение `Basic` или `Extended`.

Параметры использования облачного режима

После конвертации политики в mmc-плагине флажок **Включить облачный режим** будет снят. Конвертация политик в веб-плагине не поддерживается.

После обновления приложения с помощью командной строки для параметра `CloudMode` устанавливаются следующие значения:

- `CloudMode=No`, в случае если параметр `UseKSN=No` после обновления;
- `CloudMode=Yes`, если параметр `UseKSN=Yes` после обновления и до обновления было установлено значение `CloudMode=Yes`.

Облачный режим доступен, если включено использование KSN. Чтобы включить облачный режим, требуется:

- при использовании mmc- или веб-плагина выбрать вариант **Расширенный режим KSN** и установить флажок **Включить облачный режим**;
- при использовании командной строки задать для параметров `UseKSN` и `CloudMode` значения `Yes`.

Режим перехвата файловых операций

Если в предыдущей версии приложения флажок **Блокировать доступ к файлам во время проверки** был снят, то после конвертации политики в mmc-плагине для параметра **Первое действие** задачи Защита от файловых угроз устанавливается значение **Блокировать**. Конвертация политик в веб-плагине не поддерживается.

Название параметра командной строки, определяющего режим перехвата файловых операций, изменилось в новой версии приложения с `InterceptorProtectionMode=Block|Notify` на `FileBlockDuringScan=Yes|No`. Если в предыдущей версии приложения параметр `InterceptorProtectionMode` имел значение `Notify`, то после обновления приложения с помощью командной строки для параметра `FileBlockDuringScan` устанавливается значение `No` и для параметра `FirstAction` задачи Защита от файловых угроз устанавливается значение `Block`.

Удаление приложения

Процедура удаления приложения Kaspersky Endpoint Security состоит из следующих этапов:

1. **Удаление приложения и графического пользовательского интерфейса приложения**

   Вам нужно удалить с защищаемых устройств пакеты приложения и графического пользовательского интерфейса приложения, если вы использовали графический пользовательский интерфейс.

   Вы можете одновременно удалить пакет приложения и пакет графического пользовательского интерфейса или удалить только пакет графического пользовательского интерфейса. Невозможно удалить только пакет приложения, если установлен пакет графического пользовательского интерфейса.

   Вы можете удалять приложение и графический пользовательский интерфейс приложения следующими способами:

   - Удаленно с помощью Kaspersky Security Center.
   - Локально из командной строки.

   > В процессе удаления приложения на устройстве будут остановлены все задачи Kaspersky Endpoint Security.

2. **Удаление Агента администрирования**

   Если вы использовали Kaspersky Security Center для управления приложением Kaspersky Endpoint Security, вам нужно удалить Агент администрирования с защищаемых устройств.

   Вы можете удалять Агент администрирования следующими способами:

   - Удаленно с помощью Kaspersky Security Center.
   - Локально из командной строки.

3. **Удаление плагина управления Kaspersky Endpoint Security**

   Если вы использовали Kaspersky Security Center для управления приложением Kaspersky Endpoint Security, вам нужно удалить веб-плагин или mmc-плагин управления Kaspersky Endpoint Security, в зависимости от консоли управления Kaspersky Security Center, которую вы использовали.

> После удаления приложения удаляется вся информация, сохраненная во время его работы, кроме базы данных лицензий. Удаляются в том числе установленные сертификаты приложения. База данных лицензий сохраняется, вы можете использовать ее для повторной установки приложения.

Если приложение было установлено в systemd-системе, то после удаления приложения параметры systemd возвращаются в исходное состояние.

Об удалении приложения и Агента администрирования с помощью Kaspersky Security Center

Вы можете удаленно удалять с клиентских устройств приложение Kaspersky Endpoint Security и Агент администрирования.

Удаление выполняется с помощью задачи удаленной деинсталляции приложений в Kaspersky Security Center Web Console или в Консоли администрирования. См подробнее в справке Kaspersky Security Center.

Если вы хотите удалить только графический пользовательский интерфейс, не удаляя при этом приложение, вам нужно установить значение параметра `USE_GUI=No` в конфигурационном файле autoinstall.ini и запустить задачу удаленной установки приложений.

Удаление выполняется в фоновом режиме. После завершения удаления приложения отобразится запрос на перезагрузку клиентского устройства.

Удаление приложения с помощью командной строки

Удаление пакета приложения и пакета графического интерфейса

Чтобы удалить приложение и графический пользовательский интерфейс, установленные из пакетов формата RPM, выполните следующую команду:

```
# rpm -e kesl kesl-gui
```

Чтобы удалить приложение и графический пользовательский интерфейс, установленные из пакетов формата DEB, выполните следующую команду:

```
# apt-get purge kesl kesl-gui
```

Удаление пакета приложения без удаления пакета графического интерфейса

Чтобы удалить приложение, установленное из пакета формата RPM, без удаления графического пользовательского интерфейса, выполните следующую команду:

```
# rpm -e kesl
```

Чтобы удалить приложение, установленное из пакета формата DEB, без удаления графического пользовательского интерфейса, выполните следующую команду:

```
# apt-get purge kesl
```

Удаление пакета графического интерфейса

Чтобы удалить графический пользовательский интерфейс, установленный из пакета формата RPM, выполните следующую команду:

```
# rpm -e kesl-gui
```

Чтобы удалить графический пользовательский интерфейс, установленный из пакета формата DEB, выполните следующую команду:

```
# apt-get purge kesl-gui
```

После завершения процедуры удаления выводится сообщение о результатах удаления.

Удаление Агента администрирования с помощью командной строки

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

```
# rpm -e klnagent
```

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

```
# rpm -e klnagent64
```

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

```
# apt-get purge klnagent
```

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

```
# apt-get purge klnagent64
```

После завершения процедуры удаления выводится сообщение о результатах удаления.

Об удалении плагинов управления Kaspersky Endpoint Security

Удаление веб-плагина управления Kaspersky Endpoint Security выполняется в Kaspersky Security Center Web Console в списке установленных плагинов (**Параметры** → **Веб-плагины**).

Для удаления mmc-плагина используйте стандартные средства удаления приложений в операционной системе. В списке приложений вам нужно выбрать для удаления **Kaspersky Endpoint Security <номер версии> для Linux**.

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Endpoint Security.

О Лицензионном соглашении

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

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом использования приложения.

Вы можете ознакомиться с условиями Лицензионного соглашения для решения Kaspersky Endpoint Security и с Политикой конфиденциальности, которая описывает обработку и передачу данных, следующими способами:

- Прочитав текст файла license.<идентификатор языка>. Этот файл включен в комплект поставки приложения.
- Во время установки приложения Kaspersky Endpoint Security.

  Вы принимаете условия Лицензионного соглашения и Политики конфиденциальности, подтверждая свое согласие с текстом Лицензионного соглашения и Политики конфиденциальности во время создания инсталляционного пакета приложения (в случае установки с помощью Kaspersky Security Center) или во время первоначальной настройки приложения (в случае установки с помощью командной строки). Если вы не согласны с условиями Лицензионного соглашения и Политики конфиденциальности, вы должны прервать установку приложения и не должны использовать приложение.
- После установки приложения Kaspersky Endpoint Security.

  После установки приложения файлы с текстом Лицензионного соглашения приложения Kaspersky Endpoint Security и Политики конфиденциальности расположены на защищаемом устройстве в директории /opt/kaspersky/kesl/doc/license.<идентификатор языка>.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Endpoint Security, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

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

Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Security прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая* – платная лицензия.

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Endpoint Security вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от 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 предоставляется лицензия;
- информация о приложении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензионном ключе

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

Вы можете добавить лицензионный ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

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

Для приложения Kaspersky Endpoint Security предусмотрены лицензионные ключи следующих *типов*:

- *Ключ приложения* – лицензионный ключ для активации функциональности приложения Kaspersky Endpoint Security. Набор доступных функций приложения зависит от лицензии, связанной с ключом приложения.

- *Ключ EDR Optimum* – дополнительный лицензионный ключ Kaspersky Endpoint Detection and Response Optimum Add-on для активации функциональности Kaspersky Endpoint Detection and Response Optimum. Этот ключ требуется, если вы используете приложение по лицензии, которая не включает функциональность Kaspersky Endpoint Detection and Response Optimum.

Лицензионный ключ может быть активным и резервным.

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен лицензионный ключ для пробной лицензии, ключ для коммерческой лицензии (коммерческий ключ) или ключ по подписке. В приложении можно добавить только один активный ключ каждого типа.

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

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве резервного лицензионного ключа.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских 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 приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если код активации был потерян после активации приложения, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего приложение.

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 приложение 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" на основе имеющегося кода активации.

О подписке

Подписка на приложение Kaspersky Endpoint Security — это заказ на использование приложения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на приложение Kaspersky Endpoint Security можно оформить у поставщика услуг (например, у интернет-провайдера). Вы можете продлевать подписку 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 приложения после окончания ограниченной подписки вам нужно продлить ее. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

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

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

Чтобы использовать приложение Kaspersky Endpoint Security по подписке, вам нужно применить код активации, предоставленный поставщиком услуг. После применения кода активации в приложение добавляется активный ключ, соответствующий лицензии на использование приложения по подписке. При этом резервный ключ может быть добавлен только с помощью кода активации и не может быть добавлен с помощью файла ключа или по подписке.

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

Сравнение функций приложения в зависимости от лицензии

Набор доступных функций приложения Kaspersky Endpoint Security зависит от лицензии (см. таблицу ниже).

Сравнение функций приложения приведено для решений на базе процессоров с архитектурой Intel. Информацию по лицензиям и доступной функциональности для решений на базе процессоров с архитектурой Arm вы можете уточнить у поставщика услуг в вашем регионе.

Сравнение функций приложения

Функция	Kaspersky	Kaspersky	Kaspersky	Kaspersky	Kaspersky	Kaspersky	Kaspersk

	Endpoint Security для бизнеса Select	Endpoint Security для бизнеса Advanced	Endpoint Security для бизнеса Total	Security для виртуальных и облачных сред (Desktop)	Security для виртуальных сред (Desktop)	Security для виртуальных и облачных сред (Desktop Enterprise)	Security д виртуальн сред (Co Server)
Защита от файловых угроз	✓	✓	✓	✓	✓	✓	✓
Защита от веб-угроз	✓	✓	✓	✓	✓	✓	✓
Защита от сетевых угроз	✓	✓	✓	✓	✓	✓	✓
Управление сетевым экраном	✓	✓	✓	✓	✓	✓	✓
Анализ поведения	✓	✓	✓	✓	✓	✓	✓
Контроль устройств	✓	✓	✓	✓	✓	✓	✓
Проверка съемных дисков	✓	✓	✓	✓	✓	✓	✓
Защита от шифрования (для общих папок)	✓	✓	✓	–	–	✓	✓
Проверка контейнеров	–	–	–	–	–	✓	–
Контроль целостности системы	–	–	–	–	–	✓	–
Контроль приложений	–	✓	✓	✓	✓	✓	–
Веб-Контроль	✓	✓	✓	✓	✓	✓	✓
Интеграция с Kaspersky Endpoint Detection and Response Optimum	–	–	–	–	–	–	–

Предоставление данных

Этот раздел содержит информацию о данных, которые приложение Kaspersky Endpoint Security может сохранять на устройстве и передавать в автоматическом режиме в "Лабораторию Касперского" в ходе своей работы.

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

Более подробная информация об обработке, хранении и уничтожении информации, полученной во время использования приложения и переданной в "Лабораторию Касперского", приведена в Лицензионном соглашении, Положении о Kaspersky Security Network и Политике конфиденциальности на веб-сайте "Лаборатории Касперского". Файлы license.<идентификатор языка> и ksn_license.<идентификатор языка> с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки приложения.

Данные, предоставляемые при использовании кода активации

Если приложение Kaspersky Endpoint Security используется в стандартном режиме и было активировано с использованием кода активации, с целью проверки законности использования приложения и получения статистической информации о распространении и использовании приложения вы соглашаетесь предоставлять в "Лабораторию Касперского" в автоматическом режиме следующую информацию:

- тип, версию и локализацию установленного приложения;
- версии установленных обновлений приложения;
- идентификатор устройства и идентификатор установки приложения на устройстве;
- код активации, с помощью которого активировано приложение;
- идентификатор действующей лицензии;
- дату и время создания лицензионного ключа приложения;
- дату и время на устройстве пользователя;
- дату и время окончания срока действия лицензии на использование приложения;
- тип, версию и разрядность операционной системы.

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

Если приложение Kaspersky Endpoint Security используется в стандартном режиме и вы используете серверы обновлений "Лаборатории Касперского" для загрузки обновлений, с целью повышения эффективности процедуры обновления и для получения статистической информации о распространении и использовании приложения, вы соглашаетесь предоставлять в "Лабораторию Касперского" в автоматическом режиме следующую информацию:

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

Данные, передаваемые при использовании приложения в режиме Легкого агента

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред в составе решения Kaspersky Security для виртуальных сред Легкий агент, во время работы приложение сохраняет и передает другим компонентам решения следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Для активации приложение Kaspersky Endpoint Security передает Серверу защиты следующие данные: срок действия подтверждения статуса лицензионного ключа, идентификатор (BIOS ID) защищенной виртуальной машины, информацию о лицензии, необходимой Легкому агенту для работы.
- Для обновления баз Легкого агента приложение Kaspersky Endpoint Security передает Серверу защиты следующие данные: идентификатор ПО, полученный из лицензии; полную версию ПО; идентификатор лицензии ПО; идентификатор установки ПО (PCID); обрабатываемый веб-адрес; тип лицензии; идентификатор запуска обновления.
- Для обеспечения защиты и в ходе выполнения задач проверки приложение Kaspersky Endpoint Security передает Серверу защиты информацию, необходимую для выполнения проверки объектов. В том числе могут передаваться имена файлов и пути к ним в файловой системе, хеши файлов, веб-адреса, а также проверяемые объекты или их фрагменты.
- В инфраструктуре под управлением VMware vCenter Server и VMware NSX Manager приложение Kaspersky Endpoint Security может передавать Серверу интеграции информацию о тегах безопасности (Security Tags), которые назначаются защищенной виртуальной машине при обнаружении вирусов, вредоносных программ и активности, характерной для сетевых атак. В том числе передаются идентификаторы защищенных виртуальных машин.
- Для получения информации, которая используется при выборе SVM для подключения, приложение Kaspersky Endpoint Security передает идентификатор защищенной виртуальной машины Серверу интеграции и Серверу защиты.
- При использовании решения Kaspersky Security для виртуальных сред Легкий агент в режиме мультитенантности информация, необходимая для формирования отчетов о защите тенантов, может передаваться от приложения Kaspersky Endpoint Security Серверу защиты. В том числе могут передаваться: идентификатор защищенной виртуальной машины; тип и версия гостевой операционной системы на защищенной виртуальной машине; периоды времени, когда приложение Kaspersky Endpoint Security было подключено к SVM.

- Для получения статистики приложение Kaspersky Endpoint Security передает Серверу защиты следующую информацию: информацию о версии ОС защищенной виртуальной машины; локализацию приложения Kaspersky Endpoint Security; названия активных компонентов приложения Kaspersky Endpoint Security; идентификатор (BIOS ID) защищенной виртуальной машины.

Указанная информация, кроме информации, необходимой для выполнения проверки объектов, и информации, которая используется при выборе SVM, передается по зашифрованным каналам передачи данных. Соединение между приложением Kaspersky Endpoint Security и Серверами защиты по умолчанию не защищено. Вы можете включить шифрование канала передачи данных между Легкими агентами и Серверами защиты в параметрах приложения Kaspersky Endpoint Security.

Данные, передаваемые приложению Kaspersky Security Center

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

- Информацию о базах, используемых в приложении:
  - список категорий баз, необходимых приложению;
  - дату и время выпуска и загрузки используемых баз в приложение;
  - дату выпуска загруженных обновлений баз приложения;
  - время последнего обновления баз приложения;
  - количество записей в текущих используемых базах приложения.
- Информацию о лицензии на использование приложения:
  - серийный номер и тип лицензии;
  - срок действия лицензии в днях;
  - количество устройств, на которые распространяется лицензия;
  - даты начала и окончания срока действия лицензии;
  - статус лицензионного ключа;
  - дату и время последней удачной синхронизации с серверами активации в случае, если приложение активировано с помощью кода активации;
  - идентификатор приложения, для активации которого предоставлена лицензия;
  - доступную по лицензии функциональность;
  - название организации, которой предоставлена лицензия;
  - дополнительную информацию в случае использования приложения по подписке (признак подписки, дату истечения периода подписки и количество дней, доступных для продления подписки, веб-адрес провайдера подписки, текущий статус и причину перехода в этот статус), дату и время активации приложения на устройстве;

- дату и время окончания срока действия лицензии на устройстве.

- Информацию об обновлениях приложения:
  - список обновлений, которые требуется установить или удалить;
  - дату выпуска обновления и наличие статуса *Критическое*;
  - название, версию и краткое описание обновления;
  - ссылку на статью с полным описанием обновления;
  - идентификатор и текст Лицензионного соглашения и Политики конфиденциальности для обновления приложения;
  - идентификатор и текст Положения о Kaspersky Security Network для обновления приложения;
  - признак возможности удаления обновления;
  - версии политики и плагина управления приложения;
  - веб-адрес для загрузки плагина управления приложения;
  - названия установленных обновлений приложения, версии и даты их установки;
  - код и описание ошибки, если установка или удаление обновления завершились с ошибкой;
  - признак и причину необходимости перезагрузки устройства или приложения по причине обновления приложения.

- Согласие или несогласие пользователя с условиями Положения о Kaspersky Security Network, Лицензионного соглашения и Политики конфиденциальности.

- Список тегов, назначенных устройству.

- Список статусов устройства и причины их назначения.

- Общий статус приложения и статус всех его компонентов; информацию о соответствии политике, статус постоянной защиты устройства, статус стабильности работы приложения, информация об остановке приложения.

- Дату и время последней проверки устройства; количество проверенных объектов; количество обнаруженных вредоносных объектов; количество заблокированных, удаленных и вылеченных объектов; количество объектов, которые не удалось вылечить; количество ошибок проверки; количество обнаруженных сетевых атак.

- Данные о текущих примененных значениях параметров приложения.

- Текущий статус и результат выполнения групповых и локальных задач и значения их параметров.

- Информацию о внешних устройствах, подключенных к клиентскому устройству (идентификатор, имя, тип, производитель, описание, серийный номер и VID/PID).

- Информацию о резервных копиях файлов, помещенных в резервное хранилище (имя, путь, размер и тип объекта, описание объекта, имя обнаруженной угрозы, версию баз приложения, с помощью которых была обнаружена угроза, дату и время помещения объекта в резервное хранилище, действия над объектом в резервном хранилище (удален, восстановлен)), а также сами файлы по запросу администратора.

- Информацию о работе каждого компонента приложения и о выполнении каждой задачи в виде событий:
  - дату и время возникновения события;
  - название и тип события;
  - уровень важности события;
  - название задачи или компонента приложения, во время работы которых произошло событие;
  - информацию о приложении, которое вызвало событие: название приложения, путь к файлу на диске, идентификатор процесса, значения параметров в случае публикации события о запуске или изменении параметров работы приложения;
  - идентификатор пользователя;
  - имя инициатора (планировщика задач, или приложения, или Kaspersky Security Center, или имя пользователя), действия которого привели к возникновению события;
  - имя и идентификатор пользователя, инициировавшего доступ к файлу;
  - результат обработки объекта или действия (описание, тип, название, уровень угрозы и точность, имя файла и тип операции над устройством, решение приложения по этой операции);
  - информацию об объекте (имя и тип объекта, путь к объекту на диске, версия объекта, размер, информация о выполненном действии, описание причины возникновения события, описание причины необработки и пропуска объекта);
  - информацию об устройстве (имя производителя, имя устройства, путь, тип устройства, тип шины, идентификатор, VID/PID, признак системного устройства, название расписания правила доступа к устройству);
  - информацию о блокировке и разблокировке устройства; информацию о заблокированных подключениях (название, описание, имя устройства, протокол, удаленный адрес и порт, локальный адрес и порт, пакетные правила, действия);
  - информацию о запрошенном веб-адресе;
  - информацию об обнаруженных объектах;
  - тип, метод и идентификатор обнаружения;
  - информацию о выполненном действии;
  - информацию о базах приложения (дату выпуска загруженных обновлений баз, информацию о применении баз, ошибки применения баз, информацию об отмене установленных обновлений баз);
  - информацию об обнаружении шифрования (имя шифровальщика; имя устройства, на котором обнаружено шифрование; информацию о блокировке и разблокировке устройства);
  - параметры приложения и сетевые параметры;
  - информацию о сработавшем правиле Контроля приложений (имя и тип) и результат его применения;
  - информацию о контейнерах и образах контейнеров (имена контейнеров или образов контейнеров, пути к контейнерам или образам контейнеров, веб-адрес репозитория);

- информацию об активных и заблокированных подключениях (название, описание и тип);
- информацию о блокировке и разблокировке доступа к недоверенным устройствам;
- информацию об использовании KSN (статус подключения к KSN, инфраструктура KSN, идентификатор Положения о KSN в расширенном режиме, принятие Положения о KSN в расширенном режиме, идентификатор Положения о KSN, принятие Положения о KSN);
- информацию о сертификатах (доменное имя, название субъекта, название издателя, дату окончания срока действия, статус сертификата, тип сертификата, время добавления сертификата, дату выпуска, серийный номер, отпечаток SHA256);
- информацию о внешних системах, входящих в состав корпоративных программных решений (адрес сервера интеграции);
- информацию о включении и выключении сетевой изоляции для устройства;
- информацию о работе в режиме Легкого агента: имя шаблона виртуальной машины, адрес Сервера интеграции;
- имя устройства, для которого включена или выключена сетевая изоляция;
- статистику выполнения задачи проверки: количество проверенных объектов; количество найденных угроз; количество зараженных объектов; количество возможно зараженных объектов; количество вылеченных объектов; количество объектов, добавленных в резервное хранилище; количество удаленных объектов; количество невылеченных объектов; количество ошибок проверки; количество объектов, защищенных паролем; количество пропущенных объектов; количество проверенных контейнеров и образов;
- информацию о версии компонента EDR Optimum, используемого в приложении;
- информацию о цепочках развития угрозы: имя сетевого списка цепочек развития угрозы, идентификатор цепочки развития угрозы.

- Информацию о работе задачи проверки целостности системы (имя, тип, путь) и информацию о снимке состояния системы.
- Информацию о сетевой активности, о пакетных правилах и о сетевых атаках.
- Информацию о роли пользователя:
  - имя и идентификатор пользователя, инициировавшего изменение роли пользователя;
  - роль пользователя;
  - имя пользователя, которому назначена или у которого отозвана роль.
- Информацию об исполняемых файлах приложений, обнаруженных на клиентском устройстве (имя, путь, тип и хеш файла; список категорий, к которым отнесено приложение; KL-категория, к которой отнесено приложение; группу доверия, к которой отнесено приложение; первое время запуска файла; название и версию приложения; название производителя приложения; информацию о сертификате, которым подписано приложение: серийный номер, отпечаток, издатель, субъект, дату выпуска, дату окончания действия и открытый ключ).
- Информацию о сетевом списке цепочек развития угрозы: идентификатор цепочки развития угрозы, время создания цепочки развития угрозы в виде метки времени, формат цепочки развития угрозы (текст или архив), размер тела цепочки развития угрозы в байтах.

Данные, предоставляемые при переходе по ссылкам из интерфейса приложения

При переходе по ссылкам из интерфейса приложения Kaspersky Endpoint Security вы соглашаетесь предоставлять в "Лабораторию Касперского" в автоматическом режиме следующую информацию:

- полную версию приложения;
- локализацию приложения;
- идентификатор приложения (PID);
- имя ссылки.

Данные, предоставляемые при использовании Kaspersky Security Network

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

Файл ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Данные, предоставляемые при использовании решения Kaspersky Anti Targeted Attack Platform

При интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA) – компонентом решения Kaspersky Anti Targeted Attack Platform – приложение Kaspersky Endpoint Security сохраняет следующую служебную информацию, которая может содержать персональные и конфиденциальные данные:

- Адреса серверов KATA.
- Открытый ключ сертификата сервера для интеграции с Kaspersky Endpoint Detection and Response (KATA).
- Криптоконтейнер с сертификатом клиента для интеграции с Kaspersky Endpoint Detection and Response (KATA).
- Учетные данные для авторизации на прокси-сервере.
- Параметры частоты синхронизации с сервером KATA и параметры передачи данных на сервер KATA.
- Статус соединения с сервером KATA и сведения об ошибках сертификата клиента и сертификата сервера.

- Параметры задач, поступающих от серверов KATA:
  - Параметры расписания запуска задач.
  - Имена и пароли учетных записей, под которыми требуется запускать задачи.
  - Версии параметров.
  - Тип запуска служб.
  - Названия служб.
  - Командную строку запуска процесса с аргументами.
  - MD5 и SHA256-хеши объектов.
  - Пути к объектам.
  - IOC-файлы.
- Параметры изоляции, в соответствии с которыми устройству будет запрещено осуществлять соединение с другими устройствами, кроме указанных в исключениях.

При интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA) приложение Kaspersky Endpoint Security сохраняет и может передавать серверу KATA следующие данные:

- Данные из запросов на синхронизацию к компоненту EDR (KATA):
  - Уникальный идентификатор.
  - Базовую часть веб-адреса сервера.
  - Имя устройства.
  - IP-адрес устройства.
  - MAC-адрес устройства.
  - Локальное время на устройстве.
  - Название и версию операционной системы, установленной на устройстве.
  - Версию Kaspersky Endpoint Security.
  - Дату выпуска используемых баз приложения.
  - Состояние лицензии.
- Данные из запросов к компоненту EDR (KATA) в отчетах о результатах выполнения задач:
  - IP-адрес устройства.
  - Уникальный идентификатор.
  - Базовую часть веб-адреса сервера.

- MAC-адрес устройства.
- Ошибки выполнения задач и коды возврата.
- Статусы, с которыми завершались задачи.
- Время завершения выполнения задач.
- Версии параметров, с которыми выполнялись задачи.
- Информацию о процессах, запущенных или остановленных на устройстве по запросу сервера: PID и UniquePID, код ошибки, хеш-суммы MD5 и SHA256 объектов.
- Файлы, запрошенные сервером.
- Данные об ошибках получения информации об объектах: полное имя объекта, при обработке которого возникла ошибка; код ошибки.
- Статус применения сетевой изоляции.
- Для индикаторов IOC возвращаются результаты поиска (сработал или не сработал каждый индикатор; найденные объекты и информация о том, какая ветка индикатора сработала).
- Для объектов, вызвавших срабатывания индикаторов IOC, возвращаются разные значения в зависимости от типа индикаторов:
  - ArpEntry: IP-адрес из ARP-таблицы (в том числе ipv6), физический адрес из ARP-таблицы.
  - File: MD5-хеш файла, SHA-256-хеш файла, полное имя файла (включая путь), размер файла.
  - Port: удаленный IP-адрес и порт, с которым в момент проверки установлено соединение; IP-адрес и порт локального адаптера; тип протокола (TCP, UDP, IP, RAWIP).
  - Process: имя процесса; аргументы процесса; путь к файлу процесса; системный PID процесса; системный PID родительского процесса; имя пользователя, от имени которого запущен процесс; дата и время запуска процесса.
  - SystemInfo: имя ОС, версия ОС, сетевое имя устройства без домена, домен или рабочая группа.
  - User: имя пользователя.

- Данные в пакетах телеметрии:
  - Данные о файлах:
    - Уникальный идентификатор файла.
    - Путь к файлу.
    - Имя файла.
    - Размер файла.
    - Атрибуты файла.
    - Дату и время создания файла.

- Дату и время последнего изменения файла.
- MD5 и SHA256-хеши объекта.
- Информацию о пользователе и группе, владеющих файлом (имя и индентификатор).

- Данные о запущенных процессах:
  - Уникальный идентификатор файла процесса.
  - Параметры запуска процесса.
  - Идентификаторы процесса.
  - Идентификатор сессии.
  - Дату и время запуска процесса.
  - Информацию о пользователе и группе, от имени которых запущен процесс (имя и индентификатор).
- Информацию об обнаруженных и обработанных угрозах:
  - Название обнаруженной угрозы и технологии, обнаружившей угрозу, согласно классификации "Лаборатории Касперского".
  - Версию баз приложения.
  - Веб-адрес, с которого был загружен зараженный объект.
  - Статус обработки угрозы.
  - Причину невозможности устранения угрозы.
  - Уникальный идентификатор файла угрозы.
- Данные об изменении файлов:
  - Уникальный идентификатор изменившегося файла.
  - Уникальный идентификатор процесса, совершившего изменения.
  - Информацию о произошедшем изменении.
- Данные об изменениях в системе:
  - Уникальный идентификатор процесса, совершившего изменения.
  - Информация о произошедшем изменении.
- Информацию о входе пользователя в систему:
  - Идентификатор сессии.
  - Информация о пользователе (имя и индентификатор).
  - IP адрес устройства, с которого установлена сессия.

- Данные о завершающихся процессах: уникальный идентификатор процесса.

Также указанная информация может сохраняться в файлах трассировки и файлах дампа.

Данные, предоставляемые при использовании Kaspersky Endpoint Detection and Response Optimum

Данные, передаваемые вместе с результатами выполнения задач *Поиск IOC*

Kaspersky Endpoint Security автоматически передает данные о результатах выполнения задач *Поиск IOC* в Kaspersky Security Center.

Данные о результатах выполнения задач *Поиск IOC* могут содержать следующую информацию:

- Сетевую информацию:
  - IP-адрес из таблицы протокола разрешения адресов (Address Resolution Protocol, ARP);
  - MAC-адрес из таблицы протокола разрешения адресов;
  - тип и имя записи DNS;
  - IP-адрес защищаемого устройства;
  - MAC-адрес защищаемого устройства;
  - IP-адрес удаленного соединения и порт;
  - IP-адрес локального сетевого адаптера;
  - номер порта, открытого на локальном адаптере;
  - номер протокола согласно стандарту Internet Assigned Numbers Authority (IANA).
- Информацию о процессах:
  - имя процесса;
  - аргументы процесса;
  - путь к исполняемому файлу процесса;
  - идентификатор процесса (PID);
  - идентификатор родительского процесса (PPID);
  - имя пользователя, запустившего процесс;
  - дату и время запуска процесса.

- Информацию о службах:
  - имя службы;
  - описание службы;
  - путь и имя исполняемого файла службы;
  - идентификатор службы;
  - тип службы (драйвер ядра, адаптер и т.д.);
  - статус службы;
  - режим запуска службы;
  - имя пользователя, под которым запущена служба.
- Информацию о файловой системе:
  - имя тома;
  - букву тома;
  - тип тома.
- Информацию об операционной системе:
  - имя и версию операционной системы;
  - сетевое имя защищаемого устройства;
  - домен или группу, к которым принадлежит устройство.
- Информацию о веб-активности:
  - имя браузера;
  - версию браузера;
  - время последнего обращения к веб-ресурсу;
  - веб-адрес HTTP-запроса;
  - имя пользователя, выполнившего HTTP-запрос;
  - имя процесса, выполнившего HTTP-запрос;
  - путь к исполняемому файлу процесса, выполнившего HTTP-запрос;
  - идентификатор процесса, выполнившего HTTP-запрос;
  - веб-адрес источника HTTP-запроса;
  - веб-адрес запрошенного ресурса;

- агент пользователя обрабатываемого веб-запроса (HTTP User-Agent);
- время выполнения HTTP-запроса;
- уникальный идентификатор процесса, выполнившего HTTP-запрос.

Данные для построения цепочки развития угрозы

Данные для построения цепочки развития угрозы могут содержать следующую информацию:

- Общую информацию об алерте:
  - дату и время алерта;
  - имя объекта;
  - режим проверки;
  - статус последнего действия, связанного с алертом;
  - причину неудачной обработки алерта.
- Информацию об обрабатываемом объекте:
  - идентификатор процесса;
  - идентификатор родительского процесса;
  - идентификатор файла процесса;
  - командную строку процесса;
  - имя пользователя, запустившего процесс;
  - идентификатор сеанса, в котором запущен процесс;
  - тип сеанса, в котором запущен процесс;
  - уровень целостности обрабатываемого процесса;
  - принадлежность пользователя к привилегированным группам;
  - идентификатор обрабатываемого объекта;
  - полное имя обрабатываемого объекта;
  - идентификатор защищаемого устройства;
  - полное имя объекта (локальный файл или веб-адрес);
  - хеш-суммы MD5 и SHA256 обрабатываемого объекта;
  - тип обрабатываемого объекта;
  - дату создания и последнего изменения объекта;

- размер обрабатываемого объекта;
- атрибуты обрабатываемого объекта;
- информацию об организации, подписавшей объект;
- результат проверки цифрового сертификата объекта;
- идентификатор безопасности (SID) объекта;
- идентификатор часового пояса объекта;
- веб-адрес загрузки объекта (только для файлов);
- название приложения, загрузившего файл;
- хеш-суммы MD5 и SHA256 приложения, загрузившего файл;
- название приложения, последний раз изменившего файл;
- хеш-суммы MD5 и SHA256 приложения, последний раз изменившего файл;
- количество запусков обрабатываемого объекта;
- дату и время первого запуска объекта;
- уникальный идентификатор файла;
- полное имя файла (локальный файл или веб-адрес);
- веб-адрес обрабатываемого веб-запроса;
- источник ссылок обрабатываемого веб-запроса (HTTP referer);
- агент пользователя обрабатываемого веб-запроса;
- тип обрабатываемого веб-запроса (GET или POST);
- локальный IP-порт для обрабатываемого веб-запроса;
- удаленный IP-порт для обрабатываемого веб-запроса;
- направление соединения (входящее или исходящее) обрабатываемого веб-запроса;
- идентификатор процесса, в который произошло внедрение вредоносного кода.

Концепция управления приложением

Для управления приложением Kaspersky Endpoint Security вы можете использовать:

- Kaspersky Security Center;
- командную строку;
- графический пользовательский интерфейс.

> Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, управление приложением с помощью Kaspersky Security Center Cloud Console и графического пользовательского интерфейса недоступно.

Набор действий, которые вы можете выполнять с помощью графического пользовательского интерфейса приложения Kaspersky Endpoint Security, ограничен.

В этом разделе описаны особенности управления приложением через Kaspersky Security Center и командную строку и основные приемы работы в консолях управления Kaspersky Security Center и в командной строке.

Управление приложением через Kaspersky Security Center

Kaspersky Security Center позволяет вам удаленно и централизованно управлять работой приложения Kaspersky Endpoint Security на клиентских устройствах. Вы можете удаленно устанавливать и удалять, запускать и останавливать приложение Kaspersky Endpoint Security; настраивать параметры работы приложения, отдельных компонентов и задач приложения; запускать и останавливать задачи на управляемых устройствах.

Для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center вы можете использовать следующие консоли управления Kaspersky Security Center:

- Консоль администрирования Kaspersky Security Center (далее также "Консоль администрирования"). Представляет собой оснастку к Microsoft Management Console (MMC), которая устанавливается на рабочее место администратора и предоставляет пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

  Интерфейс для управления приложением Kaspersky Endpoint Security через Консоль администрирования Kaspersky Security Center обеспечивает mmc-плагин управления для Консоли администрирования на основе MMC (далее также "mmc-плагин").

  > В этой справке описание работы с Консолью администрирования приведено для версии Kaspersky Security Center 14.2 Windows.

- Kaspersky Security Center Web Console (далее также "Web Console"). Представляет собой веб-интерфейс для управления системой защиты, построенной на основе приложений "Лаборатории Касперского". Вы можете работать в Kaspersky Security Center Web Console через браузер на любом устройстве, которое имеет доступ к Серверу администрирования.

  Интерфейс для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console обеспечивает веб-плагин управления (далее также "веб-плагин").

В этой справке описание работы с Web Console приведено для версии Kaspersky Security Center 15.1 Linux.

- Kaspersky Security Center Cloud Console. Представляет собой облачную консоль администрирования в составе облачной версии приложения Kaspersky Security Center, которое также называется Kaspersky Security Center Cloud Console. Облачная консоль имеет интерфейс, аналогичный интерфейсу Kaspersky Security Center Web Console. Интерфейс для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center Cloud Console также обеспечивает веб-плагин.

  В Kaspersky Security Center Cloud Console не поддерживается управление параметрами интеграции Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA).

  Управление приложением с помощью Kaspersky Security Center Cloud Console недоступно, если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Mmc-плагин и веб-плагин позволяют создавать в Kaspersky Security Center политики и задачи для управления работой приложения Kaspersky Endpoint Security:

- *Политика* – это набор параметров, который применяется на всех устройствах группы администрирования. С помощью политик вы можете устанавливать одинаковые значения параметров приложения для всех клиентских устройств, входящих в состав группы администрирования.

  Политика Kaspersky Endpoint Security определяет общие параметры работы приложения Kaspersky Endpoint Security и параметры работы отдельных функциональных компонентов приложения на устройствах, где применяется политика.

- *Задачи* для Kaspersky Endpoint Security, созданные в Kaspersky Security Center, выполняются на защищаемых устройствах и реализуют такие функции Kaspersky Endpoint Security, как проверка по требованию, активация приложения, обновление баз и модулей приложения.

  В Kaspersky Security Center вы можете создавать как задачи, которые должны выполняться на отдельном устройстве (локальные задачи), так и задачи для всех устройств группы администрирования (групповые задачи) или задачи для произвольной выборки устройств (задачи для наборов устройств).

Независимо от консоли управления Kaspersky Security Center, которую вы используете, чтобы управлять через Kaspersky Security Center работой приложения Kaspersky Endpoint Security, установленного на устройствах, вам нужно поместить эти устройства в группы администрирования. Вы можете создать группы администрирования в Kaspersky Security Center перед началом установки приложения Kaspersky Endpoint Security и настроить правила автоматического перемещения устройств в группы администрирования. Или вы можете вручную переместить устройства в группы администрирования после установки приложения Kaspersky Endpoint Security (см. подробнее в документации Kaspersky Security Center).

О плагинах управления Kaspersky Endpoint Security

Для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center требуются следующие плагины управления:

- Веб-плагин управления Kaspersky Endpoint Security (далее также *веб-плагин*) обеспечивает взаимодействие приложения Kaspersky Endpoint Security с приложением Kaspersky Security Center через Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console.

Веб-плагин требуется установить на устройство с установленным приложением Kaspersky Security Center Web Console. Управление приложением Kaspersky Endpoint Security с помощью веб-плагина доступно всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console в браузере.

- Mmc-плагин управления Kaspersky Endpoint Security (далее также *mmc-плагин*) обеспечивает взаимодействие приложения Kaspersky Endpoint Security с Kaspersky Security Center через Консоль администрирования.

  Mmc-плагин требуется установить на устройство с установленной Консолью администрирования Kaspersky Security Center.

Плагины управления Kaspersky Endpoint Security позволяют управлять приложением Kaspersky Endpoint Security с помощью политик и задач.

Дополнительная информация о плагинах управления приведена в документации Kaspersky Security Center.

О политиках Kaspersky Security Center

Политика – это набор параметров приложения Kaspersky Endpoint Security, которые применяются для всех клиентских устройств, входящих в состав группы администрирования.

Для одного приложения вы можете настроить несколько политик с различными значениями параметров. Однако одновременно для приложения может быть активна только одна политика в пределах группы администрирования. При создании новой политики все остальные политики в группе администрирования становятся неактивными. Вы можете изменить статус политики позже.

Политики, как и группы администрирования, имеют иерархию. По умолчанию дочерняя политика наследует параметры родительской политики. *Дочерняя политика* – это политика вложенного уровня иерархии, то есть политика для вложенных групп администрирования и подчиненных Серверов администрирования. Вы можете выключить наследование параметров из родительской политики.

Вы можете локально изменять значения параметров, заданные политикой, для отдельных устройств в группе администрирования, если изменение этих параметров не запрещено политикой.

Использование профилей политик позволяет более гибко настроить параметры работы приложения. *Профиль политики* может содержать параметры, которые отличаются от параметров "базовой" политики и применяются на клиентских устройствах при выполнении настроенных вами условий (правил активации). Использование профилей политики позволяет более гибко настроить параметры работы на разных устройствах. Вы можете создавать и настраивать профили в свойствах политики в разделе **Профили политики**.

Каждый параметр политики имеет атрибут "замок", который показывает, наложен ли запрет на изменение параметров в дочерних политиках и локально в параметрах приложения. Возможность изменять параметр приложения на клиентском устройстве определяется статусом "замка" у параметра в свойствах политики:

- Если параметр закрыт "замком" (🔒), это означает, что вы не можете изменить значение параметра локально или в политиках вложенного уровня иерархии. Для всех клиентских устройств группы администрирования и вложенных групп используется значение параметра, заданное этой политикой.

- Если параметр не закрыт "замком" (🔓), это означает, что вы можете изменить значение параметра локально или в политиках вложенного уровня иерархии. Если для клиентских устройств группы администрирования значения параметра заданы локально или в политиках вложенного уровня иерархии, то значение параметра, заданное в свойствах политики, не применяется.

В веб-плагине и mmc-плагине количество параметров с "замками" отличается. В веб-плагине присутствуют "замки", которых нет в mmc-плагине.

Параметры работы приложения изменяются в соответствии с параметрами политики после первого применения политики.

Подробнее о политиках и профилях политик см. в справке Kaspersky Security Center.

О задачах для Kaspersky Endpoint Security, созданных в Kaspersky Security Center

Вы можете создавать в Kaspersky Security Center задачи следующих типов для приложения Kaspersky Endpoint Security:

- локальные задачи для выполнения на отдельных устройствах;
- групповые задачи для выполнения на устройствах, входящих в группу администрирования;
- задачи для наборов устройств для выполнения на нескольких устройствах, независимо от их вхождения в группы администрирования.

  Задачи для наборов устройств выполняются только на устройствах, указанных в параметрах задачи. Если в выборку устройств, для которой сформирована задача, добавлены новые устройства, то для них эта задача не выполняется. В этом случае вам нужно создать новую задачу или изменить параметры уже существующей задачи.

Вы можете создавать любое количество групповых задач, задач для наборов устройств и локальных задач.

Задачи выполняются, только если на устройствах запущено приложение Kaspersky Endpoint Security.

Общая информация о задачах, созданных в Kaspersky Security Center, приведена в документации Kaspersky Security Center.

Для управления приложением Kaspersky Endpoint Security в Kaspersky Security Center предусмотрены следующие задачи:

- **Поиск вредоносного ПО**. Во время выполнения задачи приложение проверяет области устройства, указанные в параметрах задачи, на вирусы и другие вредоносные программы.
- **Проверка важных областей**. Во время выполнения задачи приложение проверяет загрузочные секторы, объекты автозапуска, память процессов и память ядра.
- **Проверка контейнеров**. Во время выполнения задачи приложение проверяет контейнеры и образы на вирусы и другие вредоносные программы.
- **Инвентаризация**. Во время выполнения задачи приложение получает информацию обо всех исполняемых файлах приложений, хранящихся на устройствах.
- **Проверка целостности системы**. Во время выполнения задачи приложение определяет изменение каждого объекта путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.
- **Добавление ключа**. Во время выполнения задачи приложение добавляет ключ, в том числе резервный, для активации приложения.

- **Обновление**. Во время выполнения задачи приложение обновляет базы в соответствии с настроенными параметрами обновления.
- **Откат обновления баз**. Во время выполнения задачи приложение откатывает последнее обновление баз.

Набор параметров и значения по умолчанию для параметров задач зависят от типа лицензии. Задачи Добавление ключа, Обновление и Откат обновления баз неприменимы, если приложение используется в режиме Легкого агента для защиты виртуальных сред. Также некоторые функции приложения не поддерживаются в KESL-контейнере.

Вход и выход из Web Console и Cloud Console

Kaspersky Security Center Web Console

Для входа в Web Console вам нужно знать веб-адрес Сервера администрирования и номер порта, указанные во время установки Web Console (по умолчанию используется порт 8080). Также требуется включить JavaScript в браузере.

Чтобы войти в Web Console:

1. В браузере перейдите по адресу `<веб-адрес Сервера администрирования>:<номер порта>`.

   Откроется страница входа.

2. Введите имя пользователя и пароль вашей учетной записи.

   Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев.

3. Нажмите на кнопку **Войти**.

   Если Сервер администрирования не отвечает или вы указали неверные учетные данные, отобразится сообщение об ошибке.

После входа отобразится панель мониторинга (dashboard) с последними использованными языком и темой.

Подробнее об интерфейсе Web Console см. в документации Kaspersky Security Center.

Чтобы выйти из Web Console:

в левом нижнем углу экрана выберите **<Имя учетной записи>** → **Выход**.

Web Console закроется и отобразится страница входа.

Kaspersky Security Center Cloud Console

Для Kaspersky Security Center Cloud Console используйте веб-токен для входа в учетную запись на портале Cloud Console.

Подробная информация о Kaspersky Security Center Cloud Console приведена в документации Kaspersky Security Center Cloud Console.

Управление политиками в Web Console

Вы можете выполнять следующие действия с политиками в Web Console:

- Создавать политику.
- Изменять параметры политики.

  Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения. Кроме того, настройка некоторых параметров не поддерживается в KESL-контейнере.

- Экспортировать и импортировать параметры политики.
- Копировать и перемещать политику.
- Удалять политику.
- Изменять статус политики.
- Создавать профили политики.

Общую информацию о работе с политиками см. в справке Kaspersky Security Center.

Создание политики в Web Console

Чтобы создать политику в Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик и профилей политик.

2. Выберите группу администрирования, содержащую устройства, на которых должна применяться политика. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите группу администрирования в открывшемся окне.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.

4. В открывшемся окне в списке выберите **Kaspersky Endpoint Security 12.1 для Linux**.

   Перейдите к следующему шагу мастера.

5. Укажите, в каком режиме вы используете приложение Kaspersky Endpoint Security:

   - **Стандартный режим для защиты рабочих станций и серверов** – приложение используется для защиты устройств под управлением операционных систем Linux.

- **Режим Легкого агента для защиты виртуальных сред** – приложение используется в составе решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.

6. Если вы используете приложение в режиме Легкого агента для защиты виртуальных сред, настройте параметры обнаружения SVM:

   a. Выберите способ, который используют Легкие агенты для обнаружения доступных для подключения SVM:

   - **Использовать Сервер интеграции**

     Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них.

   - **Использовать список адресов SVM, заданный вручную**

     Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.

   Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

   b. Если вы выбрали Сервер интеграции, в окне мастера отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. Если требуется, укажите новые параметры подключения:

      a. Нажмите на кнопку **Настроить** и укажите новые параметры подключения в открывшемся окне:

      - **Адрес**

        IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

        Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

      - **Порт**

        Порт для подключения к Серверу интеграции.

        По умолчанию указан порт 7271.

      b. Нажмите на кнопку **Проверить**.

c. Веб-плагин проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, в окне **Подключение к Серверу интеграции** отображается сообщение об этом.

Вы можете посмотреть информацию о сертификате, полученном от Сервера интеграции, нажав на строку **Посмотреть полученный сертификат**. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

Чтобы сохранить полученный сертификат и продолжить подключение к Серверу интеграции, в блоке **Выбор действия** выберите вариант **Игнорировать**.

d. Укажите пароль администратора Сервера интеграции (пароль учетной записи `admin`) и нажмите на кнопку **Проверить**.

Мастер создания политики выполняет подключение к Серверу интеграции. Если установить подключение не удалось, в окне отображается сообщение об ошибке. Если подключение установлено, окно **Подключение к Серверу интеграции** закрывается, в окне мастера создания политики в поле **Подключение к Серверу интеграции** отображается статус **Установлено**.

c. Если вы выбрали список адресов SVM, заданный вручную, в окне отображается список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Чтобы добавить SVM в список, нажмите на кнопку **Добавить** и в открывшемся окне укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки.

> Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения.

Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**.

Перейдите к следующему шагу мастера.

7. Примите решение об использовании Kaspersky Security Network. Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

- Если вы согласны со всеми пунктами Положения и хотите использовать Kaspersky Security Network в работе приложения, выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.

- Если вы не хотите принимать использовать Kaspersky Security Network, выберите вариант **Я не принимаю условия Положения о Kaspersky Security Network** и подтвердите свое решение в открывшемся окне.

Отказ от использования Kaspersky Security Network не прерывает процесс создания политики. Вы можете в любой момент включить, выключить использование Kaspersky Security Network или изменить режим Kaspersky Security Network для управляемых устройств в параметрах политики.

Перейдите к следующему шагу мастера.

8. Откроется окно параметров созданной политики на закладке **Общие**. Укажите название новой политики.

Вы также можете настроить следующие параметры политики:

- Состояние политики:

  - **Активна**. Политика, которая применяется к устройству в настоящий момент. Если выбран этот вариант, при следующей синхронизации устройства с Сервером администрирования эта политика станет активной на устройстве. Этот вариант выбран умолчанию.

- **Неактивна**. Политика, которая в настоящее время не применяется к устройству. Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. Позже вы можете активировать неактивную политику.

- Наследование параметров политики:

  - **Наследовать параметры родительской политики**. Если переключатель включен, значения параметров политики наследуются из групповой политики верхнего уровня и, следовательно, недоступны для изменения. По умолчанию переключатель включен.

  - **Обеспечить принудительное наследование параметров для дочерних политик**. Если переключатель включен, значения параметров дочерних политик недоступны для изменения. По умолчанию переключатель выключен.

  Общая информация о параметрах политик приведена в справке Kaspersky Security Center.

9. Если вы хотите настроить другие параметры политики, перейдите на закладку **Параметры приложения** и внесите необходимые изменения.

   Вы также можете изменить параметры политики позже.

10. Нажмите на кнопку **Сохранить**.

Созданная политика появится в списке политик.

Общую информацию об управлении политиками см. в справке Kaspersky Security Center.

Изменение параметров политики в Web Console

Чтобы изменить параметры политики в Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую устройства, на которых применяется политика. Для этого нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите группу администрирования в открывшемся окне.

   В списке отобразятся политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.

   Откроется окно свойств политики.

4. Измените параметры политики на закладке **Параметры приложения**.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Политика будет сохранена с обновленными параметрами.

Параметры политики в Web Console

Набор параметров и значения по умолчанию для параметров политики зависят от лицензии, по которой активировано приложение. Некоторые параметры политики применяются или не применяются в работе приложения в зависимости от режима, в котором используется приложение. Также некоторые функции приложения не поддерживаются в KESL-контейнере.

Вы можете настраивать параметры политики на закладке **Параметры приложения** окна свойств политики.

Параметры политики

Раздел	Подразделы
Базовая защита	Защита от файловых угроз Исключения Защиты от файловых угроз Управление сетевым экраном Защита от веб-угроз Защита от сетевых угроз
Продвинутая защита	Kaspersky Security Network Защита от шифрования Анализ поведения
Detection and Response	Managed Detection and Response Endpoint Detection and Response Optimum Endpoint Detection and Response (KATA)
Контроль безопасности	Контроль приложений Контроль устройств Контроль целостности системы Веб-Контроль
Локальные задачи	Управление задачами Проверка съемных дисков
Общие параметры	Параметры прокси-сервера Параметры приложения Параметры проверки контейнеров Параметры сети Глобальные исключения Параметры Хранилища
Режим Легкого агента	Параметры обнаружения SVM Параметры подключения к Серверу интеграции Тег для подключения к SVM Алгоритм выбора SVM Защита соединения

Управление политиками в Консоли администрирования

Вы можете выполнять следующие действия с политиками в Консоли администрирования Kaspersky Security Center:

- Создавать политику.
- Изменять параметры политики.

  Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения. Кроме того, настройка некоторых параметров не поддерживается в KESL-контейнере.

- Экспортировать и импортировать параметры политики.
- Удалять политику.
- Изменять статус политики.
- Создавать профили политики.

Общую информацию о работе с политиками см. в справке Kaspersky Security Center.

Создание политики с помощью Консоли администрирования

Чтобы создать политику в Консоли администрирования:

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, содержащую устройства, на которых должна применяться политика.

   На закладке **Устройства** папки с названием группы администрирования вы можете просмотреть список устройств, которые входят в состав этой группы администрирования.

2. В рабочей области выберите закладку **Политики**.

3. Нажмите на кнопку **Новая политика**, чтобы запустить мастер создания политики.

   Вы также можете запустить мастер с помощью пункта **Создать → Политику** контекстного меню в списке политик.

4. На первом шаге мастера в списке выберите **Kaspersky Endpoint Security 12.1 для Linux**.

   Перейдите к следующему шагу мастера.

5. Введите название новой политики.

6. Если вы хотите перенести в создаваемую политику параметры из политики предыдущей версии приложения Kaspersky Endpoint Security, установите флажок **Использовать параметры политики для предыдущей версии программы**.

   Перейдите к следующему шагу мастера.

7. Примите решение об использовании Kaspersky Security Network. Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

   - Если вы согласны со всеми пунктами Положения и хотите использовать Kaspersky Security Network в работе приложения, выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.

- Если вы не хотите принимать использовать Kaspersky Security Network, выберите вариант **Я не принимаю условия Положения о Kaspersky Security Network** и подтвердите свое решение в открывшемся окне.

Отказ от использования Kaspersky Security Network не прерывает процесс создания политики. Вы можете в любой момент включить, выключить использование Kaspersky Security Network или изменить режим Kaspersky Security Network для управляемых устройств в параметрах политики.

Перейдите к следующему шагу мастера.

8. Укажите, в каком режиме вы используете приложение Kaspersky Endpoint Security:

   - **Стандартный режим для защиты рабочих станций и серверов** – приложение используется для защиты устройств под управлением операционных систем Linux.

   - **Режим Легкого агента для защиты виртуальных сред** – приложение используется в составе решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.

   Перейдите к следующему шагу мастера.

9. Если вы используете приложение в режиме Легкого агента для защиты виртуальных сред, настройте параметры обнаружения SVM:

   a. Выберите способ, который используют Легкие агенты для обнаружения доступных для подключения SVM:

      - **Использовать Сервер интеграции**

        Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них.

      - **Использовать список адресов SVM, заданный вручную**

        Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.

      Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

   b. Если вы выбрали Сервер интеграции, в окне мастера отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. Если требуется, укажите новые параметры подключения:

      a. Нажмите на кнопку **Изменить** и укажите новые параметры подключения в открывшемся окне:

         - **Адрес**

IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен, в поле по умолчанию указано доменное имя этого устройства.

Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или Сервер интеграции установлен на другом устройстве, поле требуется заполнить вручную.

Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

- Порт

Порт для подключения к Серверу интеграции.

По умолчанию указан порт 7271.

b. Нажмите на кнопку **OK**.

c. Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, для аутентификации на Сервере интеграции используется учетная запись администратора Сервера интеграции.

В открывшемся окне введите пароль администратора Сервера интеграции (пароль учетной записи `admin`) и нажмите на кнопку **OK**.

d. Mmc-плагин проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. С помощью ссылки в окне вы можете посмотреть информацию о полученном сертификате.

При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

c. Если вы выбрали список адресов SVM, заданный вручную, в окне отображается список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Чтобы добавить SVM в список, нажмите на кнопку **Добавить** и в открывшемся окне укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки.

Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения.

Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**.

Перейдите к следующему шагу мастера.

10. Если требуется, настройте основные параметры Защиты от файловых угроз.

    Перейдите к следующему шагу мастера.

11. Если требуется, измените настроенные по умолчанию параметры защиты от файловых угроз.

    Перейдите к следующему шагу мастера.

12. Если требуется, настройте исключения из защиты от файловых угроз.

    Перейдите к следующему шагу мастера.

13. Если требуется, измените настроенные по умолчанию действия при обнаружении угрозы.

    Перейдите к следующему шагу мастера.

14. Завершите работу мастера создания политики.

Созданная политика отобразится в списке политик группы администрирования на закладке **Политики** и в папке **Политики** дерева консоли.

Вы можете изменить параметры политики позже. Общую информацию об управлении политиками см. в справке Kaspersky Security Center.

Изменение параметров политики в Консоли администрирования Kaspersky Security Center

Чтобы изменить параметры политики в Консоли администрирования:

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.

2. В рабочей области выберите закладку **Политики**.

3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

   Вы также можете открыть окно свойств политики с помощью пункта **Свойства** контекстного меню политики или по ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

4. Измените параметры политики.

5. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**, чтобы сохранить изменения.

Параметры политики в Консоли администрирования

Набор параметров и значения по умолчанию для параметров политики зависят от лицензии, по которой активировано приложение. Некоторые параметры политики применяются или не применяются в работе приложения в зависимости от режима, в котором используется приложение. Также некоторые функции приложения не поддерживаются в KESL-контейнере.

Вы можете настраивать параметры политики в разделах и подразделах окна свойств политики. О настройке общих параметров политики и параметрах событий см. в справке Kaspersky Security Center.

Параметры политики

Раздел	Подразделы
Базовая защита	Защита от файловых угроз Исключения Защиты от файловых угроз Управление сетевым экраном Защита от веб-угроз Защита от сетевых угроз
Продвинутая защита	Kaspersky Security Network Защита от шифрования Анализ поведения
Detection and Response	Managed Detection and Response Endpoint Detection and Response (KATA)
Контроль безопасности	Контроль приложений Контроль устройств Контроль целостности системы Веб-Контроль
Локальные задачи	Управление задачами Проверка съемных дисков
Общие параметры	Параметры прокси-сервера Параметры приложения Параметры проверки контейнеров Параметры сети Глобальные исключения Исключение памяти процессов Параметры Хранилища
Режим Легкого агента	Подключение к Серверу интеграции Параметры обнаружения SVM Тег для подключения к SVM Алгоритм выбора SVM Защита соединения

Управление задачами в Web Console

Вы можете выполнять следующие действия над задачами для Kaspersky Endpoint Security в Web Console:

- Создавать новые задачи.
- Изменять параметры задач.

Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения. Кроме того, настройка некоторых параметров не поддерживается в KESL-контейнере.

- Запускать, останавливать, приостанавливать и возобновлять выполнение задач.

  Задачу *Обновление* невозможно приостановить и возобновить, ее можно только запустить или остановить.

- Экспортировать и импортировать задачи.
- Удалять задачи.

В списке задач вы можете следить за выполнением задачи: статус задачи и статистику выполнения задачи на устройствах. Также вы можете создать выборку событий для контроля за выполнением задач (**Мониторинг и отчеты → Выборки событий**). Дополнительная информация о выборке событий приведена в документации Kaspersky Security Center.

Результаты выполнения задач также сохраняются локально на устройстве и в отчетах Kaspersky Security Center.

Общую информацию о работе с задачами см. в справке Kaspersky Security Center.

Если устройство находится под управлением политики, просмотр и управление задачами, созданными в Kaspersky Security Center, могут быть недоступны через командную строку или локальный пользовательский интерфейс на устройстве.

Создание задач в Web Console

Чтобы создать задачу в Web Console:

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. На первом шаге мастера выполните следующие действия:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security 12.1 для Linux**.

   b. В раскрывающемся списке **Тип задачи** выберите тип задачи, которую вы хотите создать.

   c. В поле **Название задачи** введите название новой задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите способ определения области действия задачи. Область действия задачи – это устройства, на которых будет выполняться задача:

- Выберите вариант **Назначить задачу группе администрирования**, если задача должна выполняться на всех устройствах, входящих в определенную группу администрирования.

- Выберите вариант **Задать адреса устройств вручную или импортировать из списка**, если задача должна выполняться на указанных устройствах.

- Выберите вариант **Назначить задачу выборке устройств**, если задача должна выполняться на устройствах, входящих в выборку устройств по предопределенному критерию. О создании выборки устройств см. в справке Kaspersky Security Center.

Перейдите к следующему шагу мастера.

4. В зависимости от выбранного способа определения области действия задачи выполните одно из следующих действий:

   - В дереве групп администрирования установите флажки рядом с нужными группами администрирования.

   - В списке устройств установите флажки рядом с нужными устройствами. Если нужные устройства отсутствуют в списке, вы можете добавить их следующими способами:

     - С помощью кнопки **Добавить устройства**. Вы можете добавить устройства по имени или IP-адресу, добавить устройства из указанного IP-диапазона или выбрать устройства из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.

     - С помощью кнопки **Импортировать устройства из файла**. Для импорта используется файл формата TXT с перечнем адресов устройств, где каждый адрес должен располагаться в отдельной строке.

   - В списке выберите название выборки, содержащей нужные устройства.

   Перейдите к следующему шагу мастера.

5. Чтобы настроить параметры задачи сразу после создания, на последнем шаге мастера установите флажок **Открыть окно свойств задачи после ее создания**. Задача создается с параметрами по умолчанию.

6. Завершите работу мастера.

В списке задач отобразится новая задача.

Изменение параметров задач в Web Console

Чтобы изменить параметры задачи в Web Console:

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

   Откроется список задач.

2. Выполните одно из следующих действий:

   - Если вы хотите изменить параметры задачи, которая выполняется на всех устройствах, входящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и в открывшемся окне выберите группу администрирования.

     В списке отобразятся только задачи, настроенные для выбранной группы администрирования.

- Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), нажмите на ссылку в поле **Текущий путь** в верхней части окна и в открывшемся окне выберите верхний узел с именем Сервера администрирования.

  В списке отобразятся все задачи, созданные на Сервере администрирования.

3. В списке задач выберите нужную задачу и откройте окно свойств задачи по ссылке в названии задачи.

4. Настройте параметры задачи:

   - На закладке **Общие** вы можете изменить название задачи.

   - На закладке **Параметры приложения** вы можете настроить специфические параметры задачи. Наличие настраиваемых параметров зависит от типа задачи.

   - На закладке **Расписание** вы можете настроить расписание запуска задачи и дополнительные параметры запуска и остановки задачи.

   Закладки **Общие**, **Результаты**, **Параметры**, **Расписание** и **История ревизий** окна свойств задачи стандартны для Kaspersky Security Center, см. подробнее в справке Kaspersky Security Center.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск, остановка, приостановка и возобновление задач в Web Console

Чтобы запустить, остановить, приостановить или возобновить задачу в Web Console:

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Выполните одно из следующих действий:

   - Если вы хотите запустить или остановить задачу, которая выполняется на всех устройствах, входящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и в открывшемся окне выберите группу администрирования.

     В списке отобразятся только задачи, созданные для выбранной группы администрирования.

   - Если вы хотите запустить или остановить задачу, которая выполняется на одном или нескольких устройствах (задачу для набора устройств), нажмите на ссылку в поле **Текущий путь** в верхней части окна и в открывшемся окне выберите верхний узел с именем Сервера администрирования.

     В списке отобразятся все задачи, созданные на Сервере администрирования.

3. В списке задач установите флажок рядом с названием нужной задачи и нажмите на кнопку нужного действия над списком задач.

Управление задачами в Консоли администрирования

Вы можете выполнять следующие действия над задачами для Kaspersky Endpoint Security в Консоли администрирования:

- Создавать новые задачи.

- Изменять параметры задач.

  Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения. Кроме того, настройка некоторых параметров не поддерживается в KESL-контейнере.

- Запускать, останавливать, приостанавливать и возобновлять выполнение задач.

  Задачу *Обновление* невозможно приостановить и возобновить, ее можно только запустить или остановить.

- Экспортировать и импортировать задачи.

- Удалять задачи.

В списке задач вы можете следить за выполнением задачи: статус задачи и статистику выполнения задачи на устройствах.

Информацию о ходе и результатах выполнения задач вы можете посмотреть в списке событий, которые приложение Kaspersky Endpoint Security отправляет на Сервер администрирования Kaspersky Security Center (на закладке **События** в рабочей области узла **Сервер администрирования <имя сервера>**). Также вы можете создать выборку событий для контроля за выполнением задач. Дополнительная информация о выборке событий приведена в документации Kaspersky Security Center.

Результаты выполнения задач также сохраняются локально на устройстве и в отчетах Kaspersky Security Center.

Общую информацию о работе с задачами см. в справке Kaspersky Security Center.

Если устройство находится под управлением политики, просмотр и управление задачами, созданными в Kaspersky Security Center, могут быть недоступны через командную строку или локальный пользовательский интерфейс на устройстве.

Создание задач в Консоли администрирования

Чтобы создать задачу в Консоли администрирования:

1. В Консоли администрирования выполните одно из следующих действий:

   - Если вы хотите создать задачу, которая будет выполняться на устройствах, входящих в выбранную группу администрирования, в дереве консоли в папке **Управляемые устройства** выберите эту группу администрирования, затем в рабочей области выберите закладку **Задачи** и нажмите на кнопку **Новая задача**.

     Запустится мастер создания задачи для устройств выбранной группы администрирования.

   - Если вы хотите создать задачу, которая будет выполняться на одном или нескольких устройствах (задачу для набора устройств), в дереве консоли выберите папку **Задачи** и нажмите на кнопку **Новая задача** в рабочей области.

Запустится мастер создания задачи для набора устройств.

2. На первом шаге мастера выберите **Kaspersky Endpoint Security 12.1 для Linux** и тип задачи.

   Перейдите к следующему шагу мастера.

3. Если вы создаете задачу для набора устройств, мастер предложит определить область действия задачи. Область действия задачи – это устройства, на которых будет выполняться задача.

   a. Укажите способ определения области действия задачи: выбрать устройства из списка устройств, обнаруженных Сервером администрирования; задать адреса устройств вручную; импортировать список устройств из файла или указать ранее настроенную выборку устройств (см. подробнее в справке Kaspersky Security Center).

   b. В зависимости от указанного вами способа определения области действия в открывшемся окне выполните одно из следующих действий:

      - В списке обнаруженных устройств укажите устройства, на которых будет выполняться задача. Для этого установите флажок в списке слева от названия устройства.
      - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса устройств вручную.
      - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов устройств.
      - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей устройства, на которых будет выполняться задача.

   Перейдите к следующему шагу мастера.

4. Настройте доступные параметры задачи, следуя указаниям мастера.

5. Введите название новой задачи и перейдите к следующему шагу мастера.

6. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера, на последнем шаге установите флажок **Запустить задачу после завершения работы мастера**.

7. Завершите работу мастера.

   В списке задач отобразится новая задача.

Изменение параметров задач в Консоли администрирования

Чтобы изменить параметры задачи в Консоли администрирования:

1. В Консоли администрирования выполните одно из следующих действий:

   - Если вы хотите изменить параметры задачи, которая выполняется на устройствах, входящих в определенную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите закладку **Задачи**.
   - Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), в дереве консоли выберите папку **Задачи**.

2. В списке задач выберите нужную задачу и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.

   Вы также можете открыть окно свойств задачи с помощью пункта **Свойства** контекстного меню задачи.

3. Измените параметры задачи. Наличие настраиваемых параметров зависит от типа задачи.

   Закладки **Общие**, **Уведомление**, **Расписание** и **История ревизий** окна свойств задачи стандартны для Kaspersky Security Center, см. подробнее в справке Kaspersky Security Center.

4. Нажмите на кнопку **Применить** или на кнопку **ОК** в окне **Свойства: <Название задачи>**, чтобы сохранить внесенные изменения.

Запуск, остановка, приостановка и возобновление задач в Консоли администрирования

Чтобы запустить, остановить, приостановить или возобновить задачу в Консоли администрирования:

1. В Консоли администрирования выполните одно из следующих действий:

   - Если вы хотите запустить или остановить задачу, которая выполняется на устройствах, входящих в определенную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите закладку **Задачи**.

     Откроется список задач, созданных для выбранной группы администрирования.

   - Если вы хотите запустить или остановить задачу, которая выполняется на одном или нескольких устройствах (задачу для набора устройств), в дереве консоли выберите папку **Задачи**.

     Откроется список всех задачи, созданных на Сервере администрирования.

2. В списке задач выберите нужную задачу, откройте контекстное меню задачи и выберите действие, которое вы хотите выполнить.

Управление приложением через командную строку

С помощью командной строки вы можете устанавливать и удалять, запускать и останавливать приложение Kaspersky Endpoint Security на устройстве, а также локально управлять работой приложения.

Работу функциональных компонентов приложения обеспечивают *локальные задачи Kaspersky Endpoint Security*, которые выполняются в операционной системе. Вы можете включать и выключать функциональные компоненты приложения на устройстве путем запуска и остановки задач Kaspersky Endpoint Security в командной строке. Однократные проверки устройства также выполняются путем запуска задач Kaspersky Endpoint Security. Вы можете задавать параметры работы функциональных компонентов на устройстве и параметры проверки устройства, настраивая *параметры задач* Kaspersky Endpoint Security.

Помимо параметров задач для настройки работы приложения предусмотрены следующие параметры:

- Общие параметры проверки контейнеров.
- Параметры проверки защищенных соединений.
- Общие параметры приложения, которые определяют работу приложения в целом и работу отдельных функций.

Управление приложением Kaspersky Endpoint Security в командной строке выполняется с помощью *команд управления Kaspersky Endpoint Security*.

Включение автоматического дополнения команды kesl-control (bash completion)

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

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

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

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

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

Управление задачами в командной строке

Для управления приложением Kaspersky Endpoint Security с помощью командной строки предусмотрены следующие задачи приложения:

- *Защита от файловых угроз*. Эта задача позволяет включать и выключать защиту от файловых угроз в реальном времени и определяет параметры компонента Защита от файловых угроз. Задача запускается автоматически при запуске приложения.
- *Поиск вредоносного ПО*. Эта задача позволяет выполнять проверку объектов файловой системы на наличие вредоносного ПО по требованию и определяет параметры проверки. Вы можете использовать эту задачу для полной или выборочной проверки устройства.
- *Проверка важных областей*. Эта задача позволяет выполнять проверку важных областей операционной системы по требованию и определяет параметры проверки.
- *Выборочная проверка файлов*. Эта задача предназначена для настройки и хранения параметров, которые используются во время проверки указанных файлов и директорий по команде `kesl-control --scan-file`. В результате выполнения команды приложение создает и запускает временную задачу проверки файлов.
- *Проверка контейнеров*. Эта задача позволяет выполнять проверку контейнеров и образов по требованию и определяет параметры проверки.
- *Выборочная проверка контейнеров*. Эта задача предназначена для настройки и хранения параметров, которые используются во время проверки указанных контейнеров и образов по команде `kesl-control [-T] --scan-container`. В результате выполнения команды приложение создает и запускает временную задачу проверки контейнеров.
- *Проверка съемных дисков*. Эта задача позволяет в реальном времени контролировать подключение съемных дисков к устройству и определяет параметры проверки съемных дисков и их загрузочных секторов на наличие вредоносного ПО.

- *Защита от веб-угроз*. Эта задача позволяет включать и выключать защиту от веб-угроз и определяет параметры работы компонента Защита от веб-угроз.

- *Защита от сетевых угроз*. Эта задача позволяет включать и выключать защиту от сетевых угроз и определяет параметры работы компонента Защита от сетевых угроз.

- *Защита от шифрования*. Эта задача позволяет включать и выключать защиту файлов от удаленного вредоносного шифрования и определяет параметры компонента Защита от шифрования.

- *Управление сетевым экраном*. Эта задача позволяет включать и выключать управление сетевым экраном и определяет параметры контроля сетевых соединений на устройстве.

- *Контроль приложений*. Эта задача позволяет включать и выключать Контроль приложений и определяет параметры компонента Контроль приложений.

- *Инвентаризация*. Эта задача позволяет получать информацию обо всех исполняемых файлах приложений, хранящихся на устройстве.

- *Контроль устройств*. Эта задача позволяет включать и выключать Контроль устройств и определяет параметры компонента Контроль устройств. Задача запускается автоматически при запуске приложения Kaspersky Endpoint Security.

- *Веб-Контроль*. Эта задача позволяет включать и выключать Веб-Контроль и определяет параметры компонента Веб-Контроль.

- *Анализ поведения*. Эта задача позволяет контролировать вредоносную активность приложений в операционной системе. Задача запускается автоматически при запуске приложения Kaspersky Endpoint Security.

- *Контроль целостности системы*. Эта задача позволяет в реальном времени отслеживать действия, выполняемые с объектами из области мониторинга, указанной в параметрах компонента Контроль целостности системы.

- *Проверка целостности системы*. Эта задача позволяет проверять наличие изменений в файлах и директориях, которые вы включили в область мониторинга, путем сравнения текущего состояния контролируемого объекта с ранее зафиксированным состоянием.

- *Управление резервным хранилищем*. Эта задача обеспечивает возможность сохранять резервные копии файлов в резервном хранилище, расположенном на устройстве. Задача запускается автоматически при запуске приложения и постоянно находится в оперативной памяти устройства. Задача недоступна для запуска, остановки и удаления.

- *Лицензирование*. Эта задача обеспечивает возможность активировать приложение, установленное на устройстве. Задача запускается автоматически при запуске приложения и постоянно находится в оперативной памяти устройства. Задача не имеет параметров, управление лицензионными ключами реализовано с помощью специальных команд управления. Задача недоступна для запуска, остановки и удаления.

- *Обновление*. С помощью этой задачи вы можете выполнять обновление баз и модулей приложения по расписанию и по требованию и настраивать параметры обновления.

- *Откат обновления баз*. С помощью этой задачи вы можете выполнять откат последнего обновления баз и модулей приложения.

- *Интеграция с Kaspersky Endpoint Detection and Response (KATA)*. Эта задача позволяет включать и выключать интеграцию с Kaspersky Endpoint Detection and Response (KATA) и определяет параметры интеграции.

Каждая задача приложения имеет имя, используемое в командной строке, идентификатор и тип (см. таблицу ниже).

Идентификаторы уникальны для всех задач, включая удаленные. Приложение 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.

Во время установки приложения создаются *предустановленные задачи*. Эти задачи недоступны для удаления. Для каждой предустановленной задачи зарезервированы имя и идентификатор.

Задачи, которые вы создаете во время работы с приложением, называются *пользовательские задачи*. Имена этих задач вы задаете при создании задачи. Идентификаторы пользовательских задач приложение задает и присваивает задаче при ее создании. Идентификаторы пользовательских задач начинаются со 100.

Во время работы приложение создает *временные задачи проверки*. Имена и идентификаторы временных задач задаются приложением. Временные задачи автоматически удаляются после завершения.

Задачи приложения

Задача	Имя задачи в командной строке	ID задачи	Тип задачи
Защита от файловых угроз	File_Threat_Protection	1	OAS
Поиск вредоносного ПО	Scan_My_Computer	2	ODS
Поиск вредоносного ПО (пользовательская)	задается пользователем	от 100	ODS
Выборочная проверка файлов	Scan_File	3	ODS
Проверка важных областей	Critical_Areas_Scan	4	ODS
Обновление	Update	6	Update
Обновление (пользовательская)	задается пользователем	от 100	Update
Откат обновления баз	Rollback	7	Rollback
Откат обновления баз (пользовательская)	задается пользователем	от 100	Rollback
Лицензирование	License	9	License
Управление резервным хранилищем	Backup	10	Backup
Контроль целостности системы	System_Integrity_Monitoring	11	OAFIM
Контроль целостности системы (пользовательская)	задается пользователем	от 100	ODFIM
Управление сетевым экраном	Firewall_Management	12	Firewall
Защита от шифрования	Anti_Cryptor	13	AntiCryptor
Защита от веб-угроз	Web_Threat_Protection	14	WTP
Контроль устройств	Device_Control	15	DeviceControl
Проверка съемных дисков	Removable_Drives_Scan	16	RDS
Защита от сетевых угроз	Network_Threat_Protection	17	NTP
Проверка контейнеров	Container_Scan	18	ContainerScan
Проверка контейнеров (пользовательская)	задается пользователем	от 100	ContainerScan

Выборочная проверка контейнеров	Custom_Container_Scan	19	ContainerScan
Анализ поведения	Behavior_Detection	20	BehaviorDetection
Контроль приложений	Application_Control	21	AppControl
Инвентаризация	Inventory_Scan	22	InventoryScan
Инвентаризация (пользовательская)	задается пользователем	от 100	InventoryScan
Интеграция с Kaspersky Endpoint Detection and Response (KATA)	KATAEDR	24	KATAEDR
Веб-Контроль	Web_Control	26	WebControl

Вы можете выполнять следующие действия над задачами:

- Запускать и останавливать все предустановленные и пользовательские задачи, кроме задач типов *Backup* и *License*.
- Приостанавливать и возобновлять задачи типов *ODS*, *ODFIM* и *InventoryScan*.
- Создавать и удалять пользовательские задачи. В зависимости от режима использования приложения вы можете создавать задачи следующих типов:
  - стандартный режим: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*;
  - режим Легкого агента для защиты виртуальных сред: *ODS*, *ODFIM*, *ContainerScan* и *InventoryScan*.
- Изменять параметры всех пользовательских задач и всех предустановленных задач, кроме задач типов *Rollback* и *License*.

  Если приложение используется в режиме Легкого агента для защиты виртуальных сред, параметры предустановленной задачи *Update* также недоступны для изменения.

- Настраивать расписание запуска задач.

Просмотр списка задач в командной строке

Чтобы просмотреть список задач приложения, выполните следующую команду:

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

где:

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

Отобразится список задач приложения Kaspersky Endpoint Security.

Для каждой задачи отображается следующая информация:

- `Name` – имя задачи.

- `ID` – идентификатор задачи.
- `Type` – тип задачи.
- `State` – текущее состояние задачи.

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

Просмотр состояния задачи в командной строке

Чтобы посмотреть состояние задачи, выполните следующую команду:

```
kesl-control --get-task-state <идентификатор/имя задачи> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--json` – выводить параметры в формате JSON.

Для задач приложения предусмотрены следующие основные состояния:

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

Задачи типов *ODS*, *ODFIM* и *InventoryScan* могут также находиться в одном из следующих состояний:

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

Создание задачи в командной строке

Если приложение используется в стандартном режиме, вы можете создавать задачи следующих типов: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*.

Если приложение используется в режиме Легкого агента для защиты виртуальных сред, вы можете создавать задачи следующих типов: *ODS*, *ODFIM*, *ContainerScan* и *InventoryScan*.

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

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

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

где:

- `<имя задачи>` – имя, которое вы задаете для новой задачи;
- `<тип задачи>` – обозначение типа создаваемой задачи.

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

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

где:

- `<имя задачи>` – имя, которое вы задаете для новой задачи;
- `<тип задачи>` – обозначение типа создаваемой задачи;
- `<путь к файлу>` – полный путь к конфигурационному файлу, параметры из которого будут использоваться при создании задачи;
- `--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Запуск, остановка, приостановка и возобновление задачи в командной строке

Вы можете запускать и останавливать предустановленные и пользовательские задачи, кроме задач типов *Backup* и *License*.

Вы можете приостанавливать и возобновлять задачи типов *ODS*, *ODFIM* и *InventoryScan*.

Чтобы запустить задачу, выполните следующую команду:

```
kesl-control --start-task <идентификатор/имя задачи> [-W] [--progress]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

- `[-W]` – используйте эту команду совместно с командой запуска задачи, если вы хотите включить вывод текущих событий, связанных с этой задачей.
- `[--progress]` – укажите этот ключ, если вы хотите отображать ход выполнения задачи.

  Пример:
  Запустить задачу с идентификатором 1 и включить вывод текущих событий, связанных с задачей:

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

Чтобы остановить задачу, выполните следующую команду:

```
kesl-control --stop-task <идентификатор/имя задачи> [-W]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `[-W]` – используйте эту команду совместно с командой остановки задачи, если вы хотите включить вывод текущих событий, связанных с этой задачей.

Чтобы приостановить задачу, выполните следующую команду:

```
kesl-control --suspend-task <идентификатор/имя задачи>
```

Чтобы возобновить задачу, выполните следующую команду:

```
kesl-control --resume-task <идентификатор/имя задачи>
```

Удаление задачи в командной строке

Вы можете удалять только пользовательские задачи. Предустановленные задачи недоступны для удаления.

Чтобы удалить задачу, выполните следующую команду:

```
kesl-control --delete-task <идентификатор/имя задачи>
```

где `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Вывод параметров задачи в командной строке

Вы можете выводить текущие значения параметров всех пользовательских задач и всех предустановленных задач, кроме задач *Rollback* и *License* (эти задачи не имеют параметров).

Вы можете выводить текущие значения параметров задачи в консоль или в конфигурационный файл, который вы можете использовать для изменения параметров задачи.

Чтобы вывести в консоль текущие значения параметров задачи, выполните следующую команду:

```
kesl-control --get-settings <идентификатор/имя задачи> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Чтобы вывести в конфигурационный файл текущие значения параметров задачи, выполните следующую команду:

```
kesl-control --get-settings <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены параметры задачи. Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанной директории не существует, конфигурационный файл не будет создан.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Изменение параметров задачи в командной строке

Вы можете изменять параметры всех пользовательских задач и всех предустановленных задач, кроме задач *Rollback* и *License*.

> Если приложение используется в режиме Легкого агента для защиты виртуальных сред, параметры предустановленной задачи *Update* также недоступны для изменения.

В командной строке вы можете изменять параметры задач с помощью команды `kesl-control --set-settings`:

- Вы можете изменять все параметры задачи, используя конфигурационный файл, который содержит параметры задачи. Конфигурационный файл вы можете получить с помощью команды вывода параметров задачи.
- Вы можете изменять отдельные параметры задачи, используя ключи командной строки в формате `<имя параметра>=<значение параметра>`. Текущие значения параметров задачи вы можете получить с помощью команды вывода параметров задачи.
- Вы можете восстанавливать заданные по умолчанию параметры задачи.

Вы можете добавлять и удалять области проверки и области исключения используя конфигурационный файл, который содержит параметры задачи, или ключи командной строки. Настройка областей проверки и областей исключения доступна для задач с типами *OAS*, *ODS*, *OAFIM*, *ODFIM* и *AntiCryptor*.

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

Для некоторых задач также предусмотрены отдельные команды управления, которые позволяют изменять параметры задач.

Изменение параметров задачи с помощью конфигурационного файла

Чтобы изменить значения параметров задачи с помощью конфигурационного файла:

1. Выведите параметры задачи в конфигурационный файл с помощью команды `kesl-control --get-settings`.

2. Откройте конфигурационный файл и измените значения нужных параметров.

   Для задач типа *OAS*, *ODS*, *OAFIM*, *ODFIM* и *AntiCryptor* вы можете добавлять или удалять области проверки и области исключения.

   Если вы хотите добавить область проверки, добавьте в файл секцию `[ScanScope.item_#]` со следующими параметрами:

   - `AreaDesc` – описание области проверки, содержащее дополнительную информацию об этой области.
   - `UseScanArea` – включить проверку указанной области.
   - `Path` – путь к директории с проверяемыми объектами. Вы можете указывать путь к локальной директории или включать проверку удаленных директорий, смонтированных на клиентском устройстве.
   - `AreaMask.item_#` – ограничение области проверки. Вы можете указать маску имени файлов, которые нужно проверять. По умолчанию проверка включена для всех объектов области проверки. Вы можете указать несколько элементов `AreaMask.item_#`.

   Если вы хотите добавить область исключения, добавьте в файл секцию `[ExcludedFromScanScope.item_#]` со следующими параметрами:

   - `AreaDesc` – описание области исключения, содержащее дополнительную информацию об области исключения.
   - `UseScanArea` – включить исключение указанной области.
   - `Path` – путь к директории с исключаемыми объектами. Вы можете указывать путь к локальной директории или исключать удаленные директории, смонтированные на клиентском устройстве. Возможные значения параметра зависят от типа задачи.
   - `AreaMask.item_#` – ограничение области исключения. Вы можете указать маску имени файлов, которые вы хотите исключить из области проверки. По умолчанию исключаются все объекты области.

Пример:

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

Вы можете указать несколько секций `[ScanScope.item_#]` и `[ExcludedFromScanScope.item_#]`. Приложение будет обрабатывать области по индексу в порядке возрастания.

3. Сохраните конфигурационный файл.

4. Выполните команду:

   `kesl-control --set-settings <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]`

   где:

   - `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
   - `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры задачи.
   - `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения параметров задачи, заданные в файле, будут импортированы в приложение.

Если в параметрах задачи Контроль приложений вы меняете разрешающий список или запрещаете запуск всех приложений и/или приложений, влияющих на работу приложения Kaspersky Endpoint Security, требуется запускать команду `--set-settings` с ключом `--accept`.

Изменение параметров задачи с помощью ключей командной строки

С помощью ключей команды `kesl-control --set-settings` вы можете изменять отдельные значения параметров задачи, а также добавлять или удалять области проверки и области исключения для задач типа *OAS*, *ODS*, *OAFIM*, *ODFIM* и *AntiCryptor*.

Настройка отдельных параметров задач

Чтобы изменить отдельные значения параметров задачи с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-settings <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где:

- < идентификатор/имя задачи > – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- < имя параметра >=< значение параметра > – имя и значение одного из параметров задачи. Текущие значения параметров задачи вы можете получить с помощью команды вывода параметров задачи.

Значения указанных параметров задачи будут изменены.

Если в параметрах задачи Контроль приложений вы меняете разрешающий список или запрещаете запуск всех приложений и/или приложений, влияющих на работу приложения Kaspersky Endpoint Security, требуется запускать команду `--set-settings` с ключом `--accept`.

Добавление и удаление области проверки

Чтобы добавить область проверки с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-settings < идентификатор/имя задачи > --add-path < путь >
```

где:

- < идентификатор/имя задачи > – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--add-path` < путь > – добавить путь к директории с проверяемыми объектами.

В параметры задачи будет добавлена новая секция `[ScanScope.item_#]`. Приложение будет проверять объекты в директории, указанной параметром `Path`. Остальные параметры области проверки принимают значения по умолчанию.

Если в параметрах задачи уже есть секция `[ScanScope.item_#]` с указанным значением параметра `Path`, дублирующая секция не добавляется.

Если для параметра `UseScanArea` установлено значение `No`, после выполнения этой команды значение изменится на `Yes` и будет выполняться проверка объектов, расположенных в этой директории.

Пример:
Добавление области проверки для задачи с ID=100:

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

В задачу будут добавлены следующие параметры области проверки:

```
[ScanScope.item_0001]

AreaDesc=

UseScanArea=Yes

Path=/home
```

```
AreaMask.item_0000=*
```

Чтобы удалить область проверки с помощью ключей командной строки, выполните следующую команду:

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

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--del-path <путь>` – удалить путь к директории с проверяемыми объектами.

  Секция `[ScanScope.item_#]`, содержащая указанный путь, будет удалена из параметров задачи. Приложение не будет проверять объекты в указанной директории.

Добавление и удаление области исключения

Чтобы добавить область исключения с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-settings <идентификатор/имя задачи> --add-exclusion <путь>
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--add-exclusion <путь>` – добавить путь к директории с объектами, которые вы хотите исключить из проверки.

  В параметры задачи будет добавлена новая секция `[ExcludedFromScanScope.item_#]`. Приложение будет исключать из проверки объекты в директории, указанной параметром `Path`. Остальные параметры области исключения принимают значения по умолчанию.

  Если в параметрах задачи уже есть секция `[ExcludedFromScanScope.item_#]` с указанным значением параметра `Path`, дублирующая секция не добавляется.

  Если для параметра `UseScanArea` установлено значение `No`, после выполнения этой команды значение изменится на `Yes` и объекты, расположенные в этой директории, будут исключаться из проверки.

Чтобы удалить область исключения с помощью ключей командной строки, выполните следующую команду:

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

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--del-exclusion <путь>` – удалить путь к директории с исключаемыми объектами.

Секция `[ExcludedFromScanScope.item_#]`, содержащая указанный путь, будет удалена из параметров задачи. Приложение не будет исключать из проверки объекты в указанной директории.

Восстановление параметров задачи по умолчанию в командной строке

Вы можете восстанавливать заданные по умолчанию параметры для всех пользовательских задач и всех предустановленных задач, кроме задач типов *Rollback* и *License* (эти задачи не имеют параметров).

Чтобы восстановить заданные по умолчанию параметры задачи, выполните следующую команду:

```
kesl-control --set-settings <идентификатор/имя задачи> --set-to-default
```

где `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Приложение изменит значения параметров на заданные по умолчанию.

Настройка расписания задачи в командной строке

Если приложение используется в стандартном режиме, вы можете настраивать расписание запуска для задач следующих типов: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*.

Если приложение используется в режиме Легкого агента для защиты виртуальных сред, вы можете настраивать расписание запуска для задач следующих типов: *ODS*, *ODFIM*, *ContainerScan* и *InventoryScan*.

Вы можете выводить текущие значения параметров расписания запуска задачи в консоль или в конфигурационный файл.

Чтобы вывести в консоль текущие параметры расписания запуска задачи, выполните следующую команду:

```
kesl-control --get-schedule <идентификатор/имя задачи> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Чтобы вывести в конфигурационный файл текущие параметры расписания запуска задачи, выполните следующую команду:

```
kesl-control --get-schedule <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

- `--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены параметры расписания задачи. Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанной директории не существует, конфигурационный файл не будет создан.

- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

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

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

  Вывести в консоль расписание задачи обновления:

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

Вы можете изменять параметры расписания запуска задачи следующими способами:

- Импортировать параметры из конфигурационного файла, который содержит все параметры расписания.

- Задавать с помощью командной строки отдельные параметры расписания запуска задачи в формате `<имя параметра>=<значение параметра>`.

Чтобы изменить значения параметров расписания запуска задачи с помощью конфигурационного файла, выполните следующие действия:

1. Выведите параметры задачи в конфигурационный файл с помощью команды `kesl-control --get-schedule`.

2. Измените в файле значения нужных параметров и сохраните изменения.

3. Выполните команду:

   `kesl-control --set-schedule <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]`

   где:

   `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

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

   `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

   Все значения параметров расписания запуска задачи, заданные в файле, будут импортированы в приложение.

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
```

Чтобы изменить отдельные значения параметров расписания запуска задачи с помощью командной строки, выполните следующую команду:

```
kesl-control --set-schedule <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `<имя параметра>=<значение параметра>` – имя и значение одного из параметров расписания задач.

Значения указанных параметров расписания запуска задачи будут изменены.

Примеры:

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

```
RuleType=Hourly

RunMissedStartRules=No

StartTime=2021/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
```

Управление общими параметрами приложения в командной строке

Общие параметры приложения определяют работу приложения в целом и работу отдельных функций.

Вы можете управлять общими параметрами приложения с помощью специальных команд управления:

- Выводить текущие значения общих параметров приложения в консоль или в конфигурационный файл.
- Изменять общие параметры приложения, используя конфигурационный файл, содержащий все общие параметры, или ключи командной строки в формате `< имя параметра >=< значение параметра >`.

С помощью общих параметров вы можете:

- Настраивать использование Kaspersky Security Network и облегченной версии баз вредоносного ПО в работе приложения.
- Настраивать использование прокси-сервера в работе приложения.
- Выбирать режим перехвата файловых операций (блокировать / не блокировать файлы во время проверки).
- Настраивать исключения из проверки точек монтирования (глобальные исключения).
- Настраивать исключения из проверки памяти процессов.
- Включать и выключать проверку контейнеров в реальном времени.
- Включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.

- Включать и выключать интеграцию с Kaspersky Managed Detection and Response.
- Настраивать использование журналов событий.
- Настраивать ограничение на использование ресурсов процессора для задач проверки (типа ODS).
- Ограничивать количество задач выборочной проверки, которые может одновременно запустить непривилегированный пользователь.

Вывод общих параметров приложения

Вы можете выводить текущие значения общих параметров приложения в консоль или в конфигурационный файл, который вы можете использовать для изменения параметров задачи.

Чтобы вывести в консоль текущие значения общих параметров приложения, выполните следующую команду:

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

где `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Чтобы вывести в конфигурационный файл текущие значения общих параметров приложения, выполните следующую команду:

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

где:

- `--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены общие параметры приложения. Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанной директории не существует, конфигурационный файл не будет создан.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

  Пример:
  Вывести общие параметры приложения 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 приложения

В командной строке вы можете изменять общие параметры приложения с помощью команды `kesl-control --set-app-settings`:

- Вы можете изменять все общие параметры, используя конфигурационный файл, который содержит общие параметры приложения. Конфигурационный файл вы можете получить с помощью команды вывода общих параметров.

- Вы можете изменять отдельные параметры, используя ключи командной строки в формате < имя параметра >=< значение параметра >. Текущие значения общих параметров приложения вы можете получить с помощью команды вывода общих параметров.

Чтобы изменить значения общих параметров приложения с помощью конфигурационного файла:

1. Выведите общие параметры приложения в конфигурационный файл.
2. Измените значения нужных параметров в файле и сохраните изменения.
3. Выполните команду:

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

   где:

   - `--file < путь к конфигурационному файлу >` – полный путь к конфигурационному файлу с общими параметрами приложения.
   - `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

   Все значения общих параметров, заданные в файле, будут импортированы в приложение.

Чтобы изменить значения общих параметров приложения с помощью ключей командной строки, выполните следующую команду:

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

где `< имя параметра >=< значение параметра >` – имя и значение одного из общих параметров приложения.

Значения указанных общих параметров будут изменены.

Примеры:

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

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

Установить низкий уровень детализации файла трассировки:

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

Добавить точку монтирования, которую требуется исключить из перехвата файловых операций:

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

Использование фильтра для ограничения результатов запросов

Фильтр позволяет ограничивать результаты запроса при выполнении команд управления приложением.

Условия фильтра задаются с помощью одного или нескольких *логических выражений*, скомбинированных с помощью логического оператора `and`. Условия фильтра требуется заключать в кавычки:

```
"< поле > < операция сравнения > '< значение >'"

"< поле > < операция сравнения > '< значение >' and < поле > < операция сравнения >
'< значение >'"
```

где:

- < поле > – название поля базы данных.
- < операция сравнения > – одна из следующих операций сравнения:
  - > – больше.
  - < – меньше.
  - like – соответствует указанному значению. При указании значения можно использовать маски %, например: логическое выражение "FileName like '%etc%'" задает ограничение "содержит текст "etc" в поле FileName".
  - == – равно.
  - != – не равно.
  - >= – больше или равно.
  - <= – меньше или равно.
- < значение > – значение поля. Значение требуется указывать в одинарных кавычках (').

  Значение даты вы можете указывать в системе отметок времени UNIX (количество секунд, прошедших с 00:00:00 (UTC), 1 января 1970 года) или в формате YYYY-MM-DD hh:mm:ss. Значение даты и времени указывается пользователем и отображается приложением по локальному времени пользователя.

Вы можете использовать фильтр в следующих командах управления приложением:

- Вывод информации об определенных текущих событиях приложения:

  ```
  kesl-control -W --query "< условия фильтра >"
  ```

- Вывод информации об определенных событиях приложения в журнале событий:

  ```
  kesl-control -E --query "< условия фильтра >"
  ```

- Вывод информации об определенных объектах в резервном хранилище:

  ```
  kesl-control -B --query "< условия фильтра >"
  ```

- Удаление определенных объектов из резервного хранилища:

  ```
  kesl-control -B --mass-remove --query "< условия фильтра >"
  ```

  Примеры:
  Вывести информацию о событиях, которые содержат текст "etc" в поле FileName:
  `kesl-control -E --query "FileName like '%etc%'"`
  Вывести информацию о событиях с типом ThreatDetected (обнаружена угроза):
  `kesl-control -E --query "EventType == 'ThreatDetected'"`
  Вывести информацию о событиях с типом ThreatDetected, сформированных задачами типа ODS:
  `kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"`
  Вывести информацию о событиях, сформированных после даты, указанной в системе отметок времени UNIX™ (количество секунд, прошедших с 00:00:00 (UTC), 1 января 1970 года):

```
kesl-control -E --query "Date > '1583425000'"
```
Вывести информацию о событиях, сформированных после даты, указанной в формате YYYY-MM-DD hh:mm:ss:
```
kesl-control -E --query "Date > '2022-12-22 18:52:45'"
```
Вывести информацию о файлах в резервном хранилище, имеющих высокий (High) уровень важности:
```
kesl-control -B --query "DangerLevel == 'High'"
```

Экспорт и импорт параметров приложения

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

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, параметры предустановленной задачи типа *Update* недоступны для экспорта и импорта.

Kaspersky Endpoint Security позволяет импортировать и экспортировать все параметры приложения для диагностики сбоев, проверки параметров или для упрощения настройки приложения на устройствах пользователей. При экспорте параметров все параметры приложения (включая общие параметры проверки контейнеров, параметры проверки защищенных соединений, общие параметры приложения и параметры задач) сохраняются в конфигурационном файле. Вы можете использовать этот конфигурационный файл, чтобы импортировать параметры в приложение.

Во время импорта или экспорта параметров приложение должно быть запущено. После импорта параметров требуется перезапустить приложение.

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

Чтобы экспортировать параметры приложения, выполните следующую команду:

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

где:

- `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут сохранены параметры приложения.
- `--json` – экспортировать параметры в конфигурационный файл формата JSON. Если вы не укажете ключ `--json`, экспорт будет выполнен в файл формата INI.

Чтобы импортировать параметры приложения из файла, выполните следующую команду:

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

где:

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

- `--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

При импорте параметров из файла для параметров `UseKSN` и `CloudMode` устанавливается значение `No`. Чтобы начать или возобновить использование Kaspersky Security Network, требуется задать для параметра `UseKSN` значение `Basic` или `Extended`. Чтобы включить облачный режим, требуется задать для параметра `CloudMode` значение `Yes`. Облачный режим доступен, если включено использование KSN.

После импорта параметров приложения внутренние идентификаторы задач могут измениться. Для управления задачами рекомендуется использовать имена задач.

Управление ролями пользователей с помощью командной строки

Доступ к функциям приложения Kaspersky Endpoint Security через командную строку предоставляется пользователю в соответствии с его ролью. *Роль* – это набор прав и разрешений на управление приложением.

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

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

Таким образом, роли соответствуют четырем группам пользователей операционной системы:

- kesladmin соответствует роли Администратор;

- kesluser соответствует роли Пользователь;

- keslaudit соответствует роли Аудитор;

- nokesl назначается пользователю, если не назначена ни одна из ролей. В этом случае пользователь относится к отдельной группе *пользователи без прав*.

Роли пользователей

Название роли	Роль в приложении	Пользователь ОС	Права
Администратор	admin	kesladmin	Управление параметрами приложения и параметрами задач. Управление лицензированием приложения. Назначение ролей пользователям. Отзыв ролей у пользователей (администратор не имеет права отозвать роль admin у себя самого).

			Просмотр и управление хранилищами пользователей.
Пользователь	user	kesluser	Управление только задачами выборочной проверки файлов. Запуск и остановка задач обновления. Просмотр отчетов для созданных пользователем задач. Просмотр особых событий, общих для всех пользователей приложения.
Аудитор	audit	keslaudit	Просмотр параметров приложения. Просмотр статуса приложения. Просмотр всех задач, их параметров и расписания запуска. Просмотр всех событий. Просмотр всех объектов в резервном хранилище.
—	—	nokesl	Роль в приложении не назначена, права отсутствуют.

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:
Назначить роль audit пользователю test15:

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

Отзыв роли у пользователя

Чтобы отозвать роль у определенного пользователя, выполните следующую команду:

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

Пример:
Отозвать роль audit у пользователя test15:

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

Запуск и остановка приложения

После установки приложения Kaspersky Endpoint Security на устройство запуск приложения выполняется автоматически. Далее по умолчанию приложение запускается автоматически при запуске операционной системы (на уровнях выполнения по умолчанию, принятых для каждой операционной системы).

По умолчанию при запуске приложения Kaspersky Endpoint Security автоматически запускаются следующие функциональные компоненты приложения:

- Защита от файловых угроз.
- Контроль устройств.
- Анализ поведения.
- Защита от веб-угроз – только если в операционной системе установлен один из поддерживаемых браузеров и на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен).
- Защита от сетевых угроз – только если параметры защиты от сетевых угроз на устройстве заданы через политику. По умолчанию в свойствах политики включена защита от сетевых угроз. Если на устройстве применяются локально настроенные параметры, по умолчанию защита от сетевых угроз выключена.

При запуске приложения на устройстве автоматически запускаются служебные задачи, обеспечивающие работу дополнительных функций приложения: функции активации приложения и функции резервного хранилища.

По умолчанию приложение также запускает настроенные в командной строке пользовательские задачи, для которых задан режим запуска "после запуска приложения" (режим запуска `PS`).

Если вы остановите приложение, все выполняющиеся на устройстве задачи будут прерваны. Прерванные пользовательские задачи после повторного запуска приложения автоматически не возобновляются.

Запуск и остановка приложения с помощью Web Console

Чтобы запустить или остановить приложение дистанционно:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. В списке выберите устройство, на котором вы хотите запустить или остановить приложение, и по ссылке с названием устройства откройте окно свойств устройства.
3. Выберите закладку **Приложения**.
4. Установите флажок напротив приложения **Kaspersky Endpoint Security 12.1 для Linux**.
5. Выполните одно из следующих действий:
   - Если вы хотите запустить приложение, нажмите на кнопку **Запустить**.
   - Если вы хотите остановить работу приложения, нажмите на кнопку **Остановить**.

Вы можете контролировать статус работы приложения с помощью веб-виджета **Состояние защиты** в окне **Мониторинг и отчеты / Панель мониторинга**.

Запуск и остановка приложения с помощью Консоли администрирования

Чтобы запустить или остановить приложение на клиентском устройстве:

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите закладку **Устройства**.
3. В списке управляемых устройств выберите устройство, на котором вы хотите запустить или остановить приложение, и в контекстном меню устройства выберите пункт **Свойства**.
4. В окне **Свойства: <Имя устройства>** выберите раздел **Программы**.

   В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.
5. Выберите приложение **Kaspersky Endpoint Security 12.1 для Linux**.
6. Выполните одно из следующих действий:

   - Если вы хотите запустить приложение, нажмите на кнопку  справа от списка приложений "Лаборатории Касперского" или в контекстном меню приложения выберите пункт **Запустить**.
   - Если вы хотите остановить работу приложения, нажмите на кнопку  справа от списка приложений "Лаборатории Касперского" или в контекстном меню приложения выберите пункт **Остановить**.

Запуск и остановка приложения с помощью командной строки

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

Запуск, перезапуск и остановка приложения Kaspersky Endpoint Security

Чтобы запустить приложение, выполните следующую команду:

```
systemctl start kesl
```

Чтобы остановить приложение, выполните следующую команду:

```
systemctl stop kesl
```

Чтобы перезапустить приложение, выполните следующую команду:

```
systemctl restart kesl
```

Мониторинг статуса приложения Kaspersky Endpoint Security

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

В случае сбоя приложения создается файл дампа, и приложение автоматически перезапускается.

Чтобы вывести статус приложения, выполните следующую команду:

```
systemctl status kesl
```

Просмотр состояния защиты устройства и параметров приложения

Вы можете просматривать информацию о состоянии защиты устройства и о статусе работы приложения Kaspersky Endpoint Security и его компонентов на устройстве.

Вы можете получать информацию о состоянии защиты устройства следующими способами:

- В Web Console или в Консоли администрирования с помощью статусов клиентских устройств (*OK*, *Критический*, *Предупреждение*). Устройство, на котором установлен Агент администрирования Kaspersky Security Center, является клиентским устройством для Kaspersky Security Center. Статус клиентского устройства может изменяться на *Критический* или *Предупреждение* по следующим причинам:

  - В соответствии с правилами, определенными в Kaspersky Security Center. Например, статус изменяется, если на устройстве не установлено приложение защиты, давно не выполнялся поиск вирусов, устарели базы приложения, истек срок действия лицензии или приложение работает нестабильно. Подробнее о причинах изменения статусов и настройке условий присвоения статусов см. в справке Kaspersky Security Center.

  - Kaspersky Security Center получает статус устройства от управляемого приложения, то есть от Kaspersky Endpoint Security.

    Получение статуса устройства от управляемого приложения должно быть включено в Kaspersky Security Center в списках условий назначения статусов *Критический* и *Предупреждение*. Условия назначения статусов устройства настраиваются в окне свойств группы администрирования.

  Подробнее о статусах клиентского устройства см. в справке Kaspersky Security Center.

- В Web Console или в Консоли администрирования с помощью статусов функциональных компонентов приложения Kaspersky Endpoint Security на устройстве. В свойствах приложения Kaspersky Endpoint Security, установленного на устройстве, отображается список функциональных компонентов приложения. Для каждого компонента отображается его статус.

- В командной строке с помощью команды `kesl-control --app-info`. Команда выводит информацию о работе приложения и состоянии функциональных компонентов и задач приложения.

Просмотр состояния защиты устройства в Web Console

Чтобы просмотреть состояние защиты устройства в Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и в открывшемся окне выберите группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. В списке найдите устройство, информацию о котором вы хотите просмотреть, и нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства на закладке **Общие** выберите раздел **Защита**.

В разделе **Защита** отображается следующая информация об устройстве:

- **Видимо в сети** – видимость выбранного устройства в сети: *Да* или *Нет*.
- **Статус устройства** – статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на выбранном устройстве и активности устройства в сети: *OK*, *Критический* или *Предупреждение*.
- **Описание статуса** – причины смены статуса устройства на *Критический* или *Предупреждение*.
- **Состояние защиты** – текущий статус защиты от файловых угроз на выбранном устройстве, 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 приложения Kaspersky Endpoint Security.
- **Объекты, которые не удалось вылечить** – количество зараженных объектов, которые приложению Kaspersky Endpoint Security не удалось вылечить.

Просмотр состояния защиты устройства в Консоли администрирования

Чтобы просмотреть состояние защиты устройства в Консоли администрирования:

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите закладку **Устройства**.
3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.
4. В открывшемся окне свойств управляемого устройства выберите раздел **Защита**.

В разделе **Защита** отображается следующая информация об устройстве:

- **Статус устройства** – статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на выбранном устройстве и активности устройства в сети.
- **Все проблемы** – полный список проблем, обнаруженных управляемыми приложениями, установленными на выбранном устройстве. Каждая проблема имеет статус, который приложение предлагает вам назначить устройству.
- **Статус постоянной защиты** – текущий статус защиты от файловых угроз на выбранном устройстве, например, *Выполняется* или *Остановлена*. При изменении статуса защиты новый статус отображается в окне свойств устройства только после синхронизации устройства с Сервером администрирования.
- **Последняя проверка по требованию** – дата и время выполнения последнего поиска вредоносного ПО на выбранном устройстве.

- **Всего обнаружено угроз** – общее количество угроз, обнаруженных на выбранном устройстве с момента установки приложения (первой проверки устройства) или с момента последнего обнуления счетчика угроз.

  Чтобы обнулить счетчик, нажмите на кнопку **Обнулить**.

- **Активные угрозы** – количество необработанных файлов на выбранном устройстве.

Просмотр информации о работе приложения в Web Console

Чтобы просмотреть в Web Console информацию о работе приложения:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. В списке найдите устройство, информацию о котором вы хотите просмотреть, и нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.

5. В списке приложений "Лаборатории Касперского", установленных на устройстве, нажмите на название приложения **Kaspersky Endpoint Security 12.1 для Linux**.

   Откроется окно свойств приложения.

В окне **Kaspersky Endpoint Security 12.1 для Linux** отображается следующая информация о Kaspersky Endpoint Security:

- На закладке **Общие** в разделе **Информация** содержится общая информация об установленном приложении:
  - **Имя** – название приложения.
  - **Версия** – номер версии приложения.
  - **Установлено** – дата и время установки приложения на устройстве.
  - **Последнее обновление ПО** – дата и время последнего обновления модулей приложения Kaspersky Endpoint Security.
  - **Последняя синхронизация** – дата и время последнего соединения устройства с Сервером администрирования Kaspersky Security Center.
  - **Текущий статус** – состояние защиты от файловых угроз на устройстве, например: *Выполняется* или *Приостановлена*.
  - Блок **Устанавливаемые обновления** содержит информацию об обновлении модулей приложения.
  - Блок **Базы приложения** содержит информацию о дате и времени выпуска обновления баз приложения и дате и времени последнего обновления.

- На закладке **Общие** в разделе **Лицензии** приведена информация о лицензионных ключах, добавленных в приложение, и связанных с этими ключами лицензиях.
- На закладке **Общие** в разделе **Компоненты** содержится список функциональных компонентов приложения. Для каждого компонента отображается его статус (например, *Остановлен, Приостановлен, Не установлен*) и версия.

  В строке **Режим Легкого агента для защиты виртуальных сред** вы можете посмотреть информацию о режиме использования приложения:

  - статус *выполняется* означает, что приложение используется в режиме Легкого агента;
  - статус *не установлено* означает, что приложение используется в стандартном режиме.
- На закладке **События** отображается список событий приложения на устройстве.
- На закладке **Настройка событий** отображаются типы событий, которые приложение сохраняет в хранилище событий, и время их хранения.
- На закладке **Параметры приложения** в разделе **Detection and Response** вы можете управлять сетевой изоляцией устройства.

Просмотр информации о работе приложения в Консоли администрирования

Чтобы просмотреть в Консоли администрирования Kaspersky Security Center информацию о работе приложения:

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите закладку **Устройства**.
3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.
4. В открывшемся окне свойств управляемого устройства выберите раздел **Программы**.

   В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.
5. Выберите приложение **Kaspersky Endpoint Security 12.1 для Linux** и откройте окно свойств приложения двойным щелчком мыши или с помощью кнопки **Свойства** в нижней части окна.

   Откроется окно **Параметры Kaspersky Endpoint Security 12.1 для Linux**.

В окне **Параметры Kaspersky Endpoint Security 12.1 для Linux** отображается следующая информация о Kaspersky Endpoint Security:

- В разделе **Общие** содержится общая информация об установленном приложении:
  - **Номер версии** – номер версии приложения.
  - **Установлено** – дата и время установки приложения на устройстве.

- **Текущее состояние** – состояние защиты от файловых угроз на устройстве, например: *Выполняется* или *Приостановлена*.
- **Последнее обновление ПО** – дата и время последнего обновления модулей приложения Kaspersky Endpoint Security.
- **Установленные обновления** – список модулей, для которых установлены обновления.
- **Базы программы** – дата и время выпуска обновления баз приложения.

- В разделе **Компоненты** содержится список стандартных компонентов приложения. Для каждого компонента отображается его статус (например, *Остановлен, Приостановлен, Не установлен*) и версия.

  В строке **Режим Легкого агента для защиты виртуальных сред** вы можете посмотреть информацию о режиме использования приложения:

  - статус *выполняется* означает, что приложение используется в режиме Легкого агента;
  - статус *не установлено* означает, что приложение используется в стандартном режиме.

- В разделе **Лицензионные ключи** приведена информация об активном и резервном лицензионных ключах:

  - **Серийный номер** – уникальная буквенно-цифровая последовательность.
  - **Статус** – статус лицензионного ключа, например, активный или резервный.
  - **Тип** – тип лицензии: коммерческая или пробная.
  - **Срок действия лицензии** – количество дней, в течение которых возможно использование приложения, активированного путем добавления этого ключа.
  - **Ограничения лицензии** – количество устройств, на которых вы можете использовать ключ.
  - **Дата активации** (поле доступно только для активного ключа) – дата добавления активного ключа.
  - **Срок действия** (поле доступно только для активного ключа) – дата окончания срока использования приложения, активированного путем добавления активного ключа.

- В разделе **Настройка событий** отображаются типы событий, которые приложение сохраняет в хранилище событий, и время их хранения.

- В разделе **Дополнительно** содержится информация о плагине управления приложением.

Просмотр информации о работе приложения в командной строке

Чтобы посмотреть информацию о приложении, выполните следующую команду:

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

где `--json` – выводить данные в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

В результате выполнения команды в консоль будет выведена следующая информация:

- **Название**. Название приложения.
- **Версия**. Текущая версия приложения.
- **Политика**. Информация о том, применяется ли на устройстве политика Kaspersky Security Center.
- **Информация о лицензии приложения**. Информация о лицензии приложения или статус лицензионного ключа приложения.
- **Дата окончания срока действия лицензии приложения**. Дата и время окончания срока действия лицензии приложения в формате UTC.
- **Информация о лицензии EDR Optimum**. Информация о лицензии, по которой используется функциональность Kaspersky Endpoint Detection and Response Optimum, или статус лицензионного ключа EDR Optimum.
- **Дата окончания срока действия лицензии EDR Optimum**. Дата и время окончания срока действия лицензии на использование функциональности Kaspersky Endpoint Detection and Response Optimum в формате UTC.
- **Статус подписки**. Статус подписки. Это поле отображается, если приложение используется по подписке.
- **Статус файла MDR BLOB**. Статус конфигурационного файла BLOB для интеграции с Kaspersky Managed Detection and Response.
- **Дата окончания срока действия лицензии на использование MDR**. Дата и время окончания срока действия лицензии на использование Kaspersky Managed Detection and Response в формате UTC.
- **Состояние резервного хранилища**. Состояние резервного хранилища.
- **Использование резервного хранилища**. Размер резервного хранилища.
- **Дата последнего запуска задачи Scan_My_Computer**. Время последнего запуска задачи Поиск вредоносного ПО.
- **Дата последнего выпуска баз приложения**. Время последнего выпуска баз приложения.
- **Базы приложения загружены**. Информация о том, загружены ли базы приложения.
- **Использование Kaspersky Security Network**. Информация об использовании Kaspersky Security Network: `Расширенный режим KSN`, `Стандартный режим KSN` или `Выключен`.
- **Режим Легкого агента для защиты виртуальных сред**. Информация о том, что приложение используется в режиме Легкого агента для защиты виртуальных сред. Если приложение используется в стандартном режиме, строка не отображается.
- **Инфраструктура Kaspersky Security Network**. Информация об инфраструктурном решении, которое используется для работы с репутационными базами "Лаборатории Касперского": `Kaspersky Security Network` или `Kaspersky Private Security Network`.
- **Лечение и удаление файлов выключено**. Информация о том, что включен режим работы приложения, при котором лечение и удаление файлов на диске не выполняется, независимо от настроенных в свойствах политики параметров.
- **Интеграция с Kaspersky Managed Detection and Response**. Статус интеграции с Kaspersky Managed Detection and Response: `Включена`, `Выключена`.

- **Интеграция с Kaspersky Endpoint Detection and Response Optimum**. Статус интеграции с Kaspersky Endpoint Detection and Response Optimum.
- **Защита от файловых угроз**. Статус защиты от файловых угроз в реальном времени.
- **Мониторинг контейнеров**. Статус проверки контейнеров в реальном времени.
- **Контроль целостности системы**. Статус компонента Контроль целостности системы.
- **Управление сетевым экраном**. Статус компонента Управление сетевым экраном.
- **Защита от шифрования**. Статус компонента Защита от шифрования.
- **Защита от веб-угроз**. Статус компонента Защита от веб-угроз.
- **Контроль устройств**. Статус компонента Контроль устройств.
- **Проверка съемных дисков**. Статус компонента Проверка съемных дисков.
- **Защита от сетевых угроз**. Статус компонента Защита от сетевых угроз.
- **Анализ поведения**. Статус компонента Анализ поведения.
- **Контроль приложений**. Статус компонента Контроль приложений.
- **Веб-Контроль**. Статус компонента Веб-Контроль.
- **Интеграция с Kaspersky Endpoint Detection and Response (KATA)**. Статус интеграции с Kaspersky Endpoint Detection and Response (KATA).
- **Действия после обновления**. Действия по обновлению приложения и действия, которые требуется выполнить пользователю.
- **Приложение работает нестабильно**. Информация о сбое в работе приложения и создании файла дампа. Это поле отображается, если при предыдущем запуске приложения произошел сбой.

Активация приложения и управление лицензионными ключами

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии приложения в течение срока действия лицензии.

Процедура активации приложения Kaspersky Endpoint Security заключается в добавлении на устройство активного лицензионного ключа приложения.

Если вы используете приложение по лицензии, которая не включает функциональность Kaspersky Endpoint Detection and Response Optimum, для активации этой функциональности вам нужно добавить на устройство дополнительный лицензионный ключ Kaspersky Endpoint Detection and Response Optimum Add-on (далее также "ключ EDR Optimum").

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, отдельно активировать приложение не требуется. Вы активируете решение Kaspersky Security для виртуальных сред Легкий агент, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионного ключа на SVM. Для активации функциональности Kaspersky Endpoint Detection and Response Optimum вам нужно также добавить на SVM ключ EDR Optimum.

Вы можете активировать приложение одним из следующих способов:

- Удаленно через Kaspersky Security Center:
  - При установке приложения Kaspersky Endpoint Security. Вы можете добавить лицензионный ключ приложения в инсталляционный пакет. Приложение будет активировано автоматически после установки.
  - После установки приложения Kaspersky Endpoint Security с помощью задачи активации приложения.
  - После установки приложения Kaspersky Endpoint Security путем распространения на клиентские устройства лицензионного ключа, размещенного на Сервере администрирования.
- С помощью командной строки:
  - Во время первоначальной настройки приложения Kaspersky Endpoint Security.
  - После установки приложения Kaspersky Endpoint Security с помощью команд управления.

Для добавления на устройство ключа EDR Optimum вы можете использовать задачу добавления ключа или процедуру распространения ключа на клиентские устройства. Указывать тип ключа не требуется.

Ключ EDR Optimum может быть добавлен только после добавления лицензионного ключа приложения.

Вы также можете добавить на устройство резервный ключ приложения и резервный ключ EDR Optimum. Резервный ключ становится активным либо по истечении срока действия лицензии, связанной с активным ключом, либо при удалении активного ключа. Наличие резервного ключа позволяет избежать ограничения функциональности приложения в момент окончания срока действия лицензии.

Резервный ключ может быть добавлен только после добавления активного лицензионного ключа.

Вы можете посмотреть информацию о лицензионных ключах, добавленных на устройство:

- Удаленно в Web Console или в Консоли администрирования. В свойствах приложения на клиентском устройстве в разделе **Лицензионные ключи** отображается информация об активном и резервном ключах.

- В командной строке с помощью команд управления.

Просмотр информации о лицензии и ключе в командной строке

В командной строке с помощью команды `-L --query` вы можете просматривать информацию об активном и резервном лицензионных ключах, добавленных в приложение, и о лицензии, по которой активировано приложение. Если в приложение добавлен отдельный ключ для активации функциональности Kaspersky Endpoint Detection and Response Optimum, также отображается информация об активном и резервном лицензионных ключах EDR Optimum и о лицензии EDR Optimum.

Чтобы посмотреть информацию о лицензионных ключах и лицензии на устройстве, выполните следующую команду:

```
kesl-control -L --query [--json]
```

где `--json` – выводить данные в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

В результате выполнения команды в консоль будет выведена следующая информация:

- Информация об активном ключе приложения, если ключ добавлен:
  - Дата и время окончания срока действия лицензии, по которой используется приложение.
  - Количество дней до окончания срока действия лицензии.
  - Информация об ограничении функций защиты.
  - Информация об ограничении функции обновления баз приложения.
  - Информация о статусе лицензионного ключа.
  - Тип лицензии, связанной с ключом.
  - Лицензионное ограничение ключа (количество единиц лицензирования).
  - Название приложения, для активации которого предназначен ключ.
  - Активный лицензионный ключ (уникальная буквенно-цифровая последовательность).
  - Дата активации.
- Информация о резервном ключе приложения. Отображается, если приложение используется в стандартном режиме и резервный ключ добавлен. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, информация о резервном ключе не отображается, резервный ключ добавляется на SVM.
  - Дата и время окончания срока действия лицензии, по которой используется приложение.

- Количество дней до окончания срока действия лицензии.
- Информация об ограничении функций защиты.
- Информация об ограничении функции обновления баз приложения.
- Информация о статусе лицензионного ключа.
- Тип лицензии, связанной с ключом.
- Лицензионное ограничение ключа (количество единиц лицензирования).
- Название приложения, для активации которого предназначен ключ.
- Дата активации.

- Информация об активном ключе EDR Optimum, если ключ добавлен:
  - Дата и время окончания срока действия лицензии, по которой активирована функциональность Kaspersky Endpoint Detection and Response Optimum.
  - Информация об ограничении функции обновления баз приложения.
  - Информация о статусе лицензионного ключа.
  - Тип лицензии, связанной с ключом.
  - Лицензионное ограничение ключа (количество единиц лицензирования).
  - Название приложения, для активации которого предназначен ключ.
  - Активный лицензионный ключ (уникальная буквенно-цифровая последовательность).
  - Дата активации.
- Информация о резервном ключе EDR Optimum. Отображается, если приложение используется в стандартном режиме и резервный ключ EDR Optimum добавлен. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, информация о резервном ключе не отображается, резервный ключ добавляется на SVM.
  - Дата и время окончания срока действия лицензии, по которой активирована функциональность Kaspersky Endpoint Detection and Response Optimum.
  - Информация об ограничении функции обновления баз приложения.
  - Информация о статусе лицензионного ключа.
  - Тип лицензии, связанной с ключом.
  - Лицензионное ограничение ключа (количество единиц лицензирования).
  - Название приложения, для активации которого предназначен ключ.
  - Дата активации.

Управление лицензионными ключами в командной строке

Для управления лицензионными ключами на устройстве вы можете использовать команды управления лицензионными ключами.

Команды управления лицензионными ключами могут быть выполнены, только если приложение используется в стандартном режиме. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, команды управления лицензионными ключами завершаются с ошибкой. Вы активируете приложение в составе решения Kaspersky Security для виртуальных сред Легкий агент, отдельно активировать приложение не требуется.

Чтобы добавить в приложение активный лицензионный ключ, выполните следующую команду:

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

где:

- `путь к файлу ключа` – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.
- `код активации` – код активации.

Чтобы добавить в приложение резервный лицензионный ключ, выполните следующую команду:

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

Если активный ключ еще не добавлен в приложение на устройстве, команда завершается с ошибкой.

С помощью команды добавления ключа вы можете добавить как лицензионные ключи приложения, так и лицензионные ключи EDR Optimum. Указывать тип ключа в команде не требуется.

Чтобы удалить активный ключ приложения, выполните следующую команду:

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

Чтобы удалить резервный ключ приложения, выполните следующую команду:

```
kesl-control [-L] --remove-reserve-key
```

Чтобы удалить активный ключ EDR Optimum, выполните следующую команду:

```
kesl-control [-L] --remove-active-key --edr-optimum
```

Чтобы удалить резервный ключ EDR Optimum, выполните следующую команду:

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

Обновление баз и модулей приложения

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) будет недоступна в приложении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

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

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

В процессе обновления базы и модули приложения загружаются и устанавливаются на вашем устройстве.

Вы можете получать обновления баз и модулей приложения с серверов обновлений "Лаборатории Касперского", из хранилища Сервера администрирования, из локальных или сетевых директорий и из других источников обновлений.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, в качестве источника обновлений используется директория на SVM.

В процессе обновления модули приложения и базы на вашем устройстве сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули приложения отличаются от актуальной версии, на устройство устанавливается недостающая часть обновлений.

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

Загрузка обновлений с серверов обновлений "Лаборатории Касперского" или с других FTP-, HTTP- или HTTPS-серверов осуществляется по стандартным сетевым протоколам. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, укажите параметры прокси-сервера в общих параметрах приложения.

Независимо от источника обновлений загрузка пакета обновлений и установка обновления баз и модулей приложения на устройстве выполняется с помощью задачи *Обновление*.

В приложении создается предустановленная задача *Обновление*. С помощью этой задачи вы можете выполнять обновление баз и модулей приложения по расписанию и по требованию и настраивать параметры обновления.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, обновление баз на защищенных виртуальных машинах выполняется с помощью специальной локальной задачи *Обновление*, в которой в качестве источника обновлений указана директория на SVM. Задача обновления запускается автоматически. Вы не можете удалять эту задачу и изменять ее параметры.

Обновление баз и модулей приложения с помощью задач, созданных в Kaspersky Security Center, не поддерживается.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме, в Kaspersky Security Center вы можете использовать групповую задачу *Обновление*, которую мастер первоначальной настройки создает после установки mmc-плагина управления или веб-плагина управления Kaspersky Endpoint Security.

Вы также можете создавать пользовательские задачи обновления в командной строке и в Kaspersky Security Center.

Вы можете настраивать следующие параметры обновления баз и модулей приложения:

- Выбирать источник, из которого приложение будет получать обновления, в зависимости от используемой схемы обновления.
- Настраивать время ожидания ответа от выбранного источника обновлений при попытке соединения с ним. Если в течение указанного времени от источника обновлений не приходит ответ, приложение обращается к другому указанному источнику обновлений.
- Выбирать режим загрузки и установки модулей приложения и обновлений версии приложения: загружать и устанавливать, только загружать или не загружать.
- Настраивать расписание запуска задачи обновления. По умолчанию приложение обновляет базы с периодичностью один раз в 60 минут.

Об обновлении баз и модулей

В процессе обновления на вашем устройстве загружаются и устанавливаются следующие объекты:

- Базы приложения. Базы приложения включают в себя базы сигнатур вредоносных программ, описание сетевых атак, базы вредоносных и фишинговых веб-адресов, базы баннеров, спам-базы и другие данные.

  Если обновление баз на устройстве прерывается или завершается с ошибкой, приложение продолжает использовать предыдущую установленную версию баз. Если ранее базы приложения не устанавливались, приложение продолжает работу в режиме "без баз". Обновление баз и модулей приложения остается доступным.

  Базы актуальны, если они были загружены менее трех дней назад. По умолчанию приложение формирует событие *Базы устарели* (*BasesAreOutOfDate*), если последние установленные обновления баз были опубликованы на серверах "Лаборатории Касперского" более трех, но менее семи дней назад. Если базы не обновляются в течение семи дней, приложение формирует событие *Базы сильно устарели* (*BasesAreTotallyOutOfDate*).

- Модули приложения. Обновление модулей предназначено для устранения уязвимостей в приложении и улучшения методов защиты устройства. Обновления модулей могут менять поведение компонентов приложения и добавлять новые возможности.

  Обновление модулей приложения может быть установлено вне зависимости от состояния приложения (запущено или остановлено, управляется политикой Kaspersky Security Center) и расписания обновлений. Kaspersky Endpoint Security продолжает защищать ваше устройство во время процедуры обновления модулей приложения. В ходе обновления параметры приложения и журнал событий приложения переносятся в новую версию приложения. После обновления нужно перезапустить Kaspersky Endpoint Security.

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

Изменения параметров приложения, сделанные после завершения обновления и до перезапуска приложения, не сохраняются.

После обновления версии приложения с использованием автопатча изменяется механизм взаимодействия с сетевым экраном операционной системы: управление правилами осуществляется с помощью системных утилит iptables и iptables-restore.

Если приложение после обновления работает некорректно, оно автоматически откатывается на предыдущую версию. Рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Об источниках и схемах обновления

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

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, обновление баз на защищенных виртуальных машинах выполняется из директории на SVM.

Основным источником обновлений служат серверы обновлений "Лаборатории Касперского". Вы можете указывать другие источники обновлений в параметрах задачи *Обновление*. Если обновление не может быть выполнено из одного источника обновлений, приложение Kaspersky Endpoint Security переключается к следующему источнику.

Приложение Kaspersky Endpoint Security поддерживает следующие схемы обновления баз и модулей:

- Обновление с серверов обновлений "Лаборатории Касперского". Серверы обновлений "Лаборатории Касперского" расположены в разных странах по всему миру, что обеспечивает высокую надежность обновления. Если обновление не может быть выполнено с одного сервера, приложение переключается к следующему серверу. Обновления загружаются по протоколу HTTPS.

- 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.

     В качестве хранилища вы можете использовать хранилище Сервера администрирования Kaspersky Security Center.

     Загрузку пакета обновлений в хранилище Сервера администрирования обеспечивает задача Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования*.

     Если вы управляете приложением с помощью Kaspersky Security Center Cloud Console, в качестве хранилища вы можете использовать хранилища точек распространения (устройств с установленным Агентом администрирования). Подробнее о точках распространения см. в справке Kaspersky Security Center.

  2. Распространение пакета обновлений на клиентские устройства.

     Распространение пакета обновлений на клиентские устройства обеспечивает задача приложения Kaspersky Endpoint Security *Обновление*. В параметрах задачи вам нужно выбрать в качестве источника обновлений Сервер администрирования Kaspersky Security Center.

- Обновление из локальной или сетевой директории (SMB/NFS), смонтированной пользователем, или с FTP-, HTTP- или HTTPS-сервера. Вы можете указать пользовательский источник обновлений в параметрах задачи *Обновление*.

Обновление баз и модулей приложения в Web Console

Процедура обновления баз и модулей приложения Kaspersky Endpoint Security зависит от режима использования приложения. В этом разделе описана процедура обновления приложения в стандартном режиме. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, обновление баз и модулей приложения с помощью задач, созданных в Kaspersky Security Center, не поддерживается. Обновление выполняется с помощью локальной предустановленной задачи.

В Web Console вы можете выполнять обновление баз и модулей приложения с помощью задачи *Обновление*. Вы можете использовать автоматически созданную групповую задачу *Обновление*, а также создавать пользовательские задачи обновления.

Чтобы настроить параметры обновления в Web Console:

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

   Откроется список задач.

2. Выполните одно из следующих действий:

   - Если вы хотите изменить параметры задачи, которая выполняется на всех устройствах, входящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне группу администрирования.

     В списке отобразятся только задачи, настроенные для выбранной группы администрирования.

   - Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне верхний узел с именем Сервера администрирования.

     В списке отобразятся все задачи, созданные на Сервере администрирования.

3. В списке задач выберите нужную задачу **Обновление** и откройте окно свойств задачи по ссылке в названии задачи.

4. В окне свойств задачи выберите закладку **Параметры приложения**, в списке слева выберите раздел **Источники обновлений**.

5. Выберите источник обновлений, из которого приложение будет получать обновление баз и модулей, в зависимости от используемой схемы обновления.

   Если вы управляете приложением с помощью Web Console, список источников обновлений содержит серверы обновлений "Лаборатории Касперского" и Сервер администрирования Kaspersky Security Center. Если вы управляете приложением с помощью Kaspersky Security Center Cloud Console, список источников обновлений содержит серверы обновлений "Лаборатории Касперского" и точки распространения (подробнее о точках распространения см. в справке Kaspersky Security Center). Вы можете добавлять в список другие источники обновлений.

   Вы можете сформировать список источников обновления, выбрав вариант **Другие источники в локальной или глобальной сети**. В качестве источников обновлений вы можете указывать FTP-, HTTP- или HTTPS-серверы. Если обновление не может быть выполнено из одного источника обновлений, приложение Kaspersky Endpoint Security переключается к следующему источнику. Приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице.

6. Перейдите в раздел **Параметры** и настройте другие параметры обновления.

7. Выберите закладку **Расписание** и настройте расписание запуска задачи обновления.

   Если в качестве источника обновлений вы выбрали **Kaspersky Security Center**, в раскрывающемся списке **Запуск по расписанию** выберите **При загрузке обновлений в хранилище**. Подробнее о расписании задач см. в справке Kaspersky Security Center.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Задача будет запускаться в соответствии с настроенным расписанием. Вы также можете запускать задачу вручную.

Раздел Источники обновлений задачи Обновление

Параметр	Описание
Источники обновлений	В этом блоке вы можете выбрать источник обновлений: • **Серверы обновлений "Лаборатории Касперского"**, на которых публикуются обновления баз для приложений "Лаборатории Касперского" (значение по умолчанию). • **Kaspersky Security Center** – Сервер администрирования Kaspersky Security Center (этот вариант доступен только для Web Console). • **Точки распространения** (этот вариант доступен только для Kaspersky Security Center Cloud Console). • **Другие источники в локальной или глобальной сети** – HTTP-, HTTPS- и FTP-серверы или директории на серверах локальной сети.
Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны	Флажок включает или выключает использование серверов обновлений "Лаборатории Касперского" в качестве источника обновлений, если выбранные источники обновлений недоступны. Флажок доступен, если в блоке **Источники обновлений** выбран вариант **Другие источники в локальной или глобальной сети** или **Kaspersky Security Center**. По умолчанию флажок установлен.
Пользовательские источники обновлений	Таблица содержит список пользовательских источников обновлений баз. В процессе обновления приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице. Таблица содержит следующие столбцы: • **Источник обновлений** – HTTP-, HTTPS- или FTP-серверы или директории на серверах локальной сети. • Переключатель показывает, будет ли источник использоваться в задаче (**Включено** или **Выключено**). Вы можете включить или выключить переключатель в таблице, а также установить или снять флажок **Использовать этот источник** в окне **Источник обновлений**, которое открывается по ссылке с названием источника). Таблица доступна, если выбран вариант **Другие источники в локальной или глобальной сети**. По умолчанию таблица пустая. Источники обновлений в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

	При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице. Кнопка доступна, если в таблице выбран только один элемент.
	При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице. Кнопка доступна, если в таблице выбран только один элемент.
	При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент.
	Изменение параметров выбранного элемента выполняется в отдельном окне.
	При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Раздел Параметры задачи Обновление

Параметр	Описание
Максимальное время ожидания ответа от источника обновлений (сек.)	Предельный период ожидания ответа на запрос приложения от выбранного источника обновлений (в секундах). При отсутствии ответа по истечении этого времени в журнал выполнения задач записывается событие о нарушении связи с источником обновлений. Доступные значения: 0–120. Если указано значение 0, период ожидания ответа на запрос приложения от выбранного источника не ограничен. Значение по умолчанию: 10 секунд.
Режим загрузки обновлений приложения	В раскрывающемся списке вы можете выбрать режим загрузки обновлений приложения: • **Не загружать** обновления. При выборе этого элемента списка обновить приложение невозможно. • **Только загружать** обновления, но не устанавливать их на клиентские устройства (значение по умолчанию). • **Загружать и устанавливать** обновления на клиентские устройства. После установки обновлений приложение будет автоматически перезапущено. Эта функциональность не поддерживается в KESL-контейнере.

Обновление баз и модулей приложения в Консоли администрирования

Процедура обновления баз и модулей приложения Kaspersky Endpoint Security зависит от режима использования приложения. В этом разделе описана процедура обновления приложения в стандартном режиме. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, обновление баз и модулей приложения с помощью задач, созданных в Kaspersky Security Center, не поддерживается. Обновление выполняется с помощью локальной предустановленной задачи.

В Консоли администрирования вы можете выполнять обновление баз и модулей приложения с помощью задачи *Обновление*. Вы можете использовать автоматически созданную групповую задачу *Обновление*, а также создавать пользовательские задачи обновления.

Чтобы настроить параметры обновления в Консоли администрирования:

1. В Консоли администрирования выполните одно из следующих действий:

   - Если вы хотите изменить параметры задачи, которая выполняется на устройствах, входящих в определенную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите закладку **Задачи**.

   - Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), в дереве консоли выберите папку **Задачи**.

2. В списке задач выберите нужную задачу **Обновление** и откройте окно свойств задачи двойным щелчком мыши.

3. В окне свойств задачи в списке слева выберите раздел **Источники обновлений.**

4. Выберите источник обновлений, из которого приложение будет получать обновление баз и модулей, в зависимости от используемой схемы обновления.

   Список источников обновлений содержит серверы обновлений "Лаборатории Касперского" и Сервер администрирования Kaspersky Security Center. Вы можете добавлять в список другие источники обновлений.

   Вы можете сформировать список источников обновления, выбрав вариант **Другие источники в локальной или глобальной сети**. В качестве источников обновлений вы можете указывать FTP-, HTTP- или HTTPS-серверы. Если обновление не может быть выполнено с одного источника обновлений, приложение Kaspersky Endpoint Security переключается к следующему источнику. Приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице.

5. Выберите раздел **Параметры** и настройте другие параметры обновления.

6. Выберите раздел **Расписание** и настройте расписание запуска задачи обновления.

   Если в качестве источника обновлений вы выбрали **Kaspersky Security Center**, в раскрывающемся списке **Запуск по расписанию** выберите **При загрузке обновлений в хранилище**. Подробнее о расписании задач см. в справке Kaspersky Security Center.

7. Нажмите на кнопку **Применить** или на кнопку **OK** в окне **Свойства: <Название задачи>**, чтобы сохранить внесенные изменения.

Задача будет запускаться в соответствии с настроенным расписанием. Вы также можете запускать задачу вручную.

Параметр	Описание
Источники обновлений	В этом блоке вы можете выбрать источник обновлений: • **Серверы обновлений "Лаборатории Касперского"**, на которых публикуются обновления баз для приложений "Лаборатории Касперского" (значение по умолчанию). • **Kaspersky Security Center** – Сервер администрирования Kaspersky Security Center. • **Другие источники в локальной или глобальной сети** – HTTP-, HTTPS- и FTP-серверы или директории на серверах локальной сети.
Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны	Флажок включает или выключает использование серверов обновлений "Лаборатории Касперского" в качестве источника обновлений, если выбранные источники обновлений недоступны. Флажок доступен, если в блоке **Источники обновлений** выбран вариант **Другие источники в локальной или глобальной сети** или **Kaspersky Security Center**. По умолчанию флажок установлен.
Пользовательские источники обновлений	Таблица содержит список пользовательских источников обновлений баз. В процессе обновления приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице. Таблица содержит следующие столбцы: • **Адрес источника** – HTTP-, HTTPS- или FTP-серверы или директории на серверах локальной сети. • **Статус** показывает, используется ли источник в задаче (**Используется** или **Не используется**). Вы можете изменить статус, установив или сняв флажок **Использовать этот источник** в окне **Источник обновлений**, которое открывается при нажатии на кнопку **Изменить**. Таблица доступна, если выбран вариант **Другие источники в локальной или глобальной сети**. Источники обновлений в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз. При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице. Кнопка доступна, если в таблице выбран только один элемент. При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице. Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

По умолчанию таблица пустая.

Раздел Параметры задачи Обновление

Параметр	Описание
Максимальное время ожидания ответа от источника обновлений (сек.)	Предельный период ожидания ответа на запрос приложения от выбранного источника обновлений (в секундах). При отсутствии ответа по истечении этого времени в журнал выполнения задач записывается событие о нарушении связи с источником обновлений. Доступные значения: 0–120. Если указано значение 0, период ожидания ответа на запрос приложения от выбранного источника не ограничен. Значение по умолчанию: 10 секунд.
Режим загрузки обновлений	В раскрывающемся списке вы можете выбрать режим загрузки обновлений приложения: • **Не загружать** обновления. При выборе этого элемента списка обновить приложение невозможно. • **Только загружать** обновления, но не устанавливать их на клиентские устройства (значение по умолчанию). • **Загружать и устанавливать** обновления на клиентские устройства. После установки обновлений приложение будет автоматически перезапущено. Эта функциональность не поддерживается в KESL-контейнере.

Обновление баз и модулей приложения в командной строке

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, обновление баз на защищенных виртуальных машинах выполняется с помощью специальной локальной задачи *Обновление*, в которой в качестве источника обновлений указана директория на SVM. Задача обновления запускается автоматически. Вы не можете удалять эту задачу и изменять ее параметры.

В командной строке вы можете выполнять обновление баз и модулей приложения следующими способами:

- С помощью предустановленной задачи Обновление (*Update*). Вы можете запускать, останавливать, приостанавливать и возобновлять эту задачу вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.

- С помощью пользовательских задач обновления (задач типа *Update*). Вы можете запускать пользовательские задачи вручную и настраивать расписание запуска задач.

Параметры задачи Обновление

Параметр	Описание	Значения
`SourceType`	Источник, из которого приложение будет получать обновления.	`KLServers` (значение по у приложение получает обн одного из серверов обнов "Лаборатории Касперског Обновления загружаются HTTPS. `SCServer` – приложение з обновления на защищаем устройство с установленн локальной сети Сервера администрирования. Вы м выбрать этот источник об если вы используете Kasp Center для централизован управления защитой устр организации. `Custom` – приложение заг обновления из пользовате источника, указанного в се `[CustomSources.item_#` указывать директории FTP HTTPS-серверов или дире любом смонтированном у защищаемого клиентского включая директории на уд устройствах, смонтирова протоколам Samba или NF
`UseKLServersWhenUnavailable`	Обращение приложения к серверам обновлений "Лаборатории Касперского" в случае, если все пользовательские источники недоступны.	`Yes` (значение по умолчан приложение подключаетс обновлений "Лаборатории Касперского", если все пользовательские источни обновлений недоступны. `No` – приложение не подкл серверам обновлений "Ла Касперского", если все пользовательские источни обновлений недоступны.
`ApplicationUpdateMode`	Режим загрузки и установки обновлений приложения.	`Disabled` – не загружать устанавливать обновлени `DownloadOnly` (значение умолчанию) – загружать о приложения, но не устана

		`DownloadAndInstall` – а загружать и устанавливат приложения. После устан обновлений приложение б автоматически перезапуш
`ConnectionTimeout`	Время ожидания (в секундах) ответа от источника обновлений при попытке соединения с ним. Если в течение указанного промежутка времени от источника обновлений не приходит ответ, приложение обращается к другому указанному источнику обновлений.	Вы можете указывать толь числа в диапазоне от 0 до Значение по умолчанию: 1
Секция **[CustomSources.item_#]** содержит следующие параметры:		
`URL`	Адрес пользовательского источника обновлений в локальной сети или в интернете.	Значение по умолчанию н Примеры: `URL=http://example.` – адрес HTTP-сервера, расположена директори обновлениями. `URL=/home/bases/` – д на защищаемом устрой которой содержатся ба приложения.
`Enabled`	Использование источника обновлений, указанного в параметре `URL`. Для выполнения задачи требуется включить использование хотя бы одного источника обновлений.	`Yes` – приложение исполь обновлений. `No` – приложение не испо источник обновлений. Значение по умолчанию н

Обновление с помощью Kaspersky Update Utility

Для экономии интернет-трафика вы можете настроить обновление баз и модулей приложения на устройствах локальной сети организации из общей директории с помощью утилиты Kaspersky Update Utility. Для этого одно из устройств локальной сети организации должно получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или с серверов обновлений "Лаборатории Касперского" и копировать полученные пакеты обновлений в общую директорию с помощью утилиты. Остальные устройства локальной сети организации смогут получать пакет обновлений из общей директории.

Чтобы настроить обновление баз из общей директории с помощью утилиты Kaspersky Update Utility:

1. Установите Kaspersky Update Utility на одном из устройств локальной сети организации.

   Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта службы технической поддержки "Лаборатории Касперского".

2. Настройте копирование пакета обновлений в общую директорию в параметрах Kaspersky Update Utility.

   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".

3. Настройте обновления баз и модулей приложения из указанной общей директории на остальных устройствах локальной сети организации.

   a. Откройте свойства задачи **Обновление**, которая будет выполняться на нужном устройстве, с помощью Web Console или с помощью Консоли администрирования.

   b. В свойствах задачи перейдите в раздел **Источники обновлений**.

   c. В блоке **Источники обновлений** выберите вариант **Другие источники в локальной или глобальной сети**.

4. В таблице источников обновлений нажмите на кнопку **Добавить** и укажите путь к общей директории.

   Адрес источника должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.

5. Установите флажок **Использовать этот источник** и нажмите на кнопку **ОК**.

6. В таблице источников обновлений настройте порядок их использования с помощью кнопок **Вверх** и **Вниз**.

7. Сохраните изменения параметров задачи.

Откат обновления баз и модулей приложения

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, откат обновления баз с помощью задачи не поддерживается.

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

Каждый раз, когда пользователь запускает процесс обновления, приложение Kaspersky Endpoint Security создает резервную копию текущих баз приложения. Это позволяет откатить базы до предыдущей версии, если требуется.

Откат последнего обновления баз используется, например, если новая версия баз приложения содержит недопустимые сигнатуры, что приводит к блокировке безопасных приложений приложением Kaspersky Endpoint Security.

В командной строке для отката обновлений вы можете запускать предустановленную задачу *Откат обновления баз (Rollback)* или создавать и запускать пользовательские задачи отката обновления (задачи типа *Rollback*).

В Kaspersky Security Center вы можете создавать задачи отката обновления для групп администрирования или отдельных устройств с помощью Web Console или Консоли администрирования.

Задача *Откат обновления баз* не имеет параметров.

Защита от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы устройства. Компонент включается автоматически с параметрами по умолчанию при запуске приложения Kaspersky Endpoint Security, постоянно находится в оперативной памяти устройства и проверяет все открываемые, сохраняемые и запускаемые файлы в режиме реального времени.

При обнаружении вредоносного ПО приложение Kaspersky Endpoint Security может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

На работу компонента влияет режим перехвата файловых операций, который вы можете выбрать в общих параметрах приложения. По умолчанию на время проверки доступ к файлу блокируется.

Если включена защита от файловых угроз и включен Мониторинг контейнеров, приложение также проверяет все пространства имен и контейнеры во всех поддерживаемых операционных системах.

Вы можете включать и выключать защиту от файловых угроз, а также настраивать параметры защиты:

- Выбирать режим проверки файлов (при открытии, при открытии и изменении).
- Включать и выключать проверку архивов, почтовых баз, сообщений электронной почты в текстовом формате.
- Временно исключать из повторной проверки файлы в текстовом формате.
- Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
- Выбирать действия, которые приложение будет выполнять над зараженными объектами.
- Настраивать области проверки. Приложение будет проверять объекты в указанной области файловой системы.
- Настраивать исключения объектов из проверки. *Исключение из проверки* – это совокупность условий, при выполнении которых приложение не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете исключать из проверки:
  - объекты по именам или маскам;
  - объекты по названиям обнаруженных в объектах угроз;
  - файлы и директории в указанных областях файловой системы;
  - процесс и файлы, изменяемые указанным процессом.
- Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
- Включать и выключать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.

Для оптимизации работы компонента Защита от файловых угроз вы можете настроить исключение из проверки файлов, копируемых из сетевых директорий. Файлы будут проверяться только после завершения копирования в локальную директорию. Для исключения из проверки файлов в сетевых директориях вам нужно настроить исключение по процессам для утилиты, предназначенной для копирования из сетевых директорий (например, для утилиты `cp`). Если вы управляете приложением с помощью Kaspersky Security Center, вы можете настроить исключение по процессам в Web Console или в Консоли администрирования. Если вы управляете приложением с помощью командной строки, вы можете настроить исключение по процессам, добавив в параметры задачи типа OAS секцию `[ExcludedForProgram.item_#]`.

Настройка защиты от файловых угроз в Web Console

В Web Console вы можете управлять защитой от файловых угроз в свойствах политики (**Параметры приложения** → **Базовая защита** → **Защита от файловых угроз**).

Параметры компонента Защита от файловых угроз

Параметр	Описание
Защита от файловых угроз включена / выключена	Переключатель включает или выключает компонент Защита от файловых угроз на всех управляемых устройствах. По умолчанию переключатель включен.
Режим Защиты от файловых угроз	В раскрывающемся списке вы можете выбрать режим работы компонента Защита от файловых угроз: • **Интеллектуальный режим** (значение по умолчанию) – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс в течение определенного времени многократно обращается к файлу и изменяет его, приложение повторно проверяет файл только при последнем закрытии файла этим процессом. • **При открытии** – проверять файл при попытке открытия на чтение, исполнение или изменение. • **При открытии и изменении** – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Блокировать** доступ к объекту.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое

	действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Блокировать** доступ к объекту (значение по умолчанию).
Области проверки	По ссылке **Настроить области проверки** открывается окно **Области защиты**.
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, включив и настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)**. Если флажок снят, приложение 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, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение 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 приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение 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, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать текстовые файлы	Временное исключение из проверки файлов в текстовом формате.

	Если флажок установлен, приложение не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов работы приложений. Если флажок снят, приложение проверяет текстовые файлы. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: `0`–`9999`. Если указано значение `0`, время проверки не ограничено. Значение по умолчанию: `60`.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: `0`–`999999`. Если установлено значение `0`, приложение проверяет файлы любого размера. Значение по умолчанию: `0`.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал события *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал событие *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает событие в журнал. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал события *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал событие *ObjectNotProcessed*. Если флажок снят, приложение не записывает событие в журнал. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал события *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал событие *PackedObjectDetected*. Если флажок снят, приложение не записывает событие в журнал. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение 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	Если флажок **Использовать эвристический анализ** установлен, вы

анализа	можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых серверов.

Окно Области защиты

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область защиты, включающую все директории локальной файловой системы.

Параметры области защиты

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно добавления области защиты

В этом окне вы можете добавить или настроить область защиты.

Параметры области защиты

Параметр	Описание
Название области	Поле ввода названия области защиты. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область защиты во время работы. Если флажок снят, приложение не обрабатывает эту область защиты во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.

Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите включить в область защиты. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • `[container-id:<идентификатор>]/<путь к локальной директории>` • `[container-name:<название>]/<путь к локальной директории>` • `[image-id:<идентификатор>]/<путь к локальной директории>` • `[image-name:<название>]/<путь к локальной директории>` Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. Например: • `[container-name:<название>][image-name:<название>]/<путь к локальной директории>` • `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>` • `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>` • `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>` • `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>` В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file*/` или `/dir/file**/`. Маску ** можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область защиты. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Исключения Защиты от файловых угроз

Исключение из защиты – это совокупность условий, при выполнении которых приложение Kaspersky Endpoint Security не проверяет объекты на наличие вирусов и других вредоносных программ. Вы также можете исключать из защиты объекты по маскам и названиям угроз и настраивать исключения для процессов.

В Web Console вы можете настроить исключения Защиты от файловых угроз в свойствах политики (**Параметры приложения** → **Базовая защита** → **Исключения Защиты от файловых угроз**).

Параметры исключений из защиты

Параметр	Описание
Области исключения	По ссылке **Настроить области исключения** открывается окно **Области исключения**. В этом окне вы можете задать список исключений из защиты.
Исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	По ссылке **Настроить исключения по названию угрозы** открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Исключения по процессам	По ссылке **Настроить исключения по процессам** открывается окно **Исключения по процессам**. В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки или защиты во время своей работы. Если флажок снят, приложение включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные директории. • **Смонтированная** – удаленные директории, смонтированные на устройстве. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле **Путь**. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска. При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки.

Кнопка доступна, если в списке выбрана хотя бы одна маска.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную угрозу из списка исключений.

Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса и файлов, изменяемых указанным процессом, из проверки. По умолчанию таблица содержит две области исключения, содержащие пути к Агентам администрирования. Вы можете удалить эти исключения, если требуется.

Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Параметры области исключения

Параметр	Описание
Название области исключения по процессам	Поле ввода названия области исключения по процессам. Это название будет отображаться в таблице окна **Исключения по процессам**. Поле ввода не должно быть пустым.
Использовать	Переключатель включает или выключает исключение этой области во время работы

/ Не использовать это исключение	приложения. По умолчанию переключатель включен.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром **Путь к исключаемому процессу**. По умолчанию флажок снят.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать исключения из проверки для файлов, которые изменяет процесс. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список **Протокол доступа** доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.
Путь	В поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски.

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в блоке **Файловая система, протокол доступа и путь**. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска. При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Настройка защиты от файловых угроз в Консоли администрирования

В Консоли администрирования вы можете управлять защитой от файловых угроз в свойствах политики (**Базовая защита → Защита от файловых угроз**).

Параметры компонента Защита от файловых угроз

Параметр	Описание
Включить Защиту от файловых угроз	Флажок включает или выключает компонент Защита от файловых угроз на всех управляемых устройствах. По умолчанию флажок установлен.
Режим Защиты от файловых угроз	В раскрывающемся списке вы можете выбрать режим работы компонента Защита от файловых угроз: • **Интеллектуальный режим** (значение по умолчанию) – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс в течение определенного времени многократно обращается к файлу и изменяет его, приложение повторно проверяет файл только при последнем закрытии файла этим процессом. • **При открытии** – проверять файл при попытке открытия на чтение, исполнение или изменение. • **При открытии и изменении** – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки и параметры проверки.
Действие при обнаружении угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действие при обнаружении угрозы**, в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки.

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file*/` или `/dir/file**/`. Маску ** можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы Защиты от файловых угроз.

Параметры Защиты от файловых угроз

Параметр	Описание

Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, Kaspersky Endpoint Security проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, включив и настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, Kaspersky Endpoint Security не проверяет архивы. По умолчанию флажок снят.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, Kaspersky Endpoint Security проверяет самораспаковывающиеся архивы. Если флажок снят, Kaspersky Endpoint Security не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок снят.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений 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.
Пропускать текстовые файлы	Временное исключение из проверки файлов в текстовом формате. Если флажок установлен, Kaspersky Endpoint Security не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов работы приложений. Если флажок снят, Kaspersky Endpoint Security проверяет текстовые файлы. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени Kaspersky Endpoint Security прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 60.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах.

	Доступные значения: 0–999999. Если установлено значение 0, Kaspersky Endpoint Security проверяет файлы 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*. 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 файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он

	обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действие при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Параметры Защиты от файловых угроз

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Блокировать** доступ к объекту.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Блокировать** доступ к объекту (значение по умолчанию).

Исключения Защиты от файловых угроз

Исключение из защиты – это совокупность условий, при выполнении которых приложение Kaspersky Endpoint Security не проверяет объекты на наличие вирусов и других вредоносных программ. Вы также можете исключать из защиты объекты по маскам и названиям угроз и настраивать исключения для процессов.

В Консоли администрирования вы можете настроить исключения Защиты от файловых угроз в свойствах политики (**Базовая защита** → **Исключения Защиты от файловых угроз**).

Параметры исключений из проверки

Блок параметров	Описание
Исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключения из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Исключения по процессам	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по процессам**. В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска. При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки.

Кнопка доступна, если в списке выбрана хотя бы одна маска.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную угрозу из списка исключений.

Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса и файлов, изменяемых указанным процессом, из проверки. По умолчанию таблица содержит две области исключения, содержащие пути к Агентам администрирования. Вы можете удалить эти исключения, если требуется.

Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно → Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно → Экспортировать выбранное** или **Дополнительно → Экспортировать все**.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Исключения по процессам**.

	Поле ввода не должно быть пустым.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром **Путь к исключаемому процессу**. По умолчанию флажок снят.
Использовать эту область	Флажок включает или выключает исключение этой области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Путь к изменяемым файлам	Блок параметров позволяет задать исключения из проверки для файлов, которые изменяет процесс. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная** или **Общая**, то в раскрывающемся списке протоколов доступа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски. Поле ввода не должно быть пустым.

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в блоке **Путь к изменяемым файлам**. Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска. При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Настройка защиты от файловых угроз в командной строке

В командной строке вы можете управлять защитой от файловых угроз с помощью предустановленной задачи Защита от файловых угроз (*File_Threat_Protection*).

Задача Защита от файловых угроз запущена по умолчанию. Вы можете запускать и останавливать эту задачу вручную.

Для запуска и остановки задачи Защита от файловых угроз из командной строки требуются права роли Администратор.

Вы можете настраивать параметры защиты от файловых угроз, изменяя параметры предустановленной задачи Защита от файловых угроз.

Параметры задачи Защита от файловых угроз

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

Параметры задачи Защита от файловых угроз

Параметр	Описание	Значения
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	`Yes` – проверять архивы. Если указано значение `FirstAction=Recommended`, т в зависимости от типа архива приложени удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` (значение по умолчанию) – не проверять архивы.
`ScanSfxArchived`	Включение проверки только	`Yes` – проверять

	самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	самораспаковывающиеся архивы. `No` (значение по умолчанию) – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook®, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронно почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почт в текстовом формате.
`SkipPlainTextFiles`	Временное исключение из проверки файлов в текстовом формате. Если значение этого параметра `SkipPlainTextFiles=Yes`, приложение не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов работы приложений.	`Yes` – не проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. `No` (значение по умолчанию) – проверят файлы в текстовом формате.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 60.
`FirstAction`	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	`Disinfect` (лечить) – приложение пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, ти объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано `Disinfect`,

		рекомендуется задать второе действие в параметре `SecondAction`. `Remove` (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. `Recommended` (выполнять рекомендуемое действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские приложения, так как они не заражают другие файлы и поэтому не предполагают лечения. `Block` (блокировать) – приложение блокирует доступ к зараженному объекту. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `Recommended`.
`SecondAction`	Выбор второго действия, которое приложение будет выполнять над зараженными объектами. Приложение 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, приложение в качестве второго действия выполняет `Block` (блокировать). Значение по умолчанию: `Block`.
`UseExcludeMasks`	Включение исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

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

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

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		
		Значение по умолчанию не задано.
		
		Пример:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора.	`Yes` (значение по умолчанию) – включит эвристический анализатор.

	Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) - рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включит использование технологии iChecker. `No` – выключить использование технологии iChecker.
`ScanByAccessType`	Режим работы задачи Защита от файловых угроз. Этот параметр `ScanByAccessType` применяется только в задаче Защита от файловых угроз.	`SmartCheck` (значение по умолчанию) – проверять файл при попытке открытия, и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс во время своей работы многократно обращается к файлу в течение некоторого времени и изменяет его, повторно проверять файл только при последней попытке закрытия файла этим процессом. `OpenAndModify` – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. `Open` – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: `All objects`. Пример: `AreaDesc="Проверка почтовых баз"`
`UseScanArea`	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	`Yes` (значение по умолчанию) – проверя указанную область. `No` – не проверять указанную область.

`AreaMask.item_#`	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять вс объекты). Пример: `AreaMask_item_<номер элемента>=*doc`
`Path`	Путь к директории с проверяемыми объектами.	`<путь к локальной директории>` – проверять объекты в указанной директории. Для указания пути вы может использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:`

<название>]/<путь к локальной директории>

- [container-name:<название>] [image-id:<идентификатор>] [container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>

В названиях и идентификаторах можно использовать маски (символы ? и *).

Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

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

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

Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

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

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

Mounted:NFS – проверять удаленные директории, смонтированные на устройстве по протоколу NFS.

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

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:`

<название>]/<путь к локальной директории>

- [container-name:<название>] [image-id:<идентификатор>] [container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>

В названиях и идентификаторах можно использовать маски (символы ? и *).

Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

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

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

Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

Mounted:NFS – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS.

Mounted:SMB – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba.

AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS.

		<тип файловой системы> – исключать и проверки все ресурсы указанной файловой системы устройства.
Секция **[ExcludedForProgram.item_#]** содержит следующие параметры:		
ProgramPath	Путь к исключаемому процессу.	< полный путь к процессу > – исключать из проверки процесс в указанной локальной директории.
ApplyToDescendants	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром ProgramPath.	Yes – исключать из проверки указанный процесс и все его дочерние процессы. No (значение по умолчанию) – исключат из проверки только указанный процесс, и исключать из проверки дочерние процессы.
AreaDesc	Описание области исключения процессов.	Значение по умолчанию: All objects.
UseExcludedForProgram	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключа указанную область. No – не исключать указанную область.
AreaMask.item_#	Ограничение области исключения процессов. В области исключения процессов приложение не проверяет только файлы, указанные помощью масок в формате shell. Если параметр не указан, приложение исключает из проверки все объекты в области исключения процессов. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (исключать из проверки все объекты).
Path	Путь к директории с файлами, которые изменяет процесс.	< путь к локальной директории > – исключать из проверки объекты в указанной директории. Для указания пут можно использовать маски.

Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

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

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

Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

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

Shared:SMB – исключать из проверки ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba.

Mounted:NFS – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS.

Mounted:SMB – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba.

AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS.

AllShared – исключать из проверки все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS.

< тип файловой системы > – исключать из проверки все ресурсы указанной файловой системы устройства.

Оптимизация проверки сетевых директорий

Для оптимизации защиты от файловых угроз вы можете настроить исключение из проверки файлов, копируемых из сетевых директорий в локальную директорию. Для этого вам нужно настроить исключение по процессам для утилиты, предназначенной для копирования из сетевых директорий (например, для утилиты `cp`).

Чтобы настроить исключение сетевых директорий из проверки:

1. Выведите параметры задачи Защита от файловых угроз (*File_Threat_Protection*, ID:1) в конфигурационный файл с помощью команды:

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

2. Откройте конфигурационный файл и добавьте секцию `[ExcludedForProgram.item_#]` со следующими параметрами:

   - `ProgramPath` – путь к исключаемому процессу или к директории с исключаемыми процессам.
   - `ApplyToDescendants` – параметр, показывающий, нужно ли исключать из проверки дочерние процессы исключаемого процесса (возможные значения: `Yes` или `No`).
   - `AreaDesc` – описание области исключения по процессам, содержащее дополнительную информацию об области исключения.
   - `UseExcludedForProgram` – включить исключение указанной области при работе задачи (возможные значения: `Yes` или `No`).
   - `Path` – путь к файлам или к директории с файлами, которые изменяет процесс.
   - `AreaMask.item_#` – маска имени файла для файлов, которые вы хотите исключить из проверки. Вы также можете указать полный путь к файлу.

     Пример:

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

3. Выполните команду:

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

   Укажите ключ `--json`, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

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

Особенности проверки символических и жестких ссылок

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

Проверка символических ссылок

Приложение проверяет символические ссылки, только если файл, на который ссылается символическая ссылка, входит в область проверки компонента Защита от файловых угроз.

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

Проверка жестких ссылок

При обработке файла, имеющего больше одной жесткой ссылки, приложение выбирает действие в зависимости от заданного действия над объектами:

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

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

Поиск вредоносного ПО

Поиск вредоносного ПО – это однократная полная или выборочная проверка файлов на устройстве по требованию. Приложение Kaspersky Endpoint Security может выполнять несколько задач поиска вредоносного ПО одновременно.

В приложении создается предустановленная задача *Поиск вредоносного ПО (Scan_My_Computer)*. Вы можете использовать эту задачу для выполнения полной проверки устройства. При полной проверке приложение проверяет все объекты, расположенные на локальных дисках устройства, а также все смонтированные и общие объекты, доступ к которым предоставляется по протоколам Samba и NFS, с рекомендуемыми параметрами безопасности.

В Kaspersky Security Center мастер первоначальной настройки Kaspersky Security Center автоматически создает групповую задачу поиска вредоносного ПО после установки mmc-плагина управления или веб-плагина управления Kaspersky Endpoint Security.

Во время полной проверки диска процессор будет занят. Рекомендуется запускать задачу полной проверки в нерабочее время.

Вы можете настраивать параметры автоматически созданных задач в Kaspersky Security Center и в командной строке, а также создавать пользовательские задачи поиска вредоносного ПО.

При обнаружении вредоносного ПО приложение Kaspersky Endpoint Security может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

Если во время поиска вредоносного ПО приложение было перезапущено контрольной службой или вручную пользователем, выполнение задачи прерывается. В журнале приложения сохраняется событие *OnDemandTaskInterrupted*.

Вы можете запускать задачи поиска вредоносного ПО и настраивать параметры проверки:

- Выбирать объекты операционной системы, которые нужно проверять: файлы, архивы, загрузочные секторы, память процессов и память ядра, объекты автозапуска.
- Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
- Выбирать действия, которые приложение будет выполнять над зараженными объектами.
- Настраивать исключения объектов из проверки:
  - по именам или маскам;
  - по названиям обнаруженных в объектах угроз.
- Включать и выключать использование глобальных исключений и исключений Защиты от файловых угроз при проверке.
- Включать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.
- Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
- Ограничивать набор устройств, загрузочные секторы которых нужно проверять.
- Настраивать области проверки и области исключения из проверки.

Поиск вредоносного ПО в Web Console

В Web Console вы можете выполнять проверку на наличие вредоносного ПО с помощью задачи *Поиск вредоносного ПО*.

Вы можете запускать автоматически созданную групповую задачу, а также создавать и запускать пользовательские задачи проверки. Вы можете настраивать параметры проверки, изменяя параметры задач поиска вредоносного ПО.

Параметры проверки задачи Поиск вредоносного ПО

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение 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 приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение 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, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено.

	Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение 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, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение 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, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение 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, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему.

	• **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).
Области проверки	Таблица, содержащая области, проверяемые задачей. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы. Области проверки в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз. При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице. Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую. Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

При нажатии на название области проверки открывается окно **<Название области проверки>**. В этом окне вы можете изменить параметры выбранной области проверки.

При нажатии на кнопку **Добавить** открывается окно **<Новая область проверки>**. В этом окне вы можете задать новую область проверки.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области	Поле ввода названия области проверки. Это название будет отображаться в таблице **Области проверки** в разделе **Параметры проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол	В раскрывающемся списке вы можете выбрать тип файловой системы:

доступа и путь	• **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file*/` или `/dir/file**/`. Маску ** можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Раздел Области проверки

Вы можете настроить параметры области проверки для задачи Поиск вредоносного ПО. Приложение позволяет проверять файлы, загрузочные секторы, память клиентского устройства и объекты автозапуска.

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, приложение проверяет файлы. Если флажок снят, приложение не проверяет файлы. По умолчанию флажок установлен.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, приложение проверяет загрузочные секторы. Если флажок снят, приложение не проверяет загрузочные секторы. По умолчанию флажок снят.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти клиентского устройства. Если флажок установлен, приложение проверяет память ядра и запущенные процессы. Если флажок снят, приложение не проверяет память ядра и запущенные процессы. По умолчанию флажок снят.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, приложение проверяет объекты автозапуска. Если флажок снят, приложение не проверяет объекты автозапуска. По умолчанию флажок снят.
Устройства для проверки	По ссылке **Настроить маски устройств** открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Раздел Области исключения

В разделе **Области исключения** для задачи Поиск вредоносного ПО вы можете настроить области исключения, исключения по маске и по названию угрозы, а также использование глобальных исключений и исключений Защиты от файловых угроз во время работы задачи.

Параметры исключений из проверки

Параметр	Описание
Настроить области исключения	По ссылке **Настроить области исключения** открывается окно **Области исключения**. В этом окне вы можете задать список исключений из проверки.
Настроить исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Настроить исключения по названию угрозы	По ссылке **Настроить исключения по названию угрозы** открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки или защиты во время своей работы. Если флажок снят, приложение включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные директории. • **Смонтированная** – удаленные директории, смонтированные на устройстве. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле **Путь**. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска. При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки.

Кнопка доступна, если в списке выбрана хотя бы одна маска.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную угрозу из списка исключений.

Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Поиск вредоносного ПО в Консоли администрирования

В Консоли администрирования вы можете выполнять проверку на наличие вредоносного ПО с помощью задачи *Поиск вредоносного ПО*.

Вы можете запускать автоматически созданную групповую задачу, а также создавать и запускать пользовательские задачи проверки. Вы можете настраивать параметры проверки, изменяя параметры задач поиска вредоносного ПО.

В разделе **Параметры** в свойствах задачи Поиск вредоносного ПО вы можете настроить параметры, приведенные в таблице ниже.

Параметры задачи Поиск вредоносного ПО

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки, параметры области проверки и параметры проверки.
Действие при обнаружении угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действие при обнаружении угрозы**, в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В разделе **Исключения** в свойствах задачи Поиск вредоносного ПО вы можете настроить области исключения, исключения по маске и по названию угрозы.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Параметры области проверки

Параметр	Описание
Название области	Название области проверки.

Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения.

	Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file*/` или `/dir/file**/`. Маску ** можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Параметры области проверки

В этом окне вы можете настроить параметры проверки во время работы задачи Поиск вредоносного ПО. Приложение позволяет проверять файлы, загрузочные секторы, память устройства и объекты автозапуска.

Параметры области проверки

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, приложение проверяет файлы. Если флажок снят, приложение не проверяет файлы. По умолчанию флажок установлен.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, приложение проверяет загрузочные секторы. Если флажок снят, приложение не проверяет загрузочные секторы. По умолчанию флажок снят.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти устройства. Если флажок установлен, приложение проверяет память ядра и запущенные процессы. Если флажок снят, приложение не проверяет ядра и запущенные процессы. По умолчанию флажок снят.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, приложение проверяет объекты автозапуска. Если флажок снят, приложение не проверяет объекты автозапуска. По умолчанию флажок снят.
Устройства для проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение 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 приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение 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, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла.

	Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение 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, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение 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, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение 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, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему.

	• **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действие при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Действия при обнаружении угрозы

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).

Раздел Исключения

Исключение из проверки – это совокупность условий, при выполнении которых приложение Kaspersky Endpoint Security не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете также исключать объекты из проверки по маскам и названиям угроз.

Параметры исключений из проверки

Блок параметров	Описание

Области исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**.

	Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска. При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки.

Кнопка доступна, если в списке выбрана хотя бы одна маска.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную угрозу из списка исключений.

Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Поиск вредоносного ПО в командной строке

В командной строке вы можете выполнять проверку на наличие вредоносного ПО следующими способами:

- С помощью предустановленной задачи Поиск вредоносного ПО (*Scan_My_Computer*). Вы можете запускать, останавливать, приостанавливать и возобновлять эту задачу вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.
- С помощью пользовательских задач поиска вредоносного ПО (задач типа *ODS*). Вы можете запускать, останавливать, приостанавливать и возобновлять пользовательские задачи вручную и настраивать расписание запуска задач.
- С помощью команды `kesl-control --scan-file` вы можете выполнять *выборочную проверку* указанных файлов и директорий.

Параметры предустановленной задачи Поиск вредоносного ПО

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

Параметры задачи Поиск вредоносного ПО

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

		`No` – не проверять память процессов и память ядра.
`ScanStartupObjects`	Включение проверки объектов автозапуска.	`Yes` (значение по умолчанию) – проверя объекты автозапуска. `No` – не проверять объекты автозапуска.
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	`Yes` (значение по умолчанию) – проверя архивы. Если указано значение `FirstAction=Recommended`, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (значение по умолчанию) – проверя самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронно почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почт в текстовом формате.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
`FirstAction`	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	`Disinfect` (лечить) – приложение пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, ти объекта или тип угрозы в объекте не

		предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано `Disinfect`, рекомендуется задать второе действие в параметре `SecondAction`. `Remove` (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. `Recommended` (выполнять рекомендуемое действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские приложения, так как они не заражают другие файлы и поэтому не предполагают лечения. `Skip` (пропускать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `Recommended`.
`SecondAction`	Выбор второго действия, которое приложение будет выполнять над зараженными объектами. Приложение выполняет второе действие, если не удалось выполнить первое действие.	Значения параметра `SecondAction` такие же, как значения параметра `FirstActio` 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, приложение в качестве второго действи выполняет `Skip` (пропускать). Значение по умолчанию: `Skip`.
`UseExcludeMasks`	Включение исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

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

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

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.
`UseOASExclusions`	Включение использования исключений Защиты от файловых угроз при проверке.	`Yes` (значение по умолчанию) – использовать исключения Защиты от файловых угроз. `No` – не использовать исключения Защит от файловых угроз.
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.

`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включит эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) - рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включит использование технологии iChecker. `No` – выключить использование технологии iChecker.
`DeviceNameMasks.item_#`	Список названий устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску названия устройства.	`AllObjects` – проверять загрузочные секторы всех устройств. `<маска названия устройства>` – проверять загрузочные секторы устройств, названия которых содержат указанную маску. Значение по умолчанию: `/**` – любой набор символов в названии устройства, включая символ `/`.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области проверки,	Значение по умолчанию: `All objects`.

	содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Пример: `AreaDesc="Mail bases scan"`
`UseScanArea`	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	`Yes` (значение по умолчанию) – проверя указанную область. `No` – не проверять указанную область.
`AreaMask.item_#`	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (проверять вс объекты). Пример: `AreaMask.item_<номер элемента>=*doc`
`Path`	Путь к директории с проверяемыми объектами.	`<путь к локальной директории>` – проверять объекты в указанной директории. `Shared:NFS` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. `Shared:SMB` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. `Mounted:NFS` – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `AllShared` – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. `<тип файловой системы>` – проверять все ресурсы указанной файловой систем устройства.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры.		
`AreaDesc`	Описание области исключения из проверки, содержит дополнительную	Значение по умолчанию не задано.

	информацию об области исключения.	
`UseScanArea`	Исключение указанной области из проверки.	`Yes` (значение по умолчанию) – исключа указанную область. `No` – не исключать указанную область.
`AreaMask.item_#`	Ограничение области исключения из проверки. В области исключения приложение исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать вс объекты).
`Path`	Путь к директории с исключаемыми объектами.	`<путь к локальной директории>` – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

		В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида `/.snapshots/*/snapshot/`. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `<тип файловой системы>` – исключать из проверки все ресурсы указанной файловой системы устройства. Удаленные директории исключаются из проверки приложением, только если они были смонтированы до запуска задачи. Удаленные директории, смонтированные после запуска задачи, из проверки не исключаются.

Выборочная проверка файлов и директорий

Вы можете выполнять выборочную проверку указанных файлов и директорий с помощью команды `kesl-control --scan-file`.

Выборочная проверка выполняется с параметрами, которые хранятся в предустановленной задаче *Scan_File* (ID:3). Вы можете настраивать параметры выборочной проверки файлов, изменяя параметры этой задачи (см. таблицу ниже).

Чтобы запустить выборочную проверку указанных файлов и директорий, выполните следующую команду:

```
kesl-control --scan-file <путь> [--action <действие>]
```

где:

- `<путь>` – путь к файлу или директории, которые вы хотите проверить. Вы можете указать несколько путей, разделяя их пробелами.

- `--action <действие>` – действие, которое приложение будет выполнять над зараженными объектами. Если вы не укажете ключ `--action`, приложение будет выполнять действие `Recommended`.

В результате выполнения команды создается временная задача проверки файлов, которая автоматически удаляется после завершения. При этом в консоль выводятся результаты проверки.

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

Секции `[ScanScope.item_#]` и `[ExcludedFromScanScope.item_#]`, заданные в задаче *Scan_File*, не учитываются при выполнении выборочной проверки.

Параметры задачи Scan_File

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

`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронно почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почт в текстовом формате.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
`FirstAction`	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	`Disinfect` (лечить) – приложение пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, ти объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано `Disinfect`, рекомендуется задать второе действие параметре `SecondAction`. `Remove` (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. `Recommended` (выполнять рекомендуемо действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские приложения, та как они не заражают другие файлы и поэтому не предполагают лечения. `Skip` (пропускать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `Recommended`.
`SecondAction`	Выбор второго действия, которое приложение будет выполнять над зараженными объектами. Приложение выполняет второе действие,	Значения параметра `SecondAction` таки же, как значения параметра `FirstActio`

	если не удалось выполнить первое действие.	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, приложение в качестве второго действи выполняет `Skip` (пропускать). Значение по умолчанию: `Skip`.
`UseExcludeMasks`	Включение исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

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

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

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
		Значение параметра чувствительно к регистру.
		
		Значение по умолчанию не задано.
		
		Пример:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.	
`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.
`UseOASExclusions`	Включение использования исключений Защиты от файловых угроз при проверке.	`Yes` (значение по умолчанию) – использовать исключения Защиты от файловых угроз. `No` – не использовать исключения Защит от файловых угроз.
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включит эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа.	`Light` – наименее тщательная проверка минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы.

	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.	`Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) - рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включит использование технологии iChecker. `No` – выключить использование технологии iChecker.
`DeviceNameMasks.item_#`	Список названий устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску названия устройства.	`AllObjects` – проверять загрузочные секторы всех устройств. `<маска названия устройства>` – проверять загрузочные секторы устройств, названия которых содержат указанную маску. Значение по умолчанию: `/**` – любой набор символов в названии устройства, включая символ `/`.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: `All objects`. Пример: `AreaDesc="Проверка почтовых баз"`
`UseScanArea`	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	`Yes` (значение по умолчанию) – проверя указанную область. `No` – не проверять указанную область.
`AreaMask.item_#`	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (проверять вс объекты). Пример: `AreaMask.item_<номер элемента>=*doc`
`Path`	Путь к директории с проверяемыми объектами.	`<путь к локальной директории>` – проверять объекты в указанной директории.

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

Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

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

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

Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

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

Mounted:NFS – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS.

Mounted:SMB – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba.

AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS.

<тип файловой системы> – исключать из проверки все ресурсы указанной файловой системы устройства.

		Удаленные директории исключаются из проверки приложением, только если они были смонтированы до запуска задачи. Удаленные директории, смонтированные после запуска задачи, из проверки не исключаются.

Проверка важных областей

Во время проверки важных областей приложение Kaspersky Endpoint Security может проверять загрузочные секторы, объекты автозапуска, память процессов и память ядра.

При обнаружении вредоносного ПО приложение может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

Вы можете запускать проверку важных областей и настраивать параметры проверки:

- Выбирать объекты операционной системы, которые нужно проверять. По умолчанию включена проверка загрузочных секторов, памяти процессов и памяти ядра, объектов автозапуска и архивов. Файлы по умолчанию не проверяются во время проверки важных областей.
- Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
- Выбирать действия, которые приложение будет выполнять над зараженными объектами.
- Настраивать исключения объектов из проверки:
  - по именам или маскам;
  - по названиям обнаруженных в объектах угроз.
- Включать и выключать использование при проверке глобальных исключений и исключений Защиты от файловых угроз.
- Включать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.
- Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
- Ограничивать набор устройств, загрузочные секторы которых нужно проверять.
- Настраивать области проверки и области исключения из проверки.

Проверка важных областей в Web Console

В Web Console вы можете выполнять проверку важных областей операционной системы защищаемого устройства с помощью задачи *Проверка важных областей*.

Вы можете создавать и запускать пользовательские задачи проверки важных областей. Вы можете настраивать параметры проверки, изменяя параметры задач.

Параметры задачи Проверка важных областей

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы.

	Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение 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 приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение 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, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение 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, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение 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, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение 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, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию).

	• **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).
Области проверки	Таблица, содержащая области, проверяемые задачей. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы. Области проверки в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз. При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице. Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую. Кнопка доступна, если в таблице выбрана область. При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице. Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую. Кнопка доступна, если в таблице выбрана область. При нажатии на кнопку **Удалить** выбранная область исключается из проверки. Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

При нажатии на название области проверки открывается окно **<Название области проверки>**. В этом окне вы можете изменить параметры выбранной области проверки.

При нажатии на кнопку **Добавить** открывается окно **<Новая область проверки>**. В этом окне вы можете задать новую область проверки.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области	Поле ввода названия области проверки. Это название будет отображаться в таблице **Области проверки** в разделе **Параметры проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba.

	• **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги. Вы можете использовать специальные теги для указания контейнера или образа: • `[container-id:<идентификатор>]/<путь к локальной директории>` • `[container-name:<название>]/<путь к локальной директории>` • `[image-id:<идентификатор>]/<путь к локальной директории>` • `[image-name:<название>]/<путь к локальной директории>` Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`. Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен. Например: • `[container-name:<название>][image-name:<название>]/<путь к локальной директории>` • `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>` • `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>` • `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>` • `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>` В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file*/` или `/dir/file**/`. Маску ** можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Раздел Области проверки

Параметры области проверки задачи Проверка важных областей

Параметр	Описание

Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, приложение проверяет файлы. Если флажок снят, приложение не проверяет файлы. По умолчанию флажок снят.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, приложение проверяет загрузочные секторы. Если флажок снят, приложение не проверяет загрузочные секторы. По умолчанию флажок установлен.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти клиентского устройства. Если флажок установлен, приложение проверяет память ядра и запущенные процессы. Если флажок снят, приложение не проверяет память ядра и запущенные процессы. По умолчанию флажок установлен.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, приложение проверяет объекты автозапуска. Если флажок снят, приложение не проверяет объекты автозапуска. По умолчанию флажок установлен.
Устройства для проверки	По ссылке **Настроить маски устройств** открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Раздел Области исключения

В разделе **Области исключения** для задачи Проверка важных областей вы можете настроить области исключения, исключения по маске и по названию угрозы, а также использование глобальных исключений и исключений Защиты от файловых угроз во время работы задачи.

Параметры исключений из проверки

Параметр	Описание
Настроить области исключения	По ссылке **Настроить области исключения** открывается окно **Области исключения**. В этом окне вы можете задать список исключений из проверки.
Настроить исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Настроить исключения по названию угрозы	По ссылке **Настроить исключения по названию угрозы** открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки или защиты во время своей работы. Если флажок снят, приложение включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные директории. • **Смонтированная** – удаленные директории, смонтированные на устройстве. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле **Путь**. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска. При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки.

Кнопка доступна, если в списке выбрана хотя бы одна маска.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную угрозу из списка исключений.

Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Проверка важных областей в Консоли администрирования

В Консоли администрирования вы можете выполнять проверку важных областей операционной системы защищаемого устройства с помощью задачи *Проверка важных областей*.

Вы можете создавать и запускать пользовательские задачи проверки важных областей. Вы можете настраивать параметры проверки, изменяя параметры задач.

В разделе **Параметры** в свойствах задачи Проверка важных областей вы можете настроить параметры, приведенные в таблице ниже.

Параметры задачи Проверка важных областей

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки, параметры области проверки и параметры проверки.
Действие при обнаружении угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действие при обнаружении угрозы**, в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В разделе **Исключения** в свойствах задачи Проверка важных областей вы можете настроить области исключения, исключения по маске и по названию угрозы.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.

Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения.

	Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file*/` или `/dir/file**/`. Маску ** можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Параметры области проверки

В этом окне вы можете настроить параметры проверки во время работы задачи Проверка важных областей. Приложение позволяет проверять файлы, загрузочные секторы, объекты автозапуска, память процесса и память ядра.

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, Kaspersky Endpoint Security проверяет файлы. Если флажок снят, Kaspersky Endpoint Security не проверяет файлы. По умолчанию флажок снят.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, Kaspersky Endpoint Security проверяет загрузочные секторы. Если флажок снят, Kaspersky Endpoint Security не проверяет загрузочные секторы. По умолчанию флажок установлен.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти устройства. Если флажок установлен, Kaspersky Endpoint Security проверяет память ядра и запущенные процессы. Если флажок снят, Kaspersky Endpoint Security не проверяет память ядра и запущенные процессы. По умолчанию флажок установлен.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, Kaspersky Endpoint Security проверяет объекты автозапуска. Если флажок снят, Kaspersky Endpoint Security не проверяет объекты автозапуска. По умолчанию флажок установлен.
Устройства для проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области проверки

Таблица содержит маски названий устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять, и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение 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 приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение 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, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате.

	По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение 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, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение 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, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение 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, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке:

	• **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действие при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Действия при обнаружении угрозы

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).

Раздел Исключения

Исключение из проверки – это совокупность условий, при выполнении которых приложение Kaspersky Endpoint Security не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете также исключать объекты из проверки по маскам и названиям угроз.

Параметры исключений из проверки

Блок параметров	Описание
Области исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска. При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки.

Кнопка доступна, если в списке выбрана хотя бы одна маска.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную угрозу из списка исключений.

Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Проверка важных областей в командной строке

В командной строке вы можете выполнять проверку важных областей операционной системы защищаемого устройства с помощью предустановленной задачи Проверка важных областей (*Critical_Areas_Scan*).

Вы можете запускать, останавливать, приостанавливать и возобновлять эту задачу вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.

Параметры задачи Проверка важных областей

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` – проверять файлы. `No` (значение по умолчанию) – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` (значение по умолчанию) – проверя загрузочные секторы. `No` – не проверять загрузочные секторы
`ScanComputerMemory`	Включение проверки памяти процессов и памяти ядра.	`Yes` (значение по умолчанию) – проверять память процессов и память ядра. `No` – не проверять память процессов и память ядра.
`ScanStartupObjects`	Включение проверки объектов автозапуска.	`Yes` (значение по умолчанию) – проверя объекты автозапуска. `No` – не проверять объекты автозапуска.
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX).	`Yes` (значение по умолчанию) – проверя архивы. Если указано значение `FirstAction=Recommended`, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.

	Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (значение по умолчанию) – проверя самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронно почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почт в текстовом формате.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
`FirstAction`	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	`Disinfect` (лечить) – приложение пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, ти объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано `Disinfect`, рекомендуется задать второе действие в параметре `SecondAction`. `Remove` (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию.

		Recommended (выполнять рекомендуемо действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские приложения, та как они не заражают другие файлы и поэтому не предполагают лечения. Skip (пропускать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: Recommended.
SecondAction	Выбор второго действия, которое приложение будет выполнять над зараженными объектами. Приложение выполняет второе действие, если не удалось выполнить первое действие.	Значения параметра SecondAction таки же, как значения параметра FirstActio 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, приложение в качестве второго действи выполняет Skip (пропускать). Значение по умолчанию: Skip.
UseExcludeMasks	Включение исключения из проверки объектов, указанных параметром ExcludeMasks.item_#.	Yes – исключать из проверки объекты, указанные параметром ExcludeMasks.item_#. No (значение по умолчанию) – не исключать из проверки объекты, указанные параметром ExcludeMasks.item_#.
ExcludeMasks.item_#	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр UseExcludeMasks.	Значение по умолчанию не задано. Пример: UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	Включение исключения из проверки объектов с угрозами, указанными параметром ExcludeThreats.item_#.	Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром ExcludeThreats.item_#. No (значение по умолчанию) – не исключать из проверки объекты, которы содержат угрозы, указанные параметром ExcludeThreats.item_#.

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		
		Значение по умолчанию не задано.
		
		Пример:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.
`UseOASExclusions`	Включение использования исключений Защиты от файловых угроз при проверке.	`Yes` (значение по умолчанию) – использовать исключения Защиты от файловых угроз. `No` – не использовать исключения Защит от файловых угроз.
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов.	`Yes` – записывать в журнал информацию проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.

	Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включит эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) - рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включит использование технологии iChecker. `No` – выключить использование технологии iChecker.
`DeviceNameMasks.item_#`	Список названий устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску названия устройства.	`AllObjects` – проверять загрузочные секторы всех устройств. `<маска имени устройства>` – проверять загрузочные секторы устройств, названия которых содержат указанную маску. Значение по умолчанию: `/**` – любой набор символов в названии устройства, включая символ `/`.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой	Значение по умолчанию: `All objects`. Пример: `AreaDesc="Mail bases scan"`

	этим параметром: 4096 символов.	
`UseScanArea`	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	`Yes` (значение по умолчанию) – проверя указанную область. `No` – не проверять указанную область.
`AreaMask.item_#`	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (проверять вс объекты). Пример: `AreaMask.item_<номер элемента>=*doc`
`Path`	Путь к директории с проверяемыми объектами.	`<путь к локальной директории>` – проверять объекты в указанной директории. `Shared:NFS` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. `Shared:SMB` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. `Mounted:NFS` – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `AllShared` – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. `<тип файловой системы>` – проверять все ресурсы указанной файловой систем устройства.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной	`Yes` (значение по умолчанию) – исключа

	области из проверки.	указанную область. `No` – не исключать указанную область.
`AreaMask.item_#`	Ограничение области исключения из проверки. В области исключения приложение исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать вс объекты).
`Path`	Путь к директории с исключаемыми объектами.	`<путь к локальной директории>` – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

		В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида `/.snapshots/*/snapshot/`. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `<тип файловой системы>` – исключать из проверки все ресурсы указанной файловой системы устройства. Удаленные директории исключаются из проверки приложением, только если они были смонтированы до запуска задачи. Удаленные директории, смонтированные после запуска задачи, из проверки не исключаются.

Проверка съемных дисков

Kaspersky Endpoint Security может проверять следующие съемные диски при подключении их к защищаемому устройству: CD/DVD-приводы, Blu-ray диски, флеш-накопители (включая USB-модемы), внешние жесткие диски и дискеты.

Если проверка съемных дисков включена, приложение Kaspersky Endpoint Security контролирует подключение съемных дисков к защищаемому устройству и при обнаружении подключенного съемного диска проверяет диск и его загрузочные секторы на вирусы и другие вредоносные программы.

По умолчанию приложение не контролирует подключение съемных дисков и не проверяет их.

Эта функциональность не поддерживается в KESL-контейнере.

Настройка проверки съемных дисков в Web Console

В Web Console вы можете настраивать параметры проверки съемных дисков в свойствах политики (**Параметры приложения** → **Локальные задачи** → **Проверка съемных дисков**).

Параметры компонента Проверка съемных дисков

Параметр	Описание
Проверка съемных дисков включена / выключена	Переключатель включает или выключает проверку съемных дисков при подключении их к устройству пользователя. По умолчанию переключатель выключен.
Действие при подключении съемного диска	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять приложение при подключении съемных дисков к устройству пользователя: • **Не проверять** съемные диски при подключении (значение по умолчанию). • **Быстрая проверка** – проверять на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков) только файлы определенных типов и не распаковывать составные объекты. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Проверка важных областей*. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **Подробная проверка** – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Поиск вредоносного ПО*.
Действие при подключении	В раскрывающемся списке вы можете выбрать действие, которое будет

CD/DVD-привода	выполнять приложение при подключении CD/DVD-приводов и Blu-ray дисков к устройству пользователя: • **Не проверять** CD/DVD-приводы и Blu-ray диски при подключении (значение по умолчанию). • **Быстрая проверка** – проверять на CD/DVD-приводах и Blu-ray дисках только файлы определенных типов. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Проверка важных областей*. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **Подробная проверка** – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Поиск вредоносного ПО*.
Блокировать доступ к съемному диску во время проверки	Флажок включает или выключает блокировку файлов на подключенном диске во время выполнения проверки. По умолчанию флажок снят.

Настройка проверки съемных дисков в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры проверки съемных дисков в свойствах политики (**Локальные задачи** → **Проверка съемных дисков**).

Параметры компонента Проверка съемных дисков

Параметр	Описание
Включить проверку съемных дисков при подключении к устройству	Флажок включает или выключает проверку съемных дисков при подключении их к устройству пользователя. По умолчанию флажок снят.
Действие при подключении съемного диска	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять приложение при подключении съемных дисков к устройству пользователя: • **Не проверять** съемные диски при подключении (значение по умолчанию). • **Быстрая проверка** – проверять на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков) только файлы определенных типов и не распаковывать составные объекты. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Проверка важных областей*.

	На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **Подробная проверка** – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Поиск вредоносного ПО*.
Действие при подключении CD/DVD-привода	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять приложение при подключении CD/DVD-приводов и Blu-ray дисков к устройству пользователя: • **Не проверять** CD/DVD-приводы и Blu-ray диски при подключении (значение по умолчанию). • **Быстрая проверка** – проверять на CD/DVD-приводах и Blu-ray дисках только файлы определенных типов. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Проверка важных областей*. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **Подробная проверка** – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Поиск вредоносного ПО*.
Блокировать доступ к съемному диску во время проверки	Флажок включает или выключает блокировку файлов на подключенном диске во время выполнения проверки. По умолчанию флажок снят.

Настройка проверки съемных дисков в командной строке

В командной строке вы можете управлять проверкой съемных дисков с помощью предустановленной задачи Проверка съемных дисков (*Removable_Drives_Scan*).

По умолчанию задача Проверка съемных дисков не запущена. Вы можете запускать и останавливать эту задачу вручную. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.

Если задача запущена, приложение контролирует подключение съемных дисков к устройству и при подключении съемного диска создает и запускает временную задачу проверки загрузочных секторов (задачу типа *ODS*). Эту задачу остановить невозможно. После завершения выполнения задачи приложение автоматически ее удаляет.

Если в параметрах задачи Проверка съемных дисков вы включили проверку файлов, приложение также запускает одну или несколько временных задач выборочной проверки файлов (задачи типа *ODS*). Если требуется, пользователь с правами администратора может останавливать выполнение таких задач.

При изменении параметров задачи Проверка съемных дисков новые значения не применяются к уже запущенным временным задачам. При остановке задачи Проверка съемных дисков уже запущенные временные задачи не останавливаются.

Параметры задачи Проверка съемных дисков

Параметр	Описание	Значения
`ScanRemovableDrives`	Включение проверки съемных дисков при подключении к устройству. Этот параметр не применяется к CD/DVD-приводам и Blu-ray дискам (см. параметр `ScanOpticalDrives`).	`DetailedScan` – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). Детализированная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Scan_File* (ID:3). `QuickScan` – проверять на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков) только файлы определенных типов. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Critical_Areas_Scan* (ID:4). `NoScan` (значение по умолчанию) – не проверять съемные диски при подключении.
`ScanOpticalDrives`	Включение проверки CD/DVD-приводов и Blu-ray дисков при подключении к устройству.	`DetailedScan` – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. Детализированная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Scan_File* (ID:3). `QuickScan` – проверять на CD/DVD-приводах и Blu-ray дисках только файлы определенных типов. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Critical_Areas_Scan* (ID:4).

		`NoScan` (значение по умолчанию) – не проверять CD/DVD-приводы и Blu-ray диски при подключении.
`BlockDuringScan`	Включение блокировки файлов на подключенном диске при проверке. При проверке загрузочных секторов файлы не блокируются.	`Yes` – блокировать файлы при проверке. `No` (значение по умолчанию) – не блокировать файлы при проверке.

Проверка контейнеров

Вы можете выполнять проверку контейнеров и образов на наличие вредоносного ПО в режиме реального времени и по требованию:

- Компонент *Мониторинг контейнеров* позволяет проверять запускаемые контейнеры и пространства имен в реальном времени.
- С помощью задач *Проверка контейнеров* вы можете выполнять проверку контейнеров и образов по требованию.

Приложение поддерживает интеграцию с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Для использования задач Проверка контейнеров требуется лицензия, которая включает эту функцию.

Мониторинг контейнеров

По умолчанию компонент Мониторинг контейнеров включен. Приложение проверяет в реальном времени запущенные контейнеры и пространства имен.

Для работы компонента Мониторинг контейнеров должен быть включен компонент Защита от файловых угроз. Во время проверки контейнеров и пространств имен используются параметры защиты от файловых угроз.

Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен. При этом статус компонента Мониторинг контейнеров в командной строке отображается как "`Задача доступна и не выполняется`", в Kaspersky Security Center отображается как "`Остановлена`".

Вы можете включать и выключать компонент Мониторинг контейнеров, а также настраивать параметры проверки контейнеров и пространств имен в реальном времени:

- Выбирать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта.

  Этот параметр доступен при использовании приложения по лицензии, которая включает эту функцию.

- Настраивать интеграцию приложения Kaspersky Endpoint Security с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Настройка мониторинга контейнеров в Web Console

В Web Console вы можете управлять работой компонента *Мониторинг контейнеров* в свойствах политики (**Параметры приложения → Общие параметры → Параметры проверки контейнеров**).

Параметры мониторинга контейнеров

Параметр	Описание
Проверка пространств имен и контейнеров включена / выключена	Переключатель включает или выключает проверку пространств имен и контейнеров в реальном времени. По умолчанию переключатель включен.
Действие с контейнером при обнаружении угрозы	Вы можете выбрать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта: • **Пропустить контейнер** – при обнаружении зараженного объекта приложение не выполняет никаких действий над контейнером. • **Остановить контейнер** – при обнаружении зараженного объекта приложение останавливает контейнер. • **Остановить контейнер, если не удалось вылечить** (значение по умолчанию) – если не удалось вылечить зараженный объект, приложение останавливает контейнер. Этот параметр доступен при использовании приложения по лицензии, которая включает эту функцию.
Использовать Docker	Флажок включает или выключает использование среды Docker. По умолчанию флажок установлен.
Путь Docker-сокета	Поле ввода пути или URI (универсальный идентификатор ресурса) Docker-сокета. Значение по умолчанию: /var/run/docker.sock.
Использовать CRI-O	Флажок включает или выключает использование среды CRI-O. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к конфигурационному файлу CRI-O. Значение по умолчанию: /etc/crio/crio.conf.
Использовать Podman	Флажок включает или выключает использование утилиты Podman. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты Podman. Значение по умолчанию: /usr/bin/podman.
Корневая директория	Поле ввода пути к корневой директории хранилища контейнеров. Значение по умолчанию: /var/lib/containers/storage.
Использовать runc	Флажок включает или выключает использование утилиты runc. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты runc. Значение по умолчанию: /usr/bin/runc.
Корневая директория	Поле ввода пути к корневой директории хранилища состояний контейнеров.

	Значение по умолчанию: /run/runc.

Настройка мониторинга контейнеров в Консоли администрирования

В Консоли администрирования вы можете управлять работой компонента Мониторинг контейнеров в свойствах политики (**Общие параметры** → **Параметры проверки контейнеров**).

Параметры мониторинга контейнеров

Параметр	Описание
Включить проверку пространств имен и контейнеров	Флажок включает или выключает проверку пространств имен и контейнеров в реальном времени. По умолчанию флажок установлен.
Действие с контейнером при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта: • **Пропустить контейнер** – при обнаружении зараженного объекта приложение не выполняет никаких действий над контейнером. • **Остановить контейнер** – при обнаружении зараженного объекта приложение останавливает контейнер. • **Остановить, если не удалось вылечить** (значение по умолчанию) – если не удалось вылечить зараженный объект, приложение останавливает контейнер. Этот параметр доступен при использовании приложения по лицензии, которая включает эту функцию.
Параметры проверки контейнеров	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Параметры проверки контейнеров**.

Окно Параметры проверки контейнеров

В этом окне вы можете настроить параметры интеграции приложения Kaspersky Endpoint Security с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Параметры проверки контейнеров

Параметр	Описание
Использовать Docker	Флажок включает или выключает использование среды Docker. По умолчанию флажок установлен.
Путь Docker-сокета	Поле ввода пути или URI (универсальный идентификатор ресурса) Docker-сокета. Значение по умолчанию: /var/run/docker.sock.
Использовать CRI-O	Флажок включает или выключает использование среды CRI-O. По умолчанию флажок установлен.

Путь к файлу	Поле ввода пути к конфигурационному файлу CRI-O. Значение по умолчанию: /etc/crio/crio.conf.
Использовать Podman	Флажок включает или выключает использование утилиты Podman. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты Podman. Значение по умолчанию: /usr/bin/podman
Корневая директория	Поле ввода пути к корневой директории хранилища контейнеров.
Использовать runc	Флажок включает или выключает использование утилиты runc. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты runc. Значение по умолчанию: /usr/bin/runc
Корневая директория	Поле ввода пути к корневой директории хранилища состояний контейнеров. Значение по умолчанию: /run/runc.

Настройка мониторинга контейнеров в командной строке

В командной строке вы можете включать и выключать проверку пространств имен и контейнеров в реальном времени с помощью параметра `NamespaceMonitoring=Yes/No` из общих параметров приложения.

Вы можете изменять значение параметра `NamespaceMonitoring` с помощью конфигурационного файла, который содержит все общие параметры приложения, или с помощью ключей командной строки.

При проверке пространств имен и контейнеров в реальном времени используются общие параметры проверки контейнеров. Вы можете просматривать и изменять эти параметры с помощью специальных команд управления Kaspersky Endpoint Security:

- Вы можете выводить текущие значения общих параметров проверки контейнеров в консоль или в конфигурационный файл. Этот файл вы можете использовать для изменения параметров.
- Вы можете изменять все общие параметры проверки контейнеров, используя конфигурационный файл, который содержит параметры. Конфигурационный файл вы можете получить с помощью команды вывода общих параметров проверки контейнеров.
- Вы можете изменять отдельные параметры, используя ключи командной строки в формате `< имя параметра >=< значение параметра >`. Текущие значения параметров вы можете получить с помощью команды вывода общих параметров проверки контейнеров.

Чтобы вывести в консоль текущие значения общих параметров проверки контейнеров, выполните следующую команду:

```
kesl-control --get-container-settings [--json]
```

где `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Чтобы вывести в файл текущие значения общих параметров проверки контейнеров, выполните следующую команду:

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

где:

- `--file <путь к конфигурационному файлу>` – путь к файлу, в который будут сохранены общие параметры проверки контейнеров. Если вы укажете имя файла, не указав путь 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, файл не будет создан.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Чтобы изменить значения общих параметров проверки контейнеров с помощью конфигурационного файла:

1. Выведите общие параметры проверки контейнеров в конфигурационный файл, как описано выше.
2. Измените значения нужных параметров в файле и сохраните изменения.
3. Выполните команду:

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

   где:

   - `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу с общими параметрами проверки контейнеров.
   - `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

   Все значения общих параметров проверки контейнеров, заданные в файле, будут импортированы в приложение.

Чтобы изменить значения общих параметров проверки контейнеров с помощью ключей командной строки, выполните следующую команду:

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

где `<имя параметра>=<значение параметра>` – имя и значение одного из общих параметров проверки контейнеров.

Значения указанных общих параметров проверки контейнеров будут изменены.

Проверка контейнеров и образов по требованию

Во время выполнения задачи *Проверка контейнеров* приложение Kaspersky Endpoint Security проверяет контейнеры и образы на наличие вирусов и других вредоносных программ. Приложение может выполнять одновременно несколько задач проверки контейнеров.

Поддерживается интеграция с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Для использования задачи требуется лицензия, которая включает эту функцию.

Вы можете запускать проверку контейнеров и настраивать параметры проверки:

- Указывать контейнеры и образы, которые нужно проверять, по имени или маске имени.
- Включать проверку всех слоев образов и контейнеров.
- Выбирать действие, которое приложение будет выполнять над контейнером, и действие, которое приложение будет выполнять над образом при обнаружении зараженного объекта.
- Настраивать параметры проверки объектов внутри контейнеров или образов:
  - Включать и выключать проверку архивов, почтовых баз, сообщений электронной почты в текстовом формате.
  - Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
  - Выбирать действия, которые приложение будет выполнять над зараженными объектами.
  - Настраивать исключения объектов из проверки:
    - по именам или маскам;
    - по названиям обнаруженных в объектах угроз.
  - Включать и выключать использование глобальных исключений при проверке.
  - Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
  - Включать и выключать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.

Проверка контейнеров в Web Console

В Web Console вы можете выполнять проверку контейнеров и образов с помощью задачи *Проверка контейнеров*.

Вы можете создавать и запускать пользовательские задачи проверки контейнеров. Вы можете настраивать параметры проверки, изменяя параметры задач.

Параметры задачи Проверка контейнеров

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы.

	По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение 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 приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение 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, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение 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, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение 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, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение 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, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое

	действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).
Проверять контейнеры	Флажок включает или выключает проверку контейнеров. Если флажок установлен, вы можете указать имя или маску имени проверяемых контейнеров. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых контейнеров. По умолчанию указана маска * – выполняется проверка всех контейнеров.
Действие при обнаружении угрозы	Вы можете выбрать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта: • **Пропустить контейнер** – не выполнять никаких действий над контейнером при обнаружении зараженного объекта. • **Остановить контейнер** – остановить контейнер при обнаружении зараженного объекта. • **Остановить контейнер, если не удалось вылечить** (значение по умолчанию) – остановить контейнер, если не удалось вылечить зараженный объект или устранить угрозу. Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие **Остановить контейнер**.
Проверять образы	Флажок включает или выключает проверку образов. Если флажок установлен, вы можете указать имя или маску имени проверяемых образов. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых образов. По умолчанию указана маска * – выполняется проверка всех образов.
Действие при обнаружении угрозы	Вы можете выбрать действие, которое приложение будет выполнять над образом при обнаружении зараженного объекта: • **Пропустить образ** (значение по умолчанию) – не выполнять никаких действий над образом при обнаружении зараженного объекта. • **Удалить образ** при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.

Проверять каждый слой	Флажок включает или выключает проверку всех слоев образов и запущенных контейнеров. По умолчанию флажок снят.

Раздел Области исключения

В разделе **Области исключения** для задачи Проверка контейнеров вы можете настроить исключения по маске и по названию угрозы, а также использование глобальных исключений во время работы задачи.

Параметры исключений из проверки

Параметр	Описание
Настроить исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Настроить исключения по названию угрозы	По ссылке **Настроить исключения по названию угрозы** открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки.

Кнопка доступна, если в списке выбрана хотя бы одна маска.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную угрозу из списка исключений.

Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Проверка контейнеров в Консоли администрирования

В Консоли администрирования вы можете выполнять проверку контейнеров и образов с помощью задачи *Проверка контейнеров*.

Вы можете создавать и запускать пользовательские задачи проверки контейнеров. Вы можете настраивать параметры проверки, изменяя параметры задач.

В разделе **Параметры** в свойствах задачи Проверка контейнеров вы можете настроить параметры, приведенные в таблице ниже.

Параметры задачи Проверка контейнеров

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить параметры проверки контейнеров и общие параметры проверки.
Действие	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается

при обнаружении угрозы	окно **Действие при обнаружении угрозы**, в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В разделе **Исключения** в свойствах задачи Проверка контейнеров вы также можете настроить исключения по маске и по названию угрозы.

Окно Параметры проверки контейнеров

В этом окне вы можете настроить параметры проверки контейнеров и образов.

Параметры проверки контейнеров и образов

Параметр	Описание
Проверять контейнеры	Флажок включает или выключает проверку контейнеров. Если флажок установлен, вы можете указать имя или маску имени проверяемых контейнеров. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых контейнеров. По умолчанию указана маска * – выполняется проверка всех контейнеров.
Действие при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта: • **Пропустить контейнер** – не выполнять никаких действий над контейнером при обнаружении зараженного объекта. • **Остановить контейнер** – остановить контейнер при обнаружении зараженного объекта. • **Остановить, если не удалось вылечить** (значение по умолчанию) – остановить контейнер, если не удалось вылечить зараженный объект или устранить угрозу. Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие **Остановить контейнер**.
Проверять образы	Флажок включает или выключает проверку образов. Если флажок установлен, вы можете указать имя или маску имени проверяемых образов. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых образов. По умолчанию указана маска * – выполняется проверка всех образов.
Действие при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять над образом при обнаружении зараженного объекта: • **Пропустить образ** (значение по умолчанию) – не выполнять никаких действий над образом при обнаружении зараженного объекта. • **Удалить образ** при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.

Проверять каждый слой	Флажок включает или выключает проверку всех слоев образов и запущенных контейнеров. По умолчанию флажок снят.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение 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 приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение 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, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.

Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение 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, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение 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, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение 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, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему.

	• **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действие при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Действия при обнаружении угрозы

Параметр	Описание
Первое действие	В раскрывающемся списке вы можете выбрать первое действие, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения (значение по умолчанию). • **Пропускать** объект.
Второе действие	В раскрывающемся списке вы можете выбрать второе действие, которое приложение будет выполнять над зараженным объектом, если первое действие выполнить не удалось: • **Лечить** объект. Копия зараженного объекта будет помещена в резервное хранилище. • **Удалять** объект. Копия зараженного объекта будет помещена резервное хранилище. • **Выполнять рекомендованное действие** над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения. • **Пропускать** объект (значение по умолчанию).

•

Раздел Исключения

Параметры исключений из проверки

Блок параметров	Описание
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Исключения по маске. В этом окне вы можете настроить исключение объектов из проверки по маске имени.

Исключения по названию угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки.

Кнопка доступна, если в списке выбрана хотя бы одна маска.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную угрозу из списка исключений.

Кнопка доступна, если в списке выбрано хотя бы одно название угрозы.

При нажатии на название угрозы в таблице открывается окно **Название угрозы**. В этом окне вы можете изменить название угрозы, исключаемой из проверки.

При нажатии на кнопку **Добавить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

Проверка контейнеров в командной строке

В командной строке вы можете выполнять проверку контейнеров и образов следующими способами:

- С помощью предустановленной задачи Проверка контейнеров (*Container_Scan*). Вы можете запускать и останавливать эту задачу вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.
- С помощью пользовательских задач проверки контейнеров (задач типа *ContainerScan*). Вы можете запускать и останавливать пользовательские задачи вручную и настраивать расписание запуска задач.
- С помощью команды `kesl-control --scan-container` вы можете выполнять *выборочную проверку* указанных контейнеров и образов.

Параметры задачи Проверка контейнеров

В таблице описаны все доступные значения и значения по умолчанию для всех параметров проверки контейнеров и образов.

Параметры задачи Проверка контейнеров

Параметр	Описание	Значения
`ScanContainers`	Проверка контейнеров, заданных по маске. Вы можете указать маски с помощью параметра `ContainerNameMask`.	`Yes` (значение по умолчанию) – проверять контейнеры, заданные по маске. `No` – не проверять контейнеры, заданные по маске.
`ContainerNameMask`	Имя или маска имени проверяемого контейнера. Маски указываются в формате командной оболочки. Вы можете использовать символы ? и *. Прежде чем указать этот параметр, убедитесь, что значение параметра `ScanContainers=Yes`.	Значение по умолчанию: * (выполнять проверку всех контейнеров). Примеры: Проверять контейнер с именем my_container: `ContainerNameMask=my_container` Проверять все контейнеры, имена которых начинаются с my_container: `ContainerNameMask=my_container*` Проверять все контейнеры, имена которых начинаются с my_, затем содержат пять любых символов, затем слово _container и заканчиваются любой последовательностью символов:

		`ContainerNameMask=my_?????_container*`
`ScanImages`	Проверка образов, заданных по маске. Вы можете указать маски с помощью параметра `ImageNameMask`.	`Yes` (значение по умолчанию) – проверять образы, заданные по маске. `No` – не проверять образы, заданные по маске.

`ImageNameMask`	Имя или маска имени проверяемых образов.
	Прежде чем указать этот параметр, убедитесь, что для параметра `ScanImages` выбрано значение `Yes`.
	Маски указываются в формате командной оболочки.
	Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом.
		Значение по умолчанию: * (выполнять проверку 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`	Проверка всех слоев образов и запущенных контейнеров.	`Yes` – проверять все слои. `No` (значение по умолчанию) – не проверять все слои.
`ContainerScanAction`	Действие над контейнером при обнаружении зараженного объекта. Действия над зараженным объектом внутри контейнера описаны ниже.	`StopContainerIfFailed` (значение по умолчанию) – приложение останавливает контейнер, если не удалось вылечить или удалить зараженный объект. Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие `StopContainer`. `StopContainer` – приложение останавливает контейнер при обнаружении зараженного объекта. `Skip` – приложение не выполняет никаких действий над контейнерами при обнаружении зараженного объекта.
`ImageAction`	Действие над образом при обнаружении зараженного объекта. Действия над зараженным объектом внутри образа описаны ниже.	`Skip` (значение по умолчанию) – приложение не выполняет никаких действий над образами при обнаружении зараженного объекта. `Delete` – приложение удаляет образ при обнаружении зараженного объекта (не рекомендуется).

		Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.

Ниже описаны параметры, которые применяются к объектам внутри контейнеров и образов.

Параметры задачи Проверка контейнеров

Параметр	Описание	Значения
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	`Yes` (значение по умолчанию) – проверя архивы. Если указано значение `FirstAction=Recommended`, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (значение по умолчанию) – проверя самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронно почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почт в текстовом формате.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.

`FirstAction`	Выбор первого действия, которое приложение будет выполнять над зараженными объектами.	`Disinfect` (лечить) – приложение пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, ти объекта или тип угрозы в объекте не предполагает лечения), приложение оставляет объект неизменным. Если первым действием выбрано `Disinfect`, рекомендуется задать второе действие в параметре `SecondAction`. `Remove` (удалять) – приложение удаляет зараженный объект, предварительно создав его резервную копию. `Recommended` (выполнять рекомендуемо действие) – приложение автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские приложения, та как они не заражают другие файлы и поэтому не предполагают лечения. `Skip` (пропускать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `Recommended`.
`SecondAction`	Выбор второго действия, которое приложение будет выполнять над зараженными объектами. Приложение выполняет второе действие, если не удалось выполнить первое действие.	Значения параметра `SecondAction` таки же, как значения параметра `FirstActio` 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, приложение в качестве второго действи выполняет `Skip` (пропускать). Значение по умолчанию: `Skip`.
`UseExcludeMasks`	Использование исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

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

	файлов, используя маски в формате shell.	
`UseExcludeThreats`	Использование исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats.item_#`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, которы содержат угрозы, указанные параметром `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных	`Yes` – записывать в журнал информацию проверке объектов в составе архивов.

	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 приложением.	`No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включит эвристический анализатор; `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) - рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включит использование технологии iChecker. `No` – выключить использование технологии iChecker.

Выборочная проверка контейнеров и образов

Вы можете выполнять выборочную проверку указанных контейнеров и образов с помощью команды `kesl-control --scan-container`.

Выборочная проверка выполняется с параметрами, которые хранятся в предустановленной задаче *Custom_Container_Scan* (ID:19). Вы можете настраивать параметры выборочной проверки контейнеров и образов, изменяя параметры этой задачи. По умолчанию для задачи *Custom_Container_Scan* заданы такие же параметры, как для задачи *Container_Scan* (ID:18).

Чтобы запустить выборочную проверку контейнеров, выполните следующую команду:

```
kesl-control --scan-container <контейнер/образ [:тег ]>
```

где `<контейнер/образ [:тег ]>` – имя или идентификатор контейнера или образа. Для проверки нескольких объектов вы можете использовать маски.

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

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

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Если существует несколько элементов с одинаковым именем, приложение проверяет их все.

В результате выполнения команды создается временная задача проверки контейнеров и образов, которая автоматически удаляется после завершения. При этом в консоль выводятся результаты проверки.

Примеры:
Проверка контейнера с именем my_container:
```
kesl-control --scan-container my_container
```
Проверка образа с именем my_image (все теги):
```
kesl-control --scan-container my_image*
```

Интеграция с Jenkins

Kaspersky Endpoint Security поддерживает интеграцию с Jenkins. Плагины Jenkins Pipeline можно использовать для проверки Docker-образов на разных этапах. Например, можно проверять Docker-образы в репозитории в процессе разработки или перед публикацией.

Чтобы интегрировать Kaspersky Endpoint Security с Jenkins:

1. Установите Kaspersky Endpoint Security на узле Jenkins.
2. Установите Docker Engine на узле Jenkins.

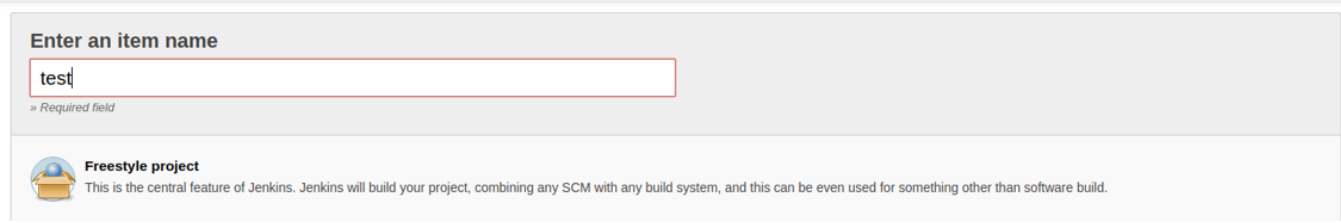
   Дополнительная информация приведена в документации Docker Engine.
3. Предоставьте пользователю Jenkins права администратора приложения Kaspersky Endpoint Security:

   ```
   kesl-control --grant-role admin <имя пользователя Jenkins>
   ```
4. Добавьте пользователя Jenkins в группу docker:

   ```
   sudo usermod -aG docker <имя пользователя Jenkins>
   ```

Обычно используется имя jenkins.

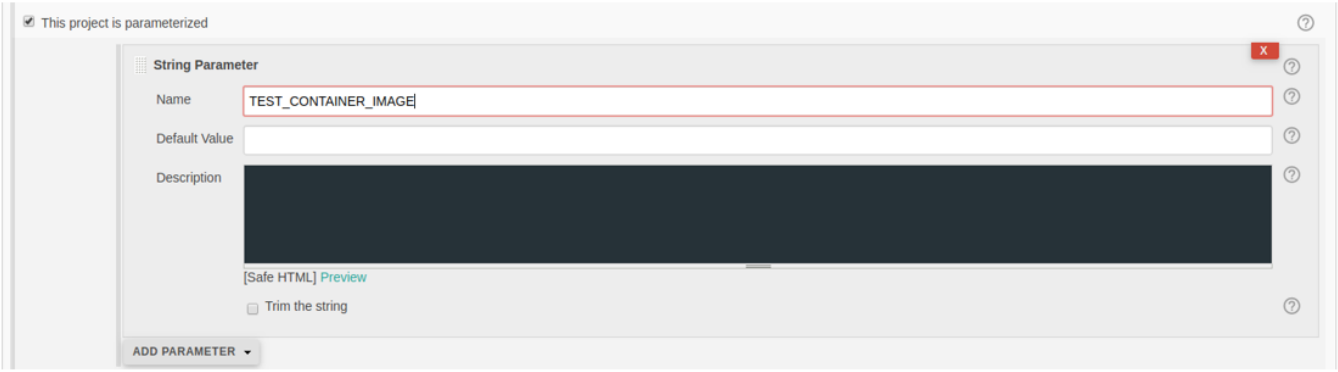
5. В Jenkins создайте новое задание на сборку с названием `test` (**New Item** → **Enter an item name**).



6. Настройте проект в соответствии с вашими требованиями. Предполагается, что в результате настройки вы получите образ или запущенный контейнер, который нужно проверить.

7. Чтобы запустить Docker-контейнер, добавьте следующий скрипт в процедуру сборки Jenkins. Если вы используете плагины Jenkins или другой способ запуска Docker-контейнеров, сохраните идентификатор запущенного Docker-контейнера в файл /tmp/kesl_cs_info для дальнейшей проверки:

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE}
/storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
exit ${EXIT_CODE}
```



8. После создания артефактов добавьте следующий сценарий к шагам создания jenkins.

   Этот скрипт поддерживает проверку одного контейнера. Если требуется, измените скрипт в соответствии с вашими требованиями.

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
```

```
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. Чтобы выполнить проверку Docker-образа из репозитория, выполните следующий скрипт:

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container ${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. Сохраните задание на сборку.

Управление сетевым экраном

Во время работы в локальных сетях и интернете устройство подвержено не только заражению вирусами и другими вредоносными приложениями, но и различного рода атакам, использующим уязвимости операционных систем и программного обеспечения. Сетевой экран операционной системы защищает данные, которые хранятся на устройстве пользователя, блокируя большую часть угроз для операционной системы, когда устройство подключено к интернету или локальной сети.

Сетевой экран операционной системы позволяет обнаружить все сетевые соединения на устройстве пользователя и предоставить список их IP-адресов. Компонент Управление сетевым экраном позволяет задать статус этих сетевых соединений при помощи настройки сетевых пакетных правил.

Эта функциональность не поддерживается в KESL-контейнере.

С помощью сетевых пакетных правил вы можете задать нужный уровень защиты устройства, от полной блокировки доступа в интернет для всех приложений до разрешения неограниченного доступа. Все исходящие соединения по умолчанию разрешены за исключением случаев, когда указаны соответствующие запрещающие правила компонента Управление сетевым экраном.

По умолчанию компонент Управление сетевым экраном выключен.

Перед включением компонента Управление сетевым экраном рекомендуется выключить другие средства управления сетевым экраном операционной системы.

При включении компонента Управление сетевым экраном приложение Kaspersky Endpoint Security автоматически удаляет все пользовательские правила, настроенные для сетевого экрана средствами операционной системы. После выключения компонента эти правила не восстанавливаются. Если требуется, сохраните пользовательские правила сетевого экрана до включения компонента Управление сетевым экраном.

Если управление сетевым экраном включено, Kaspersky Endpoint Security проверяет сетевой экран операционной системы и блокирует любую попытку изменить параметры сетевого экрана, например, когда какое-либо приложение или утилита пытается добавить или удалить какое-либо правило сетевого экрана. Kaspersky Endpoint Security проверяет сетевой экран операционной системы каждые 60 секунд и, если требуется, восстанавливает набор правил сетевого экрана, созданных с помощью приложения. Периодичность проверки изменить невозможно.

В операционных системах Red Hat Enterprise Linux и CentOS 8 правила сетевого экрана, созданные в приложении Kaspersky Endpoint Security, можно просмотреть только с помощью команд управления (команда `kesl-control -F --query`).

Kaspersky Endpoint Security по-прежнему проверяет сетевой экран операционной системы, когда управление сетевым экраном выключено. Это позволяет приложению восстанавливать динамические правила.

Вы можете включать и выключать управление сетевым экраном, а также настраивать следующие параметры:

- Настраивать список сетевых пакетных правил, которые приложение Kaspersky Endpoint Security будет применять при обнаружении попытки установить сетевое соединение. Вы можете добавлять и удалять сетевые пакетные правила, а также изменять приоритет выполнения сетевого пакетного правила.

- Выбирать действия по умолчанию, применяемые к входящим соединениям и пакетам, если другие сетевые пакетные правила не применяются к этому виду соединений.

- Устанавливать соответствие сетевых адресов предустановленным сетевым зонам. Вы можете добавлять IP-адреса или подсети в сетевые зоны и удалять адреса из сетевых зон.

- Включать и выключать автоматическое добавление разрешающих правил для портов Агента администрирования.

Во избежание возможных проблем на системах с nftables приложение Kaspersky Endpoint Security использует системные утилиты iptables и iptables-restore при добавлении правил для сетевого экрана операционной системы. Приложение создает специальную разрешающую цепочку правил kesl_bypass и добавляет ее первой в список таблицы mangle утилит iptables и ip6tables. Правила цепочки kesl_bypass позволяют исключать трафик из проверки приложением Kaspersky Endpoint Security. Изменение правил в этой цепочке выполняется средствами операционной системы. При удалении приложения цепочка правил kesl_bypass в iptables и ip6tables удаляется, только если она была пустая.

О сетевых пакетных правилах

Сетевое пакетное правило представляет собой разрешающее или запрещающее действие, которое совершает Kaspersky Endpoint Security, обнаружив попытку сетевого соединения.

Правила используются для ввода ограничений на сетевые пакеты независимо от приложения. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных.

Все исходящие соединения разрешены по умолчанию (параметр действие по умолчанию) за исключением случаев, когда указаны соответствующие запрещающие правила Управления 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.

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

Приложение Kaspersky Endpoint Security позволяет добавлять и удалять в сетевой экран *динамические правила*, необходимые для правильной работы приложения. Например, Агент администрирования добавляет динамические правила, которые разрешают соединение с Kaspersky Security Center, инициируемые как приложением, так и Kaspersky Security Center. Правила Защиты от шифрования тоже являются динамическими.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, в сетевой экран автоматически добавляются динамические правила, которые разрешают соединения с SVM и Сервером интеграции.

Kaspersky Endpoint Security не контролирует динамические правила и не блокирует доступ к сетевым ресурсам для компонентов приложения. Динамические правила не зависят от состояния компонента Управление сетевым экраном (включен/выключен) или от изменения параметров работы компонента. Приоритет выполнения динамических правил выше приоритета сетевых пакетных правил. Приложение 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 параметра "удаленный адрес" при создании сетевого пакетного правила. 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 антивирусным приложением, 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 устройстве (таким как локальные или домашние сети).
- **Доверенные**. Эта зона предназначена для безопасных сетей, в которых устройства 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 или удалять их из нее.

Управление сетевым экраном в Web Console

В Web Console вы можете настраивать параметры управления сетевым экраном в свойствах политики (**Параметры приложения** → **Базовая защита** → **Управление сетевым экраном**).

Параметры компонента Управление сетевым экраном

Параметр	Описание
Управление сетевым экраном включено / выключено	Переключатель включает или выключает Управление сетевым экраном. По умолчанию переключатель выключен.
Сетевые пакетные правила	По ссылке **Настроить сетевые пакетные правила** открывается окно **Сетевые пакетные правила**. В этом окне вы можете настроить список сетевых пакетных правил, которые будет применять компонент Управление сетевым экраном при обнаружении попытки установления сетевого соединения.
Доступные сети	По ссылке **Настроить доступные сети** открывается окно **Доступные сети**. В этом окне вы можете настроить список сетей, которые будет контролировать компонент Управление сетевым экраном.
Входящие соединения	В раскрывающемся списке вы можете выбрать действие для входящих сетевых соединений: • **Разрешать** сетевые соединения (значение по умолчанию). • **Блокировать** сетевые соединения.
Входящие пакеты	В раскрывающемся списке вы можете выбрать действие для входящих пакетов: • **Разрешать** входящие пакеты (значение по умолчанию).

	• **Блокировать** входящие пакеты.
Всегда добавлять разрешающие правила для портов Агента администрирования	Флажок включает или выключает автоматическое добавление разрешающих правил для портов Агента администрирования. По умолчанию флажок установлен.

Окно Сетевые пакетные правила

Таблица **Сетевые пакетные правила** содержит сетевые пакетные правила, используемые компонентом Управление сетевым экраном для контроля сетевой активности. Для сетевых пакетных правил вы можете настроить параметры, описанные в таблице ниже.

Параметры сетевых пакетных правил

Параметр	Описание
Название	Название сетевого пакетного правила.
Действие	Действие, выполняемое компонентом Управление сетевым экраном при обнаружении сетевой активности.
Локальный адрес	Сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты.
Удаленный адрес	Сетевые адреса удаленных устройств, которые могут передавать и/или получать сетевые пакеты.
Направление	Направление отслеживаемой сетевой активности.
Протокол	Тип протокола передачи данных, для которого отслеживается сетевая активность.
Локальные порты	Номера портов локальных устройств, между которыми контролируется соединение.
Удаленные порты	Номера портов удаленных устройств, между которыми контролируется соединение.
ICMP-тип	Тип ICMP. Компонент Управление сетевым экраном контролирует сообщения указанного типа, отправляемые узлом или шлюзом.
ICMP-код	Код ICMP. Компонент Управление сетевым экраном контролирует сообщения указанного в поле **ICMP-тип** типа и с указанным в поле **ICMP-код** кодом, отправляемые узлом или шлюзом.
Запись в отчет	В столбце указано, будет ли приложение записывать в отчет действия по сетевому пакетному правилу. Если в столбце указано **Да**, приложение записывает в журнал действия по сетевому пакетному правилу. Если в столбце указано **Нет**, приложение не записывает 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 **Вниз** выбранный элемент перемещается вниз в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Сетевое пакетное правило

В этом окне вы можете настроить сетевое пакетное правило.

Параметры сетевого пакетного правила

Параметр	Описание
Название правила	Поле ввода названия сетевого пакетного правила.
Действие	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять компонент Управление сетевым экраном при обнаружении сетевой активности: • **Блокировать** сетевую активность. • **Разрешать** сетевую активность (значение по умолчанию).
Протокол	В раскрывающемся списке вы можете выбрать тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность: • **Любой** (значение по умолчанию) • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP**

	• **UDP**
Указать ICMP-тип	Флажок позволяет указать тип ICMP. Компонент Управление сетевым экраном будет контролировать 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-код	Флажок позволяет указать код ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного (в поле под флажком **Указать ICMP-тип**) типа и с указанным (в поле под флажком **Указать ICMP-код**) 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 вы можете указать направление отслеживаемой сетевой активности: • **Входящие пакеты** (значение по умолчанию). Если выбран этот элемент, компонент Управление сетевым экраном контролирует входящие пакеты. • **Входящие**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует входящую сетевую активность. • **Входящие / Исходящие**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует входящую и исходящую сетевую активность. • **Входящие / Исходящие пакеты**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует входящие и исходящие пакеты. • **Исходящие пакеты**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует исходящие пакеты. • **Исходящие**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует исходящую сетевую активность.
Удаленный адрес	В раскрывающемся списке вы можете указать сетевые адреса удаленных устройств, которые могут передавать и получать сетевые пакеты: • **Любой адрес** (значение по умолчанию). Если выбран этот элемент, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с любым IP-адресом. • **Все адреса подсети**. Если выбран этот элемент, сетевое правило контролирует сетевые пакеты, отправляемые и получаемые удаленными устройствами с IP-адресами, которые относятся к выбранному ниже типу сети: **Публичные сети**, **Локальные сети** или **Доверенные сети**. • **Определенный адрес**. Если выбран этот элемент, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с IP-адресами, указанными в поле ввода **Адрес**.

Указать удаленные порты	Флажок позволяет указать номера портов удаленных устройств, 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 раскрывающемся списке вы можете указать сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты: • **Любой адрес** (значение по умолчанию). Если выбран этот элемент, сетевое правило контролирует отправку и получение сетевых пакетов устройствами с установленным приложением Kaspersky Endpoint Security и любым IP-адресом. • **Определенный адрес**. Если выбран этот элемент, сетевое правило контролирует указанные в поле **Адрес** сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты.
Указать локальные порты	Флажок позволяет указать номера портов локальных устройств, 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, приложение записывает в отчет действия по сетевому правилу. Если флажок снят, приложение не записывает в отчет действия по сетевому правилу. По умолчанию флажок снят.

Окно Доступные сети

Таблица **Доступные сети** содержит сети, контролируемые компонентом Управление сетевым экраном. По умолчанию таблица доступных сетей пустая.

Параметры доступных сетей

Параметр	Описание
IP-адрес	IP-адрес сети.
Тип сети	Тип сети (**Публичная сеть**, **Локальная сеть** или **Доверенная сеть**).

Вы можете добавлять, изменять и удалять доступные сети.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Сетевое соединение

В этом окне вы можете настроить сетевое соединение, которое будет контролировать компонент Управление сетевым экраном.

Сетевое соединение

Параметр	Описание
IP-адрес	Поле ввода IP-адреса сети.
Тип сети	Вы можете выбрать тип сети: • **Публичная сеть**. • **Локальная сеть**. • **Доверенная сеть**.

Управление сетевым экраном в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры управления сетевым экраном в свойствах политики (**Базовая защита** → **Управление сетевым экраном**).

Параметры компонента Управление сетевым экраном

Параметр	Описание
Включить Управление сетевым экраном	Флажок включает или выключает компонент Управление сетевым экраном. По умолчанию флажок снят.
Сетевые пакетные правила	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Сетевые пакетные правила**. В этом окне вы можете настроить сетевые пакетные правила, которые будет применять компонент Управление сетевым экраном при обнаружении попытки установления сетевого соединения.
Доступные сети	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доступные сети**. В этом окне вы можете настроить список сетей, которые будет контролировать компонент Управление сетевым экраном.
Входящие соединения	В раскрывающемся списке вы можете выбрать действие для входящих сетевых соединений: • **Разрешать** сетевые соединения (значение по умолчанию). • **Блокировать** сетевые соединения.

Входящие пакеты	В раскрывающемся списке вы можете выбрать действие для входящих пакетов: • **Разрешать** входящие пакеты (значение по умолчанию). • **Блокировать** входящие пакеты.
Всегда добавлять разрешающие правила для портов Агента администрирования	Флажок включает или выключает автоматическое добавление разрешающих правил для портов Агента администрирования. По умолчанию флажок установлен.

Окно Сетевые пакетные правила

Таблица **Сетевые пакетные правила** содержит сетевые пакетные правила, используемые компонентом Управление сетевым экраном для контроля сетевой активности. Для сетевых пакетных правил вы можете настроить параметры, описанные в таблице ниже.

Параметры сетевых пакетных правил

Параметр	Описание
Название	Название сетевого пакетного правила.
Действие	Действие, выполняемое компонентом Управление сетевым экраном при обнаружении сетевой активности.
Локальный адрес	Сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты.
Удаленный адрес	Сетевые адреса удаленных устройств, которые могут передавать и/или получать сетевые пакеты.
Запись в отчет	В столбце указано, будет ли приложение записывать в отчет действия по сетевому пакетному правилу. Если в столбце указано **Да**, приложение записывает в журнал действия по сетевому пакетному правилу. Если в столбце указано **Нет**, приложение не записывает 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 **Вниз** выбранный элемент перемещается вниз в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Добавление сетевого пакетного правила

В этом окне вы можете настроить параметры добавляемого сетевого пакетного правила.

Параметры сетевого пакетного правила

Параметр	Описание
Протокол	Вы можете выбрать тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность: • **Любой** (значение по умолчанию) • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP** • **UDP**
Направление	Вы можете указать направление отслеживаемой сетевой активности: • **Входящие пакеты**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует входящие пакеты. • **Входящие**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует входящую сетевую активность. • **Входящие / Исходящие**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует входящую и исходящую сетевую активность. • **Входящие / Исходящие пакеты**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует входящие и исходящие пакеты. • **Исходящие пакеты**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует исходящие пакеты.

	• **Исходящие**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует исходящую сетевую активность.
ICMP-тип	Вы можете указать тип ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного типа, отправляемые узлом или шлюзом. Если выбран вариант **Определенный**, отображается поле для ввода типа ICMP. Окно отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **ICMP** или **ICMPv6**.
ICMP-код	Вы можете указать код ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного в поле **ICMP-тип** типа и с указанным в поле **ICMP-код** кодом, отправляемые узлом или шлюзом. Если выбран вариант **Определенный**, отображается поле для ввода кода ICMP. Окно отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **ICMP** или **ICMPv6**.
Удаленные порты	Вы можете указать номера портов удаленных устройств, между которыми требуется контролировать соединение. Если выбран вариант **Определенный**, отображается поле для ввода номеров портов. Окно отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **TCP** или **UDP**.
Локальные порты	Вы можете указать номера портов локальных устройств, между которыми требуется контролировать соединение. Если выбран вариант **Определенный**, отображается поле для ввода номеров портов. Окно отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **TCP** или **UDP**.
Удаленные адреса	Вы можете указать сетевые адреса удаленных устройств, которые могут передавать и получать сетевые пакеты: • **Любой адрес** (значение по умолчанию). Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с любым IP-адресом. • **Определенный адрес**. Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с IP-адресами, указанными в поле ввода ниже. • **По типу сети**. Если выбран этот вариант, сетевое правило контролирует сетевые пакеты, отправляемые и получаемые удаленными устройствами с IP-адресами, которые относятся к выбранному ниже типу сетей: **Публичные сети**, **Локальные сети** или **Доверенные сети**.
Локальные адреса	Вы можете указать сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты: • **Любой адрес** (значение по умолчанию). Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов устройствами с установленным приложением Kaspersky Endpoint Security и любым IP-адресом. • **Определенный адрес**. Если выбран этот вариант, сетевое правило контролирует указанные в поле ниже сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты.
Действие	Вы можете выбрать действие, которое будет выполнять компонент Управление

	сетевым экраном при обнаружении сетевой активности: • **Блокировать** сетевую активность. • **Разрешать** сетевую активность (значение по умолчанию).
Запись в отчет	Вы можете указать, будут ли действия по сетевому правилу записываться в отчет.
Название правила	Поле ввода названия сетевого пакетного правила.

Окно Доступные сети

Таблица **Доступные сети** содержит сети, контролируемые компонентом Управление сетевым экраном. По умолчанию таблица доступных сетей пустая.

Параметры доступных сетей

Параметр	Описание
IP-адрес	IP-адрес сети.
Тип сети	Тип сети (**Публичная сеть**, **Локальная сеть** или **Доверенная сеть**).

Вы можете добавлять, изменять и удалять доступные сети.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Сетевое соединение

В этом окне вы можете настроить сетевое соединение, которое будет контролировать компонент Управление сетевым экраном.

Сетевое соединение

Параметр	Описание
IP-адрес	Поле ввода IP-адреса сети.
Тип сети	Вы можете выбрать тип сети: • **Публичная сеть**. • **Локальная сеть**.

	• **Доверенная сеть**.

Управление сетевым экраном в командной строке

В командной строке вы можете настраивать управление сетевым экраном с помощью предустановленной задачи Управление сетевым экраном (*Firewall_Management*).

По умолчанию задача Управление сетевым экраном не запущена. Вы можете запускать и останавливать эту задачу вручную.

Вы можете настраивать параметры управления сетевым экраном, изменяя параметры предустановленной задачи с помощью команды управления параметрами задач.

Вы также можете настраивать параметры управления сетевым экраном с помощью команд управления сетевым экраном:

- Создавать и удалять сетевые пакетные правила и изменять приоритет их выполнения.
- Формировать список IP-адресов или подсетей в сетевых зонах.
- Просматривать созданные в приложении Kaspersky Endpoint Security правила сетевого экрана с помощью команды `kesl-control -F --query`.

Параметры задачи Управление сетевым экраном

Параметр	Описание	Значения
`DefaultIncomingAction`	Действие по умолчанию, применяемое ко входящему соединению, если другие сетевые правила не применяются к этому виду соединения.	`Allow` (значение по умолчанию) – разрешать входящие соединения. `Block` – запрещать входящие соединения.
`DefaultIncomingPacketAction`	Действие по умолчанию, применяемое ко входящему пакету, если другие сетевые пакетные правила не применяются к этому виду соединения.	`Allow` (значение по умолчанию) – разрешать входящие пакеты. `Block` – запрещать входящие пакеты.
`OpenNagentPorts`	Добавление динамических правил для Агента администрирования в пакетные правила.	`Yes` (значение по умолчанию) – добавлять динамические правила для Агента администрирования в пакетные правила. `No` – не добавлять динамические правила для Агента администрирования в пакетные правила.
Секция **[PacketRules.item_#]** содержит сетевые пакетные правила для задачи Управление сетевым экраном. Вы можете указать несколько секций `[PacketRules.item_#]` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.		

Каждая секция [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.	Allow (значение по умолчанию) – разрешать сетевые соединения. Block – запрещать сетевые соединения.
Protocol	Тип протокола, для которого необходим мониторинг сетевой активности.	Any (значение по умолчанию) – задача Управление сетевым экраном контролирует всю сетевую активность. TCP UDP ICMP ICMPv6 IGMP GRE
RemotePorts	Номера портов удаленных устройств, соединение между которыми отслеживается. Вы можете указать значение в виде целого числа или в виде интервала. Этот параметр можно указать, только если для параметра Protocol установлено значение TCP или UDP.	Any (значение по умолчанию) – контролировать все удаленные порты. 0 – 65535.
LocalPorts	Номера портов локальных устройств, соединение между которыми отслеживается. Вы можете указать значение в виде целого числа или в виде интервала. Этот параметр можно указать, только если для параметра Protocol установлено значение TCP или UDP.	Any (значение по умолчанию) – контролировать все локальные порты. 0 – 65535.
ICMPType	Тип пакета ICMP. Этот параметр можно указать, только если для параметра Protocol установлено значение ICMP или ICMPv6.	Any (значение по умолчанию) – контролировать все типы пакетов ICMP. Целое число согласно спецификации протокола передачи данных.
ICMPCode	Код пакета ICMP.	Any (значение по умолчанию) –

	Этот параметр можно указать, только если для параметра `Protocol` установлено значение `ICMP` или `ICMPv6`.	контролировать все коды пакетов ICMP. Целое число согласно спецификации протокола передачи данных.
`Direction`	Направление отслеживаемой сетевой активности.	`IncomingOutgoing` или `InOut` (значение по умолчанию) – 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.
`RemoteAddress`	Сетевые адреса удаленных устройств, которые могут передавать и получать сетевые пакеты.	`Any` (значение по умолчанию) – контролируется отправка и / или получение сетевых пакетов удаленными устройствами 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.
`LocalAddress`	Сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты.	`Any` (значение по умолчанию) – контролируется отправка и / или получение сетевых пакетов локальными устройствами 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.
`LogAttempts`	Включение записи в отчет действия сетевого правила.	`Yes` – записывать действия в отчет. `No` (значение по умолчанию) – не записывать действия в отчет.
Секция **[NetworkZonesPublic]** содержит сетевые адреса, связанные с публичными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		
`Address.item_#`	Указывает IP-адрес или IP-подсеть.	`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).
Секция **[NetworkZonesLocal]** содержит сетевые адреса, связанные с локальными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		
`Address.item_#`	Указывает IP-адрес или IP-подсеть.	`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).
Секция **[NetworkZonesTrusted]** содержит сетевые адреса, связанные с доверенными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		
`Address.item_#`	Указывает IP-адрес или IP-подсеть.	`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).

Настройка списка сетевых пакетных правил в командной строке

Чтобы добавить сетевое пакетное правило, выполните следующую команду:

```
kesl-control --add-rule [--name <название правила>] [--action <действие>] [--protocol
<протокол>] [--direction <направление>] [--remote <удаленный адрес>[:<диапазон
портов>]] [--local <локальный адрес>[:<диапазон портов>]] [--at <индекс>]
```

где:

- `--name <название правила>` – название сетевого пакетного правила.
- `--action <действие>` – действие, применяемое к соединениям, указанным в сетевом пакетном правиле.
- `--protocol <протокол>` – тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность.

- `--direction <направление>` – направление отслеживаемой сетевой активности.
- `--remote <удаленный адрес[:<диапазон портов>]>` – сетевой адрес удаленного устройства. Вы можете указать имя предустановленной сетевой зоны в качестве удаленного адреса.
- `--local <локальный адрес[:<диапазон портов>]>` – сетевой адрес устройства с установленным приложением Kaspersky Endpoint Security.
- `--at <индекс>` – индекс правила в списке сетевых пакетных правил. Если ключ `--at` не указан или его значение больше количества правил в списке, новое правило добавляется в конец списка.

Для параметров, значения которых вы не указали в команде, устанавливаются значения по умолчанию.

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
```

Чтобы удалить сетевое пакетное правило, выполните одну из следующих команд:

- `kesl-control --del-rule --name <название правила>`
- `kesl-control --del-rule --index <индекс>`

где:

- `--name <название правила>` – название сетевого пакетного правила.
- `--index <индекс>` – текущий индекс правила в списке сетевых пакетных правил.

Если список сетевых пакетных правил содержит несколько правил с одинаковым именем или не содержит правило с указанным именем или индексом, происходит ошибка.

Чтобы изменить приоритет выполнения сетевого пакетного правила, выполните одну из следующих команд:

- `kesl-control --move-rule --name <название правила> --at <индекс>`
- `kesl-control --move-rule --index <индекс> --at <индекс>`

где:

- `--name <название правила>` – название сетевого пакетного правила.
- `--index <индекс>` – текущий индекс правила в списке сетевых пакетных правил.
- `--at <индекс>` – новый индекс правила в списке сетевых пакетных правил.

Настройка сетевых зон в командной строке

Чтобы добавить сетевой адрес в зону, выполните следующую команду:

```
kesl-control --add-zone --zone <зона> --address <адрес>
```

где:

- `--zone <зона>` – предустановленное имя сетевой зоны. Возможные значения: `Public`, `Local`, `Trusted`.
- `--address <адрес>` – сетевой адрес или подсеть.

Чтобы удалить сетевой адрес из зоны, выполните одну из следующих команд:

- `kesl-control --del-zone --zone <зона> --address <адрес>`
- `kesl-control --del-zone --zone <зона> --index <индекс адреса в зоне>`

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.

Защита от веб-угроз

Компонент Защита от веб-угроз позволяет проверять входящий трафик, передаваемый по протоколам HTTP, HTTPS и FTP, веб-сайты и IP-адреса, предотвращать загрузку вредоносных файлов из интернета, а также блокировать доступ к фишинговым, рекламным и прочим опасным веб-сайтам.

Эта функциональность не поддерживается в KESL-контейнере.

Текущие соединения для перехватываемых TCP-портов сбрасываются при включении Защиты от сетевых угроз.

По умолчанию Защита от веб-угроз выключена. При этом она включается автоматически, если на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен) и в системе обнаружен один из следующих исполняемых файлов браузеров, в том числе и snap-формата:

- chrome;
- chromium;
- chromium-browser;
- firefox;
- firefox-esr;
- google-chrome;
- opera;
- yandex-browser.

Вы можете включать и выключать Защиту от веб-угроз, а также настраивать параметры защиты:

- Выбирать действие, которое приложение будет выполнять над веб-ресурсом, на котором обнаружен опасный объект.
- Настраивать список доверенных веб-адресов. Приложение не проверяет содержание веб-сайтов, веб-адреса которых указаны в этом списке.
- Выбирать объекты, которые приложение будет обнаруживать во время проверки входящего трафика.
- Настраивать проверку защищенных соединений для проверки HTTPS-трафика.

  Для проверки FTP-трафика в параметрах проверки защищенных соединений должен быть настроен контроль всех сетевых портов.

При открытии веб-сайта приложение выполняет следующие действия:

1. Проверяет надежность веб-сайта с помощью загруженных баз приложения.
2. Проверяет надежность веб-сайта с помощью эвристического анализа, если он включен.

Во время эвристического анализа приложение Kaspersky Endpoint Security анализирует активность приложений в операционной системе. Эвристический анализ может обнаружить опасные объекты, о которых нет записей в базах приложения Kaspersky Endpoint Security.

3. Проверяет надежность веб-сайта с помощью репутационных баз "Лаборатории Касперского", если включено использование Kaspersky Security Network.

Рекомендуется включить использование Kaspersky Security Network, чтобы увеличить эффективность защиты от веб-угроз.

4. Запрещает или разрешает открыть веб-сайт.

При попытке открытия опасного веб-сайта приложение выполняет следующие действия:

- Для HTTP- или FTP-трафика приложение блокирует доступ и показывает предупреждение.
- Для HTTPS-трафика в браузере отображается страница с ошибкой.

Удаление сертификатов приложения может привести к некорректной работе компонента Защита от веб-угроз.

Приложение Kaspersky Endpoint Security добавляет в список таблицы mangle утилит iptables и ip6tables специальную разрешающую цепочку правил kesl_bypass, которая позволяет исключать трафик из проверки приложением. Если в цепочке настроены правила исключения трафика, они влияют на работу компонента Защита от веб-угроз.

Настройка защиты от веб-угроз в Web Console

В Web Console вы можете настраивать параметры защиты от веб-угроз в свойствах политики (**Параметры приложения** → **Базовая защита** → **Защита от веб-угроз**).

Параметры компонента Защита от веб-угроз

Параметр	Описание
Защита от веб-угроз включена / выключена	Переключатель включает или выключает компонент Защита от веб-угроз. По умолчанию переключатель выключен.
Действие при обнаружении угрозы	В этом разделе вы можете указать действие, которое приложение будет выполнять над веб-ресурсом, на котором обнаружен опасный объект: • **Информировать** пользователя при обнаружении опасного объекта в веб-трафике. Защита от веб-угроз позволяет выполнить загрузку объекта на устройство. При этом приложение записывает в журнал и добавляет в список активных угроз информацию об опасном объекте. • **Блокировать** доступ ко всем опасным объектам, обнаруженным в веб-трафике, показывать уведомление о заблокированных попытках доступа и записывать в журнал информацию об опасных объектах (значение по умолчанию).

Обнаруживать вредоносные объекты	Флажок включает или выключает проверку ссылок по базе вредоносных веб-адресов. По умолчанию флажок установлен.
Обнаруживать фишинговые ссылки	Флажок включает или выключает проверку ссылок по базе фишинговых веб-адресов. По умолчанию флажок установлен.
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 приложения	Флажок включает или выключает проверку ссылок по базе рекламных веб-адресов. По умолчанию флажок снят.
Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным	Флажок включает или выключает проверку ссылок по базе легальных приложений, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. По умолчанию флажок снят.
Доверенные веб-адреса	Таблица содержит веб-адреса и веб-страницы, содержимое которых вы считаете доверенным. В список доверенных веб-адресов вы можете добавлять только веб-адреса HTTP/HTTPS. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается. При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html). По умолчанию таблица пуста. Вы можете добавлять, изменять и удалять веб-адреса в таблице. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Веб-адрес

В этом окне вы можете добавить веб-адрес или маску веб-адресов в список доверенных веб-адресов.

В список доверенных веб-адресов можно добавлять только веб-адреса HTTP / HTTPS. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается.

При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html).

Настройка защиты от веб-угроз в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от веб-угроз в свойствах политики (**Базовая защита** → **Защита от веб-угроз**).

Параметры компонента Защита от веб-угроз

Параметр	Описание
Включить Защиту от веб-угроз	Флажок включает или выключает компонент Защита от веб-угроз. По умолчанию флажок снят.
Доверенные веб-адреса	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные веб-адреса**, в котором вы можете указать список доверенных веб-адресов. Приложение не проверяет содержание веб-сайтов, веб-адреса которых указаны в этом списке.
Действие при обнаружении угрозы	Действие, которое приложение будет выполнять над веб-ресурсом, на котором обнаружен опасный объект: • **Блокировать** доступ ко всем опасным объектам, обнаруженным в веб-трафике, показывать уведомление о заблокированных попытках доступа и записывать в журнал информацию об опасных объектах (значение по умолчанию). • **Информировать** пользователя при обнаружении опасного объекта в веб-трафике. Защита от веб-угроз позволяет выполнить загрузку объекта на устройство. При этом приложение записывает в журнал и добавляет в список активных угроз информацию об опасном объекте.
Параметры проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Параметры проверки**, в котором вы можете настроить параметры проверки входящего трафика.

Окно Доверенные веб-адреса

В этом окне вы можете добавить веб-адреса и веб-страницы, содержимое которых вы считаете доверенным.

В список доверенных веб-адресов вы можете добавлять только веб-адреса HTTP / HTTPS. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается. По умолчанию список пустой.

При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html).

Вы можете добавлять, изменять и удалять веб-адреса в списке.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Веб-адрес

В этом окне вы можете добавить веб-адрес или маску веб-адресов в список доверенных веб-адресов.

В список доверенных веб-адресов можно добавлять только веб-адреса HTTP / HTTPS. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается.

При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html).

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки входящего трафика во время работы компонента Защита от веб-угроз.

Параметры Защиты от веб-угроз

Параметр	Описание
Обнаруживать вредоносные объекты	Флажок включает или выключает проверку ссылок по базе вредоносных веб-адресов. По умолчанию флажок установлен.
Обнаруживать фишинговые ссылки	Флажок включает или выключает проверку ссылок по базе фишинговых веб-адресов. По умолчанию флажок установлен.
Использовать эвристический анализ для обнаружения фишинговых ссылок	Флажок включает или выключает использование эвристического анализа для обнаружения фишинговых ссылок. Флажок доступен и установлен по умолчанию, если установлен флажок **Обнаруживать фишинговые ссылки**.
Обнаруживать рекламные приложения	Флажок включает или выключает проверку ссылок по базе рекламных веб-адресов. По умолчанию флажок снят.
Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным	Флажок включает или выключает проверку ссылок по базе легальных приложений, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. По умолчанию флажок снят.

Настройка защиты от веб-угроз в командной строке

В командной строке вы можете управлять защитой от веб-угроз с помощью предустановленной задачи Защита от веб-угроз (*Web_Threat_Protection*).

Задача запускается автоматически, если в системе обнаружен один из поддерживаемых браузеров и на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен).

Вы можете запускать и останавливать задачу вручную. Вы можете настраивать параметры защиты от веб-угроз, изменяя параметры предустановленной задачи Защита от веб-угроз.

Параметры задачи Защита от веб-угроз

Параметр	Описание	Значения
`ActionOnDetect`	Действия, выполняемые при обнаружении зараженного объекта в веб-трафике.	`Notify` – разрешить загрузку обнаруженного объекта, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.

		`Block` (значение по умолчанию) – запретить доступ к обнаруженному объекту, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.
`CheckMalicious`	Включает или выключает проверку ссылок по базе вредоносных веб-адресов.	`Yes` (значение по умолчанию) – проверять ссылки на вхождение в базу вредоносных веб-адресов. `No` – не проверять ссылки на вхождение в базу вредоносных веб-адресов.
`CheckPhishing`	Включает или выключает проверку ссылок по базе фишинговых веб-адресов.	`Yes` (значение по умолчанию) – проверять ссылки на вхождение в базу фишинговых веб-адресов. `No` – не проверять ссылки на вхождение в базу фишинговых веб-адресов.
`UseHeuristicForPhishing`	Включает или выключает использование эвристического анализа для проверки веб-страниц на наличие фишинговых ссылок.	`Yes` (значение по умолчанию) – использовать эвристический анализ для обнаружения фишинговых ссылок. Если выбрано это значение, используется поверхностный уровень эвристического анализа – `Light` (наименее тщательная проверка, минимальная загрузка системы). Для задачи Защита от веб-угроз невозможно изменить уровень эвристического анализа. `No` – не использовать эвристический анализ для обнаружения фишинговых ссылок.
`CheckAdware`	Включает или выключает проверку ссылок по базе рекламных веб-адресов.	`Yes` – проверять ссылки на вхождение в базу рекламных веб-адресов. `No` (значение по умолчанию) – не проверять ссылки на вхождение в базу рекламных веб-адресов.
`CheckOther`	Включает или выключает проверку ссылок по базе веб-адресов, содержащих легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.	`Yes` – проверять ссылки на вхождение в базу веб-адресов, содержащих легальные приложения, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. `No` (значение по умолчанию) – не проверять ссылки на вхождение в базу веб-адресов, содержащих легальные приложения, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным.
`UseTrustedAddresses`	Включает или выключает использование списка доверенных веб-адресов. Приложение не проверяет доверенные веб-адреса на вирусы и другие вредоносные объекты. Вы можете указать доверенные	`Yes` (значение по умолчанию) – использовать список доверенных веб-адресов. `No` – не использовать список доверенных веб-адресов.

	веб-адреса с помощью параметра `TrustedAddresses.item_#`.	
`TrustedAddresses.item_#`	Доверенные веб-адреса.	Значение по умолчанию не задано. Для указания веб-адресов вы можете использовать маски. При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html). Использование масок для указания IP-адресов не поддерживается.

Проверка защищенных соединений

Параметры проверки защищенных соединений используются в работе компонентов Защита от веб-угроз и Веб-Контроль. Компонент Защита от веб-угроз может расшифровывать и проверять сетевой трафик, передаваемый по защищенным соединениям. По умолчанию проверка защищенных соединений включена.

Вы можете включать и выключать проверку защищенных соединений, а также настраивать параметры проверки:

- Выбирать действие, выполняемое приложением при обнаружении недоверенного сертификата.
- Выбирать действие, выполняемое приложением при возникновении ошибки проверки защищенных соединений на веб-сайте.
- Включать и выключать использование интернета при проверке сертификатов.
- Просматривать и настраивать список доверенных доменов. Приложение не будет проверять защищенные соединения, установленные при посещении указанных доменов.
- Настраивать список сертификатов, которые приложение будет считать доверенными во время проверки защищенных соединений.
- Настраивать список сетевых портов, контролируемых приложением. Вы можете указывать определенные сетевые порты или диапазоны сетевых портов для проверки.

При изменении параметров проверки защищенных соединений приложение формирует событие *NetworkSettingsChanged*.

Настройка проверки защищенных соединений в Web Console

В Web Console вы можете настраивать параметры проверки защищенных соединений в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры сети**).

Параметры проверки защищенных соединений

Параметр	Описание
Проверка защищенных соединений включена / выключена	Переключатель включает или выключает проверку защищенных соединений. По умолчанию переключатель включен.
Доверенные корневые сертификаты	По ссылке **Управлять доверенными корневыми сертификатами** открывается окно **Доверенные корневые сертификаты**, в котором вы можете настроить список доверенных сертификатов. Доверенные сертификаты используются при проверке защищенных соединений.
Переход на домен с недоверенным сертификатом	Вы можете выбрать действие, которое приложение будет выполнять при переходе на домен с недоверенным сертификатом: • **Разрешать** (значение по умолчанию) – разрешать подключение к домену с недоверенным сертификатом.

	• **Блокировать** – блокировать подключение к домену с недоверенным сертификатом.
Переход на домен с ошибкой проверки защищенных соединений	Вы можете выбрать действие, которое приложение будет выполнять при переходе на домен с ошибкой проверки защищенных соединений: • **Разрешать и добавлять домен в исключения** (значение по умолчанию) – добавить домен, вызвавший ошибку, в список доменов с ошибками при проверке и не проверять зашифрованный сетевой трафик при посещении этого домена. • **Блокировать** – блокировать подключение к домену с ошибкой проверки.
Политика проверки сертификатов	Вы можете выбрать способ проверки сертификатов приложением: • **Локальная проверка** – приложение не использует интернет для проверки сертификата. • **Полная проверка** (значение по умолчанию) – приложение использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.
Доверенные домены	По ссылке **Настроить доверенные домены** открывается окно **Доверенные домены**, в котором вы можете настроить список имен доверенных доменов.
Контролировать все сетевые порты	Если выбран этот вариант, приложение проверяет все сетевые порты.
Контролировать только выбранные сетевые порты	Если выбран этот вариант, приложение проверяет только сетевые порты, указанные в окне **Контролируемые порты**. Этот вариант выбран по умолчанию.
Контролируемые порты	По ссылке **Настроить параметры сетевых портов** открывается окно **Контролируемые порты**, в котором вы можете указать, какие сетевые порты будет проверять приложение.

Окно Доверенные корневые сертификаты

Вы можете настроить список сертификатов, которые приложение Kaspersky Endpoint Security будет считать доверенными. Список доверенных сертификатов используется при проверке зашифрованных соединений.

Для каждого сертификата отображаются следующие сведения:

- субъект сертификата;
- серийный номер;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;

- отпечаток сертификата SHA256.

По умолчанию список сертификатов пуст.

Вы можете добавлять и удалять сертификаты.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно добавления доверенного сертификата

В этом окне вы можете добавить сертификат, который приложение Kaspersky Endpoint Security будет считать доверенным.

По ссылке **Добавить сертификат** открывается стандартное окно для выбора файла. Укажите путь к файлу формата DER или PEM, содержащему сертификат.

После выбора файла сертификата в окне отображается информация о сертификате и путь к файлу.

Окно Доверенные домены

Список содержит доменные имена и маски доменных имен, которые будут исключены из проверки зашифрованных соединений.

Пример: `*example.com`. Например, `*example.com/*` – это неправильное значение, так как требуется указывать адрес домена, а не веб-страницы.

По умолчанию список пуст.

Вы можете добавлять, изменять и удалять домены в списке доверенных доменов.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Контролируемые порты

Таблица содержит сетевые порты, которые будет проверять приложение, если в окне **Параметры сети** в блоке **Контролируемые порты** выбран вариант **Контролировать только выбранные сетевые порты**.

Таблица содержит два столбца:

- **Порт** – контролируемый порт.
- **Описание** – описание контролируемого порта.

По умолчанию в таблице отображается список сетевых портов, которые обычно используются для передачи почтового и сетевого трафика. Список сетевых портов входит в пакет приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Настройка проверки защищенных соединений в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры проверки защищенных соединений в свойствах политики (**Общие параметры** → **Параметры сети**).

Параметры проверки защищенных соединений

Параметр	Описание
Включить проверку защищенных соединений	Флажок включает или выключает проверку защищенных соединений. По умолчанию флажок установлен.
Переход на домен с недоверенным сертификатом	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять при переходе на домен с недоверенным сертификатом: • **Разрешать** (значение по умолчанию) – разрешать подключение к домену с недоверенным сертификатом. • **Блокировать** – блокировать подключение к домену с недоверенным сертификатом.
Переход на домен с ошибкой проверки защищенных соединений	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять при переходе на домен с ошибкой проверки защищенных соединений:

	• **Добавлять домен в исключения** (значение по умолчанию) – добавить домен, вызвавший ошибку, в список доменов с ошибками при проверке и не проверять зашифрованный сетевой трафик при посещении этого домена. • **Блокировать** – блокировать подключение к домену с ошибкой проверки.
Политика проверки сертификатов	В раскрывающемся списке вы можете выбрать способ проверки сертификатов приложением: • **Локальная проверка** – приложение не использует интернет для проверки сертификата. • **Полная проверка** (значение по умолчанию) – приложение использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.
Доверенные домены	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные домены**, в котором вы можете настроить список имен доверенных доменов.
Доверенные корневые сертификаты	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные корневые сертификаты**, в котором вы можете настроить список доверенных сертификатов. Доверенные сертификаты используются при проверке защищенных соединений.
Параметры сетевых портов	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Контролируемые порты**.

Окно Доверенные домены

Список содержит доменные имена и маски доменных имен, которые будут исключены из проверки зашифрованных соединений.

Пример: `*example.com`. Например, `*example.com/*` – это неправильное значение, так как требуется указывать адрес домена, а не веб-страницы.

По умолчанию список пуст.

Вы можете добавлять, изменять и удалять домены в списке доверенных доменов.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Доверенные корневые сертификаты

Вы можете настроить список сертификатов, которые приложение Kaspersky Endpoint Security будет считать доверенными. Список доверенных сертификатов используется при проверке зашифрованных соединений.

Для каждого сертификата отображаются следующие сведения:

- **Субъект** – субъект сертификата;
- **Серийный номер** – серийный номер сертификата;
- **Издатель** – издатель сертификата;
- **Действует с** – дата начала срока действия сертификата;
- **Действует до** – дата окончания срока действия сертификата;
- **Отпечаток SHA256** – отпечаток сертификата SHA256.

По умолчанию список сертификатов пуст.

Вы можете добавлять и удалять сертификаты.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно Добавление сертификата

В этом окне вы можете добавить сертификат в список доверенных сертификатов одним из следующих способов:

- Указать путь к файлу сертификата. По кнопке **Обзор** открывается стандартное окно для выбора файла. Укажите путь к файлу формата DER или PEM, содержащему сертификат.
- Скопировать содержимое файла сертификата в поле **Ввести данные сертификата**.

Окно Контролируемые порты

Параметры сетевых портов

Параметр	Описание
Контролировать все сетевые порты	Если выбран этот вариант, приложение проверяет все сетевые порты.
Контролировать только выбранные сетевые порты	Если выбран этот вариант, приложение проверяет только сетевые порты, указанные в таблице.

	Этот вариант выбран по умолчанию.
Параметры сетевых портов	Таблица содержит сетевые порты, которые будет проверять приложение, если выбран вариант **Контролировать только указанные порты**. Таблица содержит два столбца: • **Порт** – контролируемый порт. • **Описание** – описание контролируемого порта. По умолчанию в таблице отображается список сетевых портов, которые обычно используются для передачи почтового и сетевого трафика. Список сетевых портов входит в пакет приложения. Элементы в таблице можно добавлять, изменять и удалять. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Настройка проверки защищенных соединений в командной строке

В командной строке для управления параметрами проверки защищенных соединений предусмотрены специальные команды управления. С помощью команд управления параметрами проверки защищенных соединений вы можете:

- Настраивать параметры проверки защищенных соединений.
- Просматривать исключения из проверки защищенных соединений.
- Очищать список доменов, которые приложение автоматически исключило из проверки.
- Управлять списком сертификатов, которые приложение считает доверенными.

Просмотр и изменение параметров проверки защищенных соединений

Вы можете просматривать и изменять параметры проверки защищенных соединений с помощью специальных команд управления:

- Вы можете выводить текущие значения параметров проверки защищенных соединений в консоль или в конфигурационный файл. Этот файл вы можете использовать для изменения параметров.

- Вы можете изменять все параметры проверки защищенных соединений, используя конфигурационный файл, который содержит параметры. Конфигурационный файл вы можете получить с помощью команды вывода параметров проверки защищенных соединений.

- Вы можете изменять отдельные параметры, используя ключи командной строки в формате `< имя параметра >=< значение параметра >`. Текущие значения параметров вы можете получить с помощью команды вывода параметров проверки защищенных соединений.

Чтобы вывести в консоль текущие значения параметров проверки защищенных соединений, выполните следующую команду:

```
kesl-control --get-net-settings [--json]
```

где `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Чтобы вывести в файл текущие значения параметров проверки защищенных соединений, выполните следующую команду:

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

где:

- `--file < путь к конфигурационному файлу >` – путь к файлу, в который будут сохранены параметры проверки защищенных соединений. Если вы укажете имя файла, не указав путь 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, файл не будет создан.

- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Чтобы изменить значения параметров проверки защищенных соединений с помощью конфигурационного файла:

1. Выведите общие параметры приложения в конфигурационный файл, как описано выше.

2. Измените значения нужных параметров в файле и сохраните изменения.

3. Выполните команду:

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

   где:

   - `--file < путь к конфигурационному файлу >` – полный путь к конфигурационному файлу с параметрами проверки защищенных соединений.

   - `--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

   Все значения параметров проверки защищенных соединений, заданные в файле, будут импортированы в приложение.

Чтобы изменить значения параметров проверки защищенных соединений с помощью командной строки, выполните следующую команду:

```
kesl-control --set-net-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где <имя параметра>=<значение параметра> – имя и значение одного из параметров проверки защищенных соединений.

Значения указанных параметров проверки защищенных соединений будут изменены.

Просмотр исключений из проверки защищенных соединений

Вы можете просматривать следующие списки исключений из проверки защищенных соединений:

- список исключений, добавленных пользователем;
- список исключений, добавленных приложением;
- список исключений, полученных из баз приложения.

Чтобы просмотреть список исключений из проверки защищенных соединений, добавленных пользователем, выполните следующую команду:

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

Чтобы просмотреть список исключений из проверки защищенных соединений, добавленных приложением, выполните следующую команду:

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

Чтобы просмотреть список исключений из проверки защищенных соединений, полученных из баз приложения, выполните следующую команду:

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

Чтобы очистить список доменов, которые приложение автоматически исключило из проверки, выполните следующую команду:

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

Управление списком доверенных сертификатов

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

```
kesl-control --add-certificate <путь к сертификату>
```

где:

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

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

```
kesl-control --remove-certificate <субъект сертификата>
```

Чтобы просмотреть список доверенных сертификатов, выполните следующую команду:

```
kesl-control --list-certificates
```

Для каждого сертификата отображается следующая информация:

- субъект сертификата;
- серийный номер;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- отпечаток сертификата SHA256.

Защита от сетевых угроз

Компонент Защита от сетевых угроз позволяет проверять входящий сетевой трафик на действия, характерные для сетевых атак.

Эта функциональность не поддерживается в KESL-контейнере.

Приложение проверяет входящий трафик для TCP-портов, номера которых приложение Kaspersky Endpoint Security получает из актуальных баз приложения.

Для проверки сетевого трафика задача Защита от сетевых угроз принимает подключения по всем портам, номера которых получает из баз приложения. При проверке сети это может выглядеть как открытый порт на устройстве, даже если никакое приложение в системе его не прослушивает. Неиспользуемые порты рекомендуется закрывать средствами сетевого экрана.

Текущие соединения для перехватываемых TCP-портов сбрасываются при включении Защиты от сетевых угроз.

Если Защита от сетевых угроз включена, при обнаружении попытки сетевой атаки на защищаемое устройство приложение блокирует сетевую активность со стороны атакующего устройства и создает событие *Обнаружена сетевая атака*. Событие содержит информацию об атакующем устройстве.

По умолчанию сетевой трафик со стороны атакующего устройства блокируется на один час. По истечении времени блокировки приложение разблокирует устройство.

Защита от сетевых угроз включена по умолчанию, если параметры защиты от сетевых угроз на устройстве заданы через политику. Если на устройстве применяются локально настроенные параметры, по умолчанию защита от сетевых угроз выключена.

Вы можете включать и выключать Защиту от сетевых угроз, а также настраивать параметры защиты:

- Выбирать действие, которое приложение будет выполнять при обнаружении сетевой активности, характерной для сетевых атак.
- Включать и выключать блокировку сетевой активности при обнаружении попытки сетевой атаки.
- Задавать продолжительность блокировки атакующего устройства.
- Настраивать список IP-адресов, сетевая активность которых не блокируется приложением.

С помощью команд управления заблокированными устройствами в командной строке вы можете посмотреть список заблокированных устройств и вручную разблокировать эти устройства. В Kaspersky Security Center нет инструментов мониторинга и управления заблокированными устройствами, кроме событий *Обнаружена сетевая атака*.

Приложение Kaspersky Endpoint Security добавляет в список таблицы mangle утилит iptables и ip6tables специальную разрешающую цепочку правил kesl_bypass, которая позволяет исключать трафик из проверки приложением. Если в цепочке настроены правила исключения трафика, они влияют на работу задачи Защита от сетевых угроз. Например, для исключения исходящего http-трафика вам нужно добавить следующую команду: `iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT`.

Настройка защиты от сетевых угроз в Web Console

В Web Console вы можете настраивать параметры защиты от сетевых угроз в свойствах политики (**Параметры приложения** → **Базовая защита** → **Защита от сетевых угроз**).

Параметры компонента Защита от сетевых угроз

Параметр	Описание
Защита от сетевых угроз включена / выключена	Переключатель включает или выключает компонент Защита от сетевых угроз. По умолчанию переключатель включен.
Действие при обнаружении угрозы	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак: • **Информировать** пользователя. Приложение разрешает сетевую активность и записывает в журнал информацию об обнаруженной сетевой активности. • **Блокировать** сетевую активность со стороны атакующего устройства и записывать в журнал информацию об обнаруженной сетевой активности (значение по умолчанию).
Блокировка атакующих устройств включена / выключена	Переключатель включает или выключает блокировку сетевой активности при обнаружении попытки сетевой атаки. По умолчанию переключатель включен.
Блокировать атакующее устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки атакующего устройства в минутах. По истечении указанного времени приложение Kaspersky Endpoint Security разрешает сетевую активность со стороны этого устройства. Доступные значения: целые числа от 1 до 32768. Значение по умолчанию: 60.
Исключения	Таблица содержит список IP-адресов, сетевые атаки с которых не будут заблокированы. По умолчанию список пуст. Вы можете добавлять, настраивать и удалять IP-адреса в таблице. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно IP-адрес

Вы можете добавлять и изменять IP-адреса, сетевые атаки с которых не будут заблокированы приложением Kaspersky Endpoint Security.

IP-адреса

Параметр	Описание
Введите IP-адрес	Поле для ввода IP-адреса. Вы можете указывать IP-адреса в форматах IPv4 и IPv6.

Настройка защиты от сетевых угроз в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от сетевых угроз в свойствах политики (**Базовая защита → Защита от сетевых угроз**).

Параметры компонента Защита от сетевых угроз

Параметр	Описание
Включить Защиту от сетевых угроз	Флажок включает или выключает компонент Защита от сетевых угроз. По умолчанию флажок установлен.
Действие при обнаружении угрозы	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак: • **Информировать** пользователя. Приложение разрешает сетевую активность и записывает в журнал информацию об обнаруженной сетевой активности. • **Блокировать** сетевую активность со стороны атакующего устройства и записывать в журнал информацию об обнаруженной сетевой активности (значение по умолчанию).
Блокировать атакующие устройства	Флажок включает или выключает блокировку сетевой активности при обнаружении попытки сетевой атаки. По умолчанию флажок установлен.
Блокировать атакующее устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки атакующего устройства в минутах. По истечении указанного времени приложение Kaspersky Endpoint Security разрешает сетевую активность со стороны этого устройства. Доступные значения: целые числа от 1 до 32768. Значение по умолчанию: 60.
Исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения**, в котором вы можете указать список IP-адресов, сетевые атаки с которых не будут заблокированы.

Окно Исключения

В этом окне вы можете добавить IP-адреса, сетевые атаки с которых не будут заблокированы.

По умолчанию список пустой.

Вы можете добавлять, изменять и удалять IP-адреса в списке.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно IP-адрес

Вы можете добавлять и изменять IP-адреса, сетевые атаки с которых не будут заблокированы приложением Kaspersky Endpoint Security.

IP-адреса

Параметр	Описание
Введите IP-адрес	Поле для ввода IP-адреса. Вы можете указывать IP-адреса в форматах IPv4 и IPv6.

Настройка защиты от сетевых угроз в командной строке

В командной строке вы можете управлять защитой от сетевых угроз с помощью предустановленной задачи Защита от сетевых угроз (*Network_Threat_Protection*).

По умолчанию задача Защита от сетевых угроз не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры защиты от сетевых угроз, изменяя параметры предустановленной задачи Защита от сетевых угроз.

Параметры задачи Защита от сетевых угроз

Параметр	Описание	Значения
`ActionOnDetect`	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак. При изменении значения этого параметра с `Block` на `Notify` список заблокированных устройств очищается.	`Notify` – разрешить сетевую активность, записать в журнал информацию об обнаруженной сетевой активности. Если указано это значение, значение параметра `BlockAttackingHosts` не учитывается. `Block` (значение по умолчанию) – заблокировать сетевую активность и записать в журнал информацию об этом.

`BlockAttackingHosts`	Блокировка сетевой активности со стороны атакующих устройств.	`Yes` (значение по умолчанию) – заблокировать сетевую активность атакующего устройства. `No` – не блокировать сетевую активность атакующего устройства. Если указано это значение, а для параметра `ActionOnDetect` указано значение `Block`, приложение блокирует сетевую активность со стороны атакующего устройства, но не вносит это устройство в список заблокированных устройств.
`BlockDurationMinutes`	Продолжительность блокировки атакующих устройств (в минутах).	1 – 32768 Значение по умолчанию: 60.
`UseExcludeIPs`	Использование списка IP-адресов, сетевую активность которых не требуется блокировать при обнаружении сетевой атаки. Приложение записывает в журнал информацию о вредоносной активности со стороны этих устройств. Вы можете добавить IP-адреса в список исключений с помощью параметра `ExcludeIPs.item_#`.	`Yes` – использовать список исключений IP-адресов. `No` (значение по умолчанию) – не использовать список исключений IP-адресов.
`ExcludeIPs.item_#`	IP-адреса, сетевая активность которых не блокируется приложением. По умолчанию список пуст.	`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 не задано.

Защита от удаленного вредоносного шифрования

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

Для использования компонента требуется лицензия, которая включает эту функцию.

Эта функциональность не поддерживается в KESL-контейнере.

Если защита от шифрования включена, приложение Kaspersky Endpoint Security проверяет действия удаленных устройств с файловыми ресурсами, расположенным в общих сетевых директориях защищаемого устройства, на наличие вредоносного шифрования. Если приложение расценивает действия удаленного устройства, получающего доступ к общим сетевым ресурсам, как вредоносное шифрование, приложение создает и включает правило для сетевого экрана операционной системы, которое блокирует сетевой трафик от скомпрометированного устройства. Скомпрометированное устройство добавляется в список недоверенных устройств, доступ к общим сетевым директориям для всех недоверенных устройств блокируется. Приложение создает событие *Обнаружено шифрование*, которое содержит информацию о скомпрометированном устройстве.

По умолчанию приложение блокирует доступ недоверенных устройств к сетевым файловым ресурсам на 30 минут. По истечении времени блокировки приложение удаляет скомпрометированное устройство из списка недоверенных устройств, доступ устройства к сетевым файловым ресурсам автоматически восстанавливается.

Правила сетевого экрана, созданные компонентом Защита от шифрования, нельзя удалить с помощью утилиты iptables, так как приложение восстанавливает набор правил каждую минуту.

По умолчанию Защита от удаленного вредоносного шифрования выключена.

Вы можете включать и выключать защиту от вредоносного шифрования, а также настраивать параметры защиты:

- Выбирать действие, которое приложение будет выполнять при обнаружении шифрования: информировать пользователя или блокировать устройство, осуществляющее вредоносное шифрование.

  Если выбрано действие *Информировать*, приложение все равно проверяет действия удаленных устройств с сетевыми файловыми ресурсами на наличие вредоносного шифрования, когда защита от шифрования включена. В случае обнаружения вредоносного шифрования создается событие *Обнаружено шифрование*, но скомпрометированное устройство не блокируется.

- Задавать продолжительность блокировки недоверенного устройства.

- Указывать файлы и директории, которые приложение защищает от вредоносного шифрования.

- Указывать файлы и директории, которые исключены из защиты от вредоносного шифрования.

  Приложение не расценивает действия как шифрование, если активность шифрования обнаружена в директориях, исключенных из защиты от шифрования.

С помощью команд управления заблокированными устройствами в командной строке вы можете посмотреть список заблокированных устройств и вручную разблокировать эти устройства. В Kaspersky Security Center нет инструментов мониторинга и управления заблокированными устройствами, кроме событий *Обнаружено шифрование*.

Для корректной работы компонента Защита от шифрования требуется, чтобы в операционной системе была установлена хотя бы одна из служб: Samba или NFS. Для службы NFS требуется установленный пакет rpcbind.

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

Kaspersky Endpoint Security не блокирует доступ к сетевым файловым ресурсам, пока действия устройства не расцениваются как вредоносные. Таким образом, минимум один файл будет зашифрован, прежде чем приложение обнаружит вредоносную активность.

Настройка защиты от шифрования в Web Console

В Web Console вы можете настраивать параметры защиты от шифрования в свойствах политики (**Параметры приложения** → **Продвинутая защита** → **Защита от шифрования**).

Параметры компонента 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.
Области защиты	По ссылке **Настроить область защиты** открывается окно **Области защиты**.
Действие при обнаружении шифрования	Действие, которое Kaspersky Endpoint Security будет выполнять при обнаружении вредоносного шифрования: • **Информировать** пользователя. Kaspersky Endpoint Security не блокирует устройство, осуществляющее шифрование, только записывает событие об обнаружении вредоносного шифрования в журнал событий. • **Блокировать** устройство, осуществляющее шифрование (значение по умолчанию).
Блокировать недоверенное устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки недоверенного устройства в минутах. Изменение параметра не влияет на длительность блокировки ранее заблокированных скомпрометированных устройств. Длительность блокировки не является динамическим значением и рассчитывается в момент блокировки. Доступные значения: целые числа от 1 до 4294967295. Значение по умолчанию: 30.
Исключения	По ссылке **Настроить исключения** открывается окно **Области исключения**.
Исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**.

Окно Области защиты

Таблица содержит области защиты компонента Защита от шифрования. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Параметры области защиты

Параметр	Описание
Название области	Название области защиты.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security защищает объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно добавления области защиты

В этом окне можно добавить или настроить область защиты компонента Защита от шифрования.

Параметры области защиты

Параметр	Описание
Название области	Поле ввода названия области защиты. Это название будет отображаться в таблице окна **Области защиты**.

	Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область защиты во время работы компонента. Если флажок снят, приложение не обрабатывает эту область защиты во время работы компонента. В дальнейшем вы можете включить эту область в параметры работы компонента, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все общие** – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран элемент **Общая**.
Путь	Поле ввода пути к директории, которую вы хотите включить в область защиты. Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**. Поле не должно быть пустым. По умолчанию указан путь **/** (корневая директория).
Маски	Список содержит маски имен объектов, которые приложение проверяет во время

работы компонента Защита от шифрования.

По умолчанию список содержит маску * (все объекты).

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки или защиты во время своей работы. Если флажок снят, приложение включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные директории. • **Смонтированная** – удаленные директории, смонтированные на устройстве. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле **Путь**. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска. При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки.

Кнопка доступна, если в списке выбрана хотя бы одна маска.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Настройка защиты от шифрования в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от шифрования в свойствах политики (**Продвинутая защита → Защита от шифрования**).

Параметры компонента Защита от шифрования

Параметр	Описание

Включить Защиту от шифрования	Флажок включает или выключает защиту файлов в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования. По умолчанию флажок снят.
Области защиты	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки и параметры защиты.
Исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне можно добавить или настроить область защиты компонента Защита от шифрования.

Параметры области защиты

Параметр	Описание
Название области	Поле ввода названия области защиты. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область защиты во время работы компонента. Если флажок снят, приложение не обрабатывает эту область защиты во время работы компонента. В дальнейшем вы можете включить эту область в параметры работы компонента, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** – локальные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все общие** (значение по умолчанию) – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область защиты. Для указания пути вы можете использовать маски.

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы компонента Защита от шифрования. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Параметры защиты

Параметры защиты

Параметр	Описание
Действие при обнаружении	Действие, которое Kaspersky Endpoint Security будет выполнять при обнаружении вредоносного шифрования:

шифрования	• **Информировать** пользователя. Kaspersky Endpoint Security не блокирует устройство, осуществляющее шифрование, только записывает событие об обнаружении вредоносного шифрования в журнал событий. • **Блокировать** устройство, осуществляющее шифрование (значение по умолчанию).
Блокировать недоверенное устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки недоверенного устройства в минутах. По истечении указанного времени приложение 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 2147483647. Значение по умолчанию: 30.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из проверки.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги.

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>]/<путь к локальной директории>`
- `[image-id:<идентификатор>]/<путь к локальной директории>`
- `[image-name:<название>]/<путь к локальной директории>`

Также вы можете использовать уникальные комбинации из тегов `[container-id:<идентификатор>]`, `[container-name:<название>]`, `[image-id:<идентификатор>]` и `[image-name:<название>]/<путь к локальной директории>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<название>][image-name:<название>]/<путь к локальной директории>`
- `[container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[image-name:<название>][image-id:<идентификатор>]/<путь к локальной директории>`
- `[container-name:<название>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`
- `[container-name:<название>][image-id:<идентификатор>][container-id:<идентификатор>][image-name:<название>]/<путь к локальной директории>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки. Кнопка доступна, если в списке выбрана хотя бы одна маска. При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранную маску имен файлов, исключаемых из проверки.

Кнопка доступна, если в списке выбрана хотя бы одна маска.

При нажатии на маску открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете изменить шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Настройка защиты от шифрования в командной строке

В командной строке вы можете управлять защитой от шифрования с помощью задачи Защита от шифрования (*Anti_Cryptor*).

По умолчанию задача Защита от шифрования не запущена. Вы можете запускать и останавливать эту задачу вручную.

Вы можете настраивать параметры защиты от шифрования, изменяя параметры предустановленной задачи Защита от шифрования.

Параметры задачи Защита от шифрования

Параметр	Описание	Значения
ActionOnDetect	Включение блокировки недоверенных устройств.	`Block` (значение по умолчанию) – включить блокировку недоверенных устройств. `Notify` – выключить блокировку недоверенных устройств.
`BlockTime`	Длительность блокировки недоверенного устройства в минутах. Изменение параметра `BlockTime` не влияет на длительность блокировки ранее заблокированных скомпрометированных устройств. Длительность блокировки не является динамическим значением и рассчитывается на момент блокировки.	Целое значение от 1 до 4294967295. Значение по умолчанию: 30.
`UseExcludeMasks`	Включение исключения из области защиты объектов, указанных параметром `ExcludeMasks.item_#`. Этот параметр работает, только если указано значение параметра `ExcludeMasks.item_#`.	`Yes` – исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области защиты. `No` (значение по умолчанию) – не исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области защиты.
`ExcludeMasks.item_#`	Исключение из области защиты объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области защиты отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`. Если вы хотите указать несколько масок, указывайте каждую маску в новой строке с новым индексом.	Значение по умолчанию не задано.
Секция **[ScanScope.item_#]** содержит области, защищаемые приложением. Для задачи Защита от шифрования требуется указать хотя бы одну область защиты, можно указывать только общие директории. Вы можете указать несколько секций [ScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области защиты, содержит дополнительную информацию об области защиты.	Значение по умолчанию: `All shared directories`.

`UseScanArea`	Включение защиты указанной области. Для выполнения задачи требуется включить защиту хотя бы одной области.	`Yes` (значение по умолчанию) – защищать указанную область. `No` – не защищать указанную область.
`AreaMask.item_#`	Ограничение области защиты. В области защиты приложение защищает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (защищать все объекты).
`Path`	Путь к директории с защищаемыми объектам.	`<путь к локальной директории>` – защищать локальную директорию, доступную через SMB/NFS. Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. `AllShared` (значение по умолчанию) – защищать все ресурсы, доступные через SMB/NFS.

		`Shared:SMB` – защищать ресурсы, доступные через SMB. `Shared:NFS` – защищать ресурсы, доступные через NFS.
Секция **[ExcludedFromScanScope.item_#]** содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#]. Объекты, удовлетворяющие правилам любой из секций [ExcludedFromScanScope.item_#], не проверяются. Формат секции [ExcludedFromScanScope.item_#] аналогичен формату секции [ScanScope.item_#]. Вы можете указать несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области исключения из защиты, содержит дополнительную информацию об области исключения.	Значение по умолчанию: `All objects`.
`UseScanArea`	Исключение указанной области из защиты.	`Yes` (значение по умолчанию) – исключать указанную область из защиты. `No` – не исключать указанную область из защиты.
`AreaMask.item_#`	Ограничение области исключения из защиты. В области исключения приложение исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (исключать все объекты).
`Path`	Путь к директории с объектами, исключаемыми из защиты.	`<путь к локальной директории>` – исключать из защиты объекты в указанной директории. Для указания пути вы можете использовать маски.

		Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file*/` или `/dir/file**/`. Маску ** можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. `Mounted:NFS` – исключать из защиты удаленные директории, смонтированные на клиентском устройстве по протоколу NFS. `Mounted:SMB` – исключать из защиты удаленные директории, смонтированные на клиентском устройстве по протоколу Samba. `AllRemoteMounted` – исключать из защиты все удаленные директории, смонтированные на клиентском устройстве с помощью протоколов Samba и NFS.

Управление заблокированными устройствами

В ходе защиты устройства от сетевых угроз и от удаленного вредоносного шифрования приложение Kaspersky Endpoint Security может блокировать удаленные устройства, действия которых расцениваются как вредоносные:

- При обнаружении вредоносного шифрования приложение блокирует доступ удаленного устройства к общим сетевым директориям защищаемого устройства.
- При обнаружении попытки сетевой атаки на защищаемое устройство приложение блокирует сетевой трафик со стороны атакующего устройства.

Вы можете изменять продолжительность блокировки в параметрах защиты от сетевых угроз и защиты от удаленного вредоносного шифрования. По истечении заданного периода времени приложение разблокирует устройство.

Если вы управляете приложением с помощью командной строки, вы можете использовать команды управления заблокированными устройствами, чтобы посмотреть список устройств, заблокированных в результате работы приложения на устройстве, и вручную разблокировать эти устройства до истечения времени блокировки. В Kaspersky Security Center нет инструментов мониторинга и управления заблокированными устройствами, кроме событий *Обнаружена сетевая атака* и *Обнаружено шифрование*.

-H –префикс, указывающий, что команда принадлежит к группе команд управления устройствами, заблокированными Защитой от шифрования и Защитой от сетевых угроз.

Команда kesl-control --get-blocked-hosts

Команда позволяет вывести в консоль список заблокированных устройств.

Синтаксис команды

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

Команда kesl-control --allow-hosts

Команда позволяет разблокировать заблокированные устройства.

Синтаксис команды

```
kesl-control [-H] --allow-hosts <адрес>
```

Аргументы и ключи

<адрес> – IP-адрес устройства или подсети (IPv4/IPv6, включая адреса в короткой форме). Вы можете указать несколько IP-адресов устройств или подсетей, разделяя их пробелами.

Чтобы просмотреть список заблокированных устройств, выполните следующую команду:

```
kesl-control --get-blocked-hosts
```

В результате выполнения команды приложение выводит список заблокированных устройств в консоль.

Чтобы разблокировать устройства, выполните следующую команду:

```
kesl-control --allow-hosts <адрес>
```

где <адрес> – один или несколько IP-адресов устройств или подсетей (IPv4/IPv6, включая адреса в короткой форме). Вы можете указать несколько IP-адресов устройств или подсетей, разделяя их пробелами.

В результате выполнения команды приложение разблокирует указанные устройства.

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 - ::
```

Контроль приложений

Компонент Контроль приложений позволяет управлять запуском приложений на защищаемых устройствах. Контроль приложений снижает риск заражения устройства, ограничивая доступ пользователей к приложениям.

Для использования компонента требуется лицензия, которая включает эту функцию.

Эта функциональность не поддерживается в KESL-контейнере.

Запуск приложений регулируется с помощью *правил контроля приложений*.

Компонент Контроль приложений может работать в одном из двух режимов:

- *Список запрещенных*. Режим, при котором приложение Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. По умолчанию компонент Контроль приложений работает в этом режиме.
- *Список разрешенных*. Режим, при котором приложение Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.

Если правила контроля приложений сформированы максимально полно, Kaspersky Endpoint Security запрещает запуск всех новых, не проверенных администратором локальной сети организации приложений, но обеспечивает работоспособность операционной системы и проверенных приложений, которые нужны пользователям для выполнения должностных обязанностей.

Администратор Kaspersky Security Center или локальный пользователь с назначенной в приложении ролью admin может запрещать или разрешать запуск процессов под учетной записью root, используя Контроль приложений.

По умолчанию Контроль приложений выключен. Вы можете включать и выключать Контроль приложений, а также настраивать параметры работы компонента:

- Выбирать режим компонента Контроль приложений: с*писок разрешенных* или *список запрещенных*.
- Создавать правила контроля приложений для каждого режима компонента.
- Выбирать действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего правилам: *применять правила* или *тестировать правила* и информировать о попытке запуска приложения, удовлетворяющего правилам.

Вы можете получать информацию о приложениях, установленных на защищаемых устройствах с помощью задачи Инвентаризация.

Контроль приложений не поддерживает управление запуском приложений Snap, Flatpak и AppImage.

Контроль приложений не контролирует запуск скриптов из интерпретаторов, не поддерживаемых приложением Kaspersky Endpoint Security и запуск скриптов, передаваемых интерпретатору не через командную строку. Kaspersky Endpoint Security поддерживает следующие интерпретаторы: python, perl, bash, ssh.

Если запуск интерпретатора разрешен правилами Контроля приложений, то Kaspersky Endpoint Security не блокирует скрипт, запущенный из этого интерпретатора. Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами Контроля приложений, то Kaspersky Endpoint Security блокирует все скрипты, указанные в командной строке интерпретатора. Исключение: cat script.py | python.

О правилах контроля приложений

Правило контроля приложений представляет собой набор параметров, которые содержат условия срабатывания правила и действия компонента Контроль приложений при срабатывании правила (разрешение или запрещение пользователям запускать приложение):

- Принадлежность приложения к категории приложений. *Категория приложений* – это группа приложений, обладающих общими признаками. Например, категория, в которую входят исполняемые файлы установленных приложений, или категория приложений, необходимых для работы, в которую входит стандартный набор приложений, используемых в организации. Вы можете использовать одну и ту же категорию только в одном правиле.

  Использование KL-категорий приложения Kaspersky Security Center не поддерживается приложением Kaspersky Endpoint Security.

- Разрешение или запрещение выбранным пользователям и/или группам пользователей запускать приложения. Вы можете указать пользователя и/или группу пользователей, которым разрешен или запрещен запуск приложений из указанной категории.

- Условие срабатывания правила. Условие представляет собой соответствие "тип условия – критерий условия – значение условия". На основании условий срабатывания правила приложение Kaspersky Endpoint Security применяет или не применяет правило к приложению. В правилах используются включающие и исключающие условия:

  - *Включающие условия*. Kaspersky Endpoint Security применяет правило к приложению, если приложение соответствует хотя бы одному включающему условию.

  - *Исключающие условия*. Kaspersky Endpoint Security не применяет правило к приложению, если приложение соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию.

  Условия срабатывания правила формируются с помощью следующих критериев:

  - имя исполняемого файла приложения;

  - имя директории с исполняемым файлом приложения;

  - хеш исполняемого файла приложения. Допускается использование только SHA256.

  Для каждого критерия, используемого в условии, вам нужно указать его значение.

  Для указания имен файлов и директорий вы можете использовать маски.

Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории.

Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/*/file*/` или `/dir/file*/`.

Вы можете указать символ ? вместо любого одного символа (включая символ `/`) в имени файла или директории.

Если параметры запускаемого приложения соответствуют критериям, указанным во включающем условии, правило срабатывает. В этом случае Kaspersky Endpoint Security выполняет действие, указанное в правиле. Если параметры приложения соответствуют критериям, указанным в исключающем условии, Kaspersky Endpoint Security не контролирует запуск приложения.

Правила контроля приложений могут иметь один из следующих *статусов работы*:

- *Включено* – правило включено, Kaspersky Endpoint Security применяет это правило для контроля приложений.
- *Выключено* – правило выключено и не используется для контроля приложений.
- *Тест* – Kaspersky Endpoint Security разрешает запуск приложений, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих приложений в отчете.

Статус работы правила имеет более высокий приоритет чем действие, указанное в правиле.

Настройка контроля приложений в Web Console

В Web Console вы можете настраивать параметры контроля приложений в свойствах политики (**Параметры приложения** → **Контроль безопасности** → **Контроль приложений**).

Параметры компонента Контроль приложений

Параметр	Описание
Контроль приложений включен / выключен	Переключатель включает или выключает компонент Контроль приложений. По умолчанию переключатель выключен.
Действие при запуске приложений, запрещенных правилами	Действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам: • **Тестировать правила**. При выборе этого варианта приложение Kaspersky Endpoint Security тестирует правила и формирует событие о попытке запуска приложения, удовлетворяющего правилам. • **Применять правила** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security применяет правила контроля приложений и выполняет заданное в правилах действие.
Режим Контроля приложений	Режим работы компонента Контроль приложений: • **Список разрешенных**. При выборе этого варианта приложение Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений,

	кроме тех, которые указаны в правилах контроля приложений. • **Список запрещенных** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.
Правила Контроля приложений	По ссылке **Настроить правила** открывается окно **Правила Контроля приложений**.
Применение правил	В раскрывающемся списке вы можете выбрать способ добавления правил: • **Заменить правилами из политики локальные правила**. При выборе этого элемента списка приложение применяет только правила, заданные в политике. • **Добавить правила из политики к локальным правилам** (значение по умолчанию). При выборе этого элемента списка приложение применяет правила, заданные в политике, совместно с локальными правилами, настроенными на защищаемом устройстве.

Окно Правила Контроля приложений

Таблица **Правила Контроля приложений** содержит закладки с правилами для каждого режима работы Контроля приложений: **Список запрещенных (активен)** и **Список разрешенных**. По умолчанию таблица правил контроля приложений на обеих закладках пустая.

Параметры правил контроля приложений

Параметр	Описание
Категория	Название категории приложений, которая используется в работе правила.
Статус	Статус работы правила контроля приложений: • *Включено* – правило включено, Контроль приложений применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля приложений. • *Тест* – Контроль приложений разрешает запуск приложений, которые удовлетворяют условиям правила, но записывает информацию о запуске этих приложений в отчет.

Вы можете добавлять, изменять и удалять правила контроля приложений.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

Окно Правило Контроля приложений

В этом окне вы можете настроить параметры правила Контроля приложений.

Настройка правила контроля приложений

Параметр	Описание
Описание правила	Описание правила Контроля приложений.
Статус	Вы можете выбрать статус работы правила контроля приложений: • *Включено* – правило включено, Контроль приложений применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля приложений. • *Тест* – Контроль приложений разрешает запуск приложений, которые удовлетворяют условиям правила, но записывает информацию о запуске этих приложений в отчет.
Категория	По ссылке **Выбрать категорию** открывается окно **Категории приложений**.
Пользователи и их права	Таблица содержит список имен пользователей или названий групп пользователей, на которых распространяется правило контроля приложений, и назначенные им типы доступа, и состоит из следующих столбцов: • **Имя пользователя или группы** – имена пользователей или названия групп пользователей, на которых распространяется правило контроля приложений. • **Доступ** – тип доступа (разрешение или запрет на запуск приложений). Переключатель включает или выключает тип доступа: **Разрешать** запуск приложений или **Блокировать** запуск приложений. Вы можете добавлять, изменять и удалять пользователей или группы пользователей. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно Категории приложений

В этом окне вы можете добавить новую категорию или настроить параметры категории для правила контроля приложений.

Использование KL-категорий приложения Kaspersky Security Center не поддерживается приложением Kaspersky Endpoint Security.

Категории Контроля приложений

Параметр	Описание
Название категории	Строка поиска добавленных категорий приложений.
Добавить	При нажатии на кнопку запускается мастер создания категории. Следуйте указаниям мастера.
Изменить	При нажатии на кнопку открывается окно свойств категории, в котором вы можете изменить параметры категории.
Удалить	При нажатии на кнопку выбранная категория удаляется. Категорию **Золотой образ (локальная)** удалить нельзя.

Окно Выбор пользователя или группы

В этом окне вы можете указать локального или доменного пользователя или группу пользователей, для которых вы хотите настроить правило.

Настройка правила Контроля приложений

Параметр	Описание
Вручную	Если выбран этот вариант, в поле ниже вам нужно ввести имя локального или доменного пользователя или название группы пользователей, на которых будет распространяться правило контроля приложений.
Список групп или пользователей	Если выбран этот вариант, в поле поиска вы можете ввести критерии поиска имени пользователя или названия группы пользователей, на которых будет распространяться правило контроля приложений, или выбрать название группы пользователей в списке ниже.

Настройка контроля приложений в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры контроля приложений в свойствах политики (**Контроль безопасности** → **Контроль приложений**).

Параметры компонента Контроль приложений

Параметр	Описание
Включить Контроль приложений	Флажок включает компонент Контроль приложений. По умолчанию флажок снят.
Действие при попытке запуска приложения	Действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам: • **Применять правила** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security применяет правила контроля приложений и выполняет заданное в правилах действие. • **Тестировать правила**. При выборе этого варианта приложение Kaspersky Endpoint Security тестирует правила и формирует событие о попытке запуска приложения, удовлетворяющего правилам.
Режим	Режим работы компонента Контроль приложений:

Контроля приложений	• **Список разрешенных**. При выборе этого варианта приложение Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. • **Список запрещенных** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.
Правила Контроля приложений	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Правила Контроля приложений**.
Применение правил	В раскрывающемся списке вы можете выбрать способ добавления правил: • **Заменить правилами из политики локальные правила**. При выборе этого элемента списка приложение применяет только правила, заданные в политике. • **Добавить правила из политики к локальным правилам** (значение по умолчанию). При выборе этого элемента списка приложение применяет правила, заданные в политике, совместно с локальными правилами, настроенными на защищаемом устройстве.

Окно Правила Контроля приложений

Таблица **Правила Контроля приложений** содержит правила, используемые компонентом Контроль приложений. По умолчанию таблица правил контроля приложений пустая.

Параметры правил контроля приложений

Параметр	Описание
Название категории	Название категории приложений, которая используется в работе правила.
Статус	Статус работы правила контроля приложений: • *Включено* – правило включено, Контроль приложений применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля приложений. • *Тест* – Контроль приложений разрешает запуск приложений, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих приложений в отчете. Вы можете изменить статус правила в окне **Добавление правила / Изменение правила**.

Вы можете добавлять, изменять и удалять правила контроля приложений.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно Добавление правила

В этом окне вы можете настроить параметры правила контроля приложений.

Добавление правила контроля приложений

Параметр	Описание
Описание	Описание правила Контроля приложений.
Статус правила	В раскрывающемся списке вы можете выбрать статус работы правила контроля приложений: • *Включено* – правило включено, Контроль приложений применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля приложений. • *Тест* – Контроль приложений разрешает запуск приложений, которые удовлетворяют условиям правила, но записывает информацию о запуске этих приложений в отчет.
Категория	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Категории приложений**.
Пользователи и их права	Таблица содержит список пользователей или групп пользователей, на которых распространяется правило контроля приложений, и назначенные им типы доступа, и состоит из следующих столбцов: • **Имя пользователя или группы** – имена пользователей или названия групп пользователей, на которых распространяется правило контроля приложений. • **Доступ** – тип доступа: **Разрешать** запуск приложений или **Блокировать** запуск приложений. Вы можете добавлять, изменять и удалять пользователей или группы пользователей. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно Категории приложений

В этом окне вы можете добавить новую категорию или настроить параметры категории для правила контроля приложений.

Использование KL-категорий приложения Kaspersky Security Center не поддерживается приложением Kaspersky Endpoint Security.

Категории Контроля приложений

Параметр	Описание
Название категории	Список добавленных категорий Контроля приложений.
Добавить	При нажатии на кнопку запускается мастер создания категории. Следуйте указаниям мастера.
Изменить	При нажатии на кнопку открывается окно свойств категории, в котором вы можете изменить параметры категории.

Окно Пользователь или группа

В этом окне вы можете указать локального или доменного пользователя или группу пользователей, для которых вы хотите настроить правило.

Добавление правила Контроля приложений

Параметр	Описание
Тип	**Пользователь** или **Группа**, на которых распространяется правило.
Имя пользователя или группы	Имя пользователя или название группы пользователей, на которых распространяется правило контроля приложений.
Доступ	Тип доступа: **Разрешать** запуск приложений или **Блокировать** запуск приложений.

Настройка контроля приложений в командной строке

В командной строке вы можете управлять контролем приложений с помощью предустановленной задачи Контроль приложений (*Application_Control*).

По умолчанию задача Контроль приложений не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры контроля приложений на устройстве, изменяя параметры предустановленной задачи Контроль приложений.

Если вы меняете список разрешенных приложений или запрещаете запуск всех приложений и/или приложений, влияющих на работу Kaspersky Endpoint Security, то при изменении параметров задачи с помощью конфигурационного файла или с помощью ключей командной строки требуется запускать команду `kesl-control --set-settings` с флагом `--accept`.

Вы также можете настраивать параметры Контроля приложений с помощью команд управления Контролем приложений:

- Создавать и изменять списки категорий.
- Просматривать список созданных в приложении категорий.
- Настраивать список правил контроля приложений.

Параметры задачи Контроль приложений

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

Параметры задачи Контроль приложений

Параметр	Описание	Значения
`AppControlMode`	Режим работы компонента Контроль приложений.	`AllowList` – Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. `DenyList` (значение по умолчанию) – Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.
`AppControlRulesAction`	Действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам.	`ApplyRules` (значение по умолчанию) – Kaspersky Endpoint Security применяет правила контроля приложений и выполняет заданное в правилах действие. `TestRules` – Kaspersky Endpoint Security тестирует правила и формирует событие об обнаружении приложения, удовлетворяющего правилу.
Секция **[Categories.item_#]** содержит следующие параметры:		
`Name`	Название категории приложений, для которой будет применяться правило.	
`UseIncludes`	Использование включающих условий для срабатывания правила.	`Yes` – применять правило к приложению, если приложение соответствует хотя бы одному включающему условию. `No` (значение по умолчанию) – не применять правило к приложению, даже если приложение соответствует включающему условию.
`IncludeFileNames.item_#`	Имя исполняемого файла, на которое срабатывает правило.	Для указания имени файла вы можете использовать маски.

		Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории. Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/*/file*/` или `/dir/file*/`. Вы можете указать символ ? вместо любого одного символа (включая символ /) в имени файла или директории.
`IncludeFolders.item_#`	Имя директории с исполняемым файлом приложения, на которое срабатывает правило.	Для указания имени директории вы можете использовать маски. Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории. Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/*/file*/` или `/dir/file*/`. Вы можете указать символ ? вместо любого одного символа (включая символ /) в имени файла или директории.
`IncludeHashes.item_#`	Хеш SHA256 исполняемого файла, на который срабатывает правило.	Допускается использование только SHA256.
`UseExcludes`	Использование исключающих условий для срабатывания правила.	`Yes` – не применять правило к приложению, если приложение соответствует хотя бы одному исключающему условию или не

		соответствует ни одному включающему условию. `No` (значение по умолчанию) – применять правило к приложению, даже если приложение соответствует исключающему условию.
`ExcludeFileNames.item_#`	Имя исполняемого файла, на которое срабатывает правило.	Для указания имени файла вы можете использовать маски. Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории. Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/*/file*/` или `/dir/file*/`. Вы можете указать символ ? вместо любого одного символа (включая символ /) в имени файла или директории.
`ExcludeFolders.item_#`	Имя директории с исполняемым файлом приложения, на которое срабатывает правило.	Для указания имени директории вы можете использовать маски. Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории. Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/*/file*/` или `/dir/file*/`. Вы можете указать символ ? вместо любого одного символа (включая символ /) в имени файла или директории.

`ExcludeHashes.item_#`	Хеш SHA256 исполняемого файла, на который срабатывает правило.	Допускается использование только SHA256.
Секция **[AllowListRules.item_#]** содержит список правил контроля приложений для режима работы *Список разрешенных* (*AllowList*). Каждая секция [AllowListRules.item_#] содержит следующие параметры:		
`Description`	Описание правила контроля приложений.	
`AppControlRuleStatus`	Статус работы правила контроля приложений.	`On` (значение по умолчанию) – правило включено, Kaspersky Endpoint Security применяет это правило для контроля приложений. `Off` – правило не используется для контроля приложений. `Test` – Kaspersky Endpoint Security разрешает запуск приложений, на которые распространяется действие правила, но фиксирует информацию о запуске этих приложений в отчете.
`Category`	Название категории приложений, для которой применяется правило. Вы можете указать в качестве категории категорию "Golden Image".	
Секция **[AllowListRules.item_#.ACL.item_#]** содержит список пользователей, которым разрешен или запрещен запуск приложений.		
`Access`	Тип доступа, назначаемый пользователю или группе пользователей.	`Allow` (значение по умолчанию) – разрешать запуск приложений. `Block` – запрещать запуск приложений.
`Principal`	Пользователь или группа пользователей, на которых распространяется правило контроля приложений.	`\Everyone` (значение по умолчанию) – правило применяется для всех пользователей. `<имя пользователя>` – имя пользователя, для которого применяется правило. `@<название группы>` – название группы пользователей, для которых применяется правило.
Секция **[DenyListRules.item_#]** содержит список правил контроля приложений для режима работы *Список запрещенных* (*DenyList*). Каждая секция [DenyListRules.item_#] содержит следующие параметры:		
`Description`	Описание правила контроля приложений.	
`AppControlRuleStatus`	Статус работы правила контроля приложений.	`On` (значение по умолчанию) – правило включено, Kaspersky

		Endpoint Security применяет это правило для контроля приложений. `Off` – правило не используется для контроля приложений. `Test` – Kaspersky Endpoint Security разрешает запуск приложений, на которые распространяется действие правила, но фиксирует информацию о запуске этих приложений в отчете.
`Category`	Название созданной категории приложений, для которой применяется правило. Вы можете указать в качестве категории список приложений "Golden Image".	
Секция **[DenyListRules.item_#.ACL.item_#]** содержит список пользователей, которым разрешен или запрещен запуск приложений.		
`Access`	Тип доступа, назначаемый пользователю или группе пользователей.	`Allow` – разрешать запуск приложений. `Block` (значение по умолчанию) – запрещать запуск приложений.
`Principal`	Пользователь или группа пользователей, на которых распространяется правило контроля приложений.	`\Everyone` (значение по умолчанию) – правило применяется для всех пользователей. `<имя пользователя>` – имя пользователя, для которого применяется правило. `@<название группы>` – название группы пользователей, для которых применяется правило.

Создание и изменение списка категорий

Вы можете создать новую категорию двумя способами:

- с помощью команды kesl --set-settings и конфигурационного файла параметров задачи Контроль приложений (Application_Control);
- с помощью команды kesl --set-categories и конфигурационного файла параметров категории.

Чтобы создать категории приложений, выполните следующую команду:

```
kesl-control --set-categories --file <путь к конфигурационному файлу>
```

где:

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу с параметрами категорий.

Файл с параметрами категорий должен иметь такую структуру:

```
[
     {
          "Exclude" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)",
   "(FileHash == <хеш исполняемого файла>)" ],
          "GUID" : "<уникальный идентификатор категории>",
          "Include" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)",
   "(FileHash == <хеш исполняемого файла>)" ],
          "Name" : "<название категории 1>"
     },
   {
          "Exclude" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)",
   "(FileHash == <хеш исполняемого файла>)" ],
          "GUID" : "<уникальный идентификатор категории>",
          "Include" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)",
   "(FileHash == <хеш исполняемого файла>)" ],
          "Name" : "<название категории 2>"
     }
]
```

Для указания имени файла в полях `Exclude` и `Include` вы можете использовать маски.

Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории.

Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/*/file*/` или `/dir/file*/`.

Вы можете указать символ ? вместо любого одного символа (включая символ `/`) в имени файла или директории.

Параметр `Name` обязательный, если вы не укажете название категории, она не будет создана или будет удалена. Параметр `GUID` также обязательный, если вы его не укажете, отобразится сообщение об ошибке и категория не будет создана. Параметр `GUID` требуется указывать без дефисов.

Чтобы изменить список созданных категорий приложений, выполните следующую команду:

```
kesl-control --set-categories [--names <название категории 1> <название категории 2>
... <название категории N>] --file <путь к конфигурационному файлу>
```

где:

- `<название категории 1> <название категории 2> ... <название категории N>` – названия категорий, информацию о которых вы хотите изменить. Если вы хотите изменить информацию о нескольких категориях, укажите названия категорий через пробел. Если вы не укажете название категории, существующие категории будут удалены и будут созданы новые категории из указанного файла.
- `--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу с параметрами категорий.

Просмотр списка созданных категорий

В командной строке вы можете просматривать список созданных категорий приложений с помощью команды управления контролем приложений.

Список созданных категорий содержит следующие категории:

- категории, созданные в Kaspersky Security Center;
- категории, добавленные в параметрах задачи Контроль приложений через командную строку;
- категория "GoldenImage", созданная с помощью задачи Инвентаризация (в Kaspersky Security Center или через командную строку).

Чтобы просмотреть список всех созданных категорий приложений, выполните следующую команду:

```
kesl-control --get-categories [--file <путь к конфигурационному файлу>] [--json]
```

где:

- `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу формата JSON, в который будут выведены параметры.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ --json, параметры будут выведены в формате INI.

Kaspersky Endpoint Security отобразит следующую информацию о каждой категории приложений:

- уникальный идентификатор (GUID) категории;
- название категории;
- список включающих условий для срабатывания правила;
- список исключающих условий для срабатывания правила.

Чтобы просмотреть список созданных категорий приложений, выполните следующую команду:

```
kesl-control --get-categories [--names <название категории 1> <название категории 2>
... <название категории N>] [--file <путь к конфигурационному файлу>] [--json]
```

где:

- `<название категории 1> <название категории 2> ... <название категории N>` – названия категорий, информацию о которых вы хотите просмотреть. Если вы хотите просмотреть информацию о нескольких категориях, укажите названия категорий через пробел.
- `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу формата JSON, в который будут выведен список категорий.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ --json, параметры будут выведены в формате INI.

Если в параметрах задачи Контроль приложений в секции `[Categories.item_#]` для включающих или исключающих условий срабатывания правила вы указали символические ссылки на файл приложения или на директорию с исполняемыми файлами, то при просмотре списка категорий для этих условий будет отображаться исходный путь, на который ссылается символическая ссылка.

Настройка списка правил контроля приложений

Чтобы просмотреть список правил контроля приложений, выполните следующую команду:

```
kesl-control --get-settings 21 [--file <путь к конфигурационному файлу>] [--json]
```

где:

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут выведены параметры.

`--json` – выводить данные в формате JSON.

Kaspersky Endpoint Security отобразит следующую информацию о правилах контроля приложений:

- режим работы компонента Контроль приложений;
- действие, которое Контроль приложений будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенному правилу;
- описание правила контроля приложений (если есть);
- статус работы правила контроля приложений;
- название категории приложений, для которой применяется правило;
- тип доступа, назначенный пользователю или группе пользователей;
- пользователь или группа пользователей, на которых распространяется правило контроля приложений.

Чтобы изменить список категорий приложений и правил контроля приложений, выполните следующую команду:

```
kesl-control --set-settings 21 [--file <путь к конфигурационному файлу>] [--json]
```

где:

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

`--json` – импорт данных из файла в формате JSON.

Чтобы удалить список категорий приложений и правил контроля приложений, выполните следующую команду:

```
kesl-control --set-settings 21 --set-to-default
```

Инвентаризация

Задача Инвентаризация позволяет получить информацию обо всех исполняемых файлах приложений, хранящихся на клиентских устройствах. Получение информации о приложениях, установленных на устройствах, может быть полезно, например, для создания правил контроля приложений.

Эта функциональность не поддерживается в KESL-контейнере.

Для использования задачи требуется лицензия, которая включает эту функцию.

Вы можете настраивать следующие параметры инвентаризации:

- Выбирать типы объектов, которые приложение будет обнаруживать на устройстве в ходе инвентаризации (файлы, скрипты).
- Включать и выключать добавление приложений, обнаруженных на устройстве задачей Инвентаризация, в категорию приложений "Золотой образ" ("Golden Image").
- Настраивать области инвентаризации (пути к директориям, в которых нужно искать исполняемые файлы приложений).
- Настраивать исключения из инвентаризации.

Инвентаризация в Web Console

В Web Console вы можете выполнять инвентаризацию приложений защищаемого устройства с помощью задачи *Инвентаризация*.

Вы можете создавать и запускать пользовательские задачи инвентаризации. Вы можете настраивать параметры инвентаризации, изменяя параметры этих задач.

В базе данных приложения Kaspersky Security Center может храниться информация о 150 000 обработанных файлов. При достижении этого количества записей новые файлы не будут обработаны. Для возобновления работы инвентаризации требуется удалить с устройства с установленным приложением Kaspersky Endpoint Security файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

Параметры задачи Инвентаризация

Параметр	Описание
Добавлять файлы в категорию Золотой образ	Флажок включает или выключает добавление приложений, обнаруженных на устройстве задачей Инвентаризация, в категорию приложений "Золотой образ" ("Golden Image"). Если флажок установлен, то в правилах контроля приложений вы можете использовать категорию "Золотой образ". По умолчанию флажок снят.
Проверять все исполняемые файлы	Флажок включает или выключает проверку исполняемых файлов. По умолчанию флажок установлен.

Проверять двоичные файлы	Флажок включает или выключает проверку двоичных файлов (с расширениями elf, java и pyc). По умолчанию флажок установлен.
Проверять скрипты	Флажок включает или выключает проверку скриптов. По умолчанию флажок установлен.
Области инвентаризации	Таблица, содержащая области инвентаризации, проверяемые приложением. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область инвентаризации – /usr/bin. Области инвентаризации в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз. При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице. Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую. Кнопка доступна, если в таблице выбрана область. При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице. Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую. Кнопка доступна, если в таблице выбрана область. При нажатии на кнопку **Удалить** выбранная область исключается из проверки. Кнопка доступна, если в таблице выбрана хотя бы одна область проверки. При нажатии на название области проверки открывается окно **<Название области проверки>**. В этом окне вы можете изменить параметры выбранной области проверки. При нажатии на кнопку **Добавить** открывается окно **<Новая область проверки>**. В этом окне вы можете задать новую область проверки.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки для задачи Инвентаризация.

Параметры области инвентаризации

Параметр	Описание
Название области	Поле ввода названия области инвентаризации. Это название будет отображаться в таблице раздела **Параметры проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время выполнения задачи. Если флажок установлен, приложение обрабатывает эту область инвентаризации во время выполнения задачи. Если флажок снят, приложение не обрабатывает эту область инвентаризации во время выполнения задачи. В дальнейшем вы можете включить эту область в параметры задачи, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область инвентаризации. Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. Поле не должно быть пустым. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время выполнения задачи. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне.

	При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Раздел Области исключения

В разделе **Области исключения** для задачи Инвентаризация вы можете настроить области исключения из проверки.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения из проверки для задачи Инвентаризация.

Параметры области исключения

Параметр	Описание
Название области	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**.

исключения	Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время выполнения задачи. Если флажок установлен, приложение исключает эту область во время выполнения задачи. Если флажок снят, приложение включает эту область во время выполнения задачи. В дальнейшем вы можете исключить эту область из проверки, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения из инвентаризации. Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Инвентаризация в Консоли администрирования

В Консоли администрирования Kaspersky Security Center вы можете выполнять инвентаризацию приложений защищаемого устройства с помощью задачи *Инвентаризация*.

Вы можете создавать и запускать пользовательские задачи инвентаризации. Вы можете настраивать параметры проверки, изменяя параметры задач.

В базе данных приложения Kaspersky Security Center может храниться информация о 150 000 обработанных файлов. При достижении этого количества записей новые файлы не будут обработаны. Для возобновления работы инвентаризации требуется удалить с устройства с установленным приложением Kaspersky Endpoint Security файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

Параметры задачи Инвентаризация

Параметр	Описание
Добавлять файлы в категорию Золотой образ	Флажок включает или выключает добавление приложений, обнаруженных на устройстве задачей Инвентаризация, в категорию приложений "Золотой образ" ("Golden Image"). Если флажок установлен, то в правилах контроля приложений вы можете использовать категорию "Золотой образ". По умолчанию флажок снят.
Проверять все исполняемые файлы	Флажок включает или выключает проверку исполняемых файлов. По умолчанию флажок установлен.
Проверять двоичные файлы	Флажок включает или выключает проверку двоичных файлов (с расширениями elf, java и pyc). По умолчанию флажок установлен.
Проверять скрипты	Флажок включает или выключает проверку скриптов. По умолчанию флажок установлен.
Области инвентаризации	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки**.

В разделе **Области исключения** для задачи Инвентаризация вы можете также настроить области исключения из проверки.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки – /usr/bin.

Параметры области проверки задачи Инвентаризация

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки для задачи Инвентаризация.

Параметры области инвентаризации

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время выполнения задачи. Если флажок установлен, приложение обрабатывает эту область проверки во время выполнения задачи.

	Если флажок снят, приложение не обрабатывает эту область проверки во время выполнения задачи. В дальнейшем вы можете включить эту область в параметры задачи, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время выполнения задачи. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Раздел Исключения

Параметры исключений из проверки

Блок параметров	Описание
Области исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключений

	из мониторинга.

Окно Области исключения

Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из проверки для задачи Инвентаризация.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время выполнения задачи. Если флажок установлен, приложение исключает эту область во время выполнения задачи. Если флажок снят, приложение включает эту область во время выполнения задачи. В дальнейшем вы можете исключить эту область из проверки, установив флажок. По умолчанию флажок установлен.

Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения из инвентаризации. Для указания пути вы можете использовать маски. Поле не должно быть пустым. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки. Примеры: Маска `*.txt` – все текстовые файлы. Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Инвентаризация в командной строке

В командной строке вы можете выполнять инвентаризацию приложений защищаемого устройства следующими способами:

- С помощью предустановленной задачи Инвентаризация (*Inventory_Scan*). Вы можете запускать и останавливать эту задачу вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.

- С помощью пользовательских задач инвентаризации (задач типа *InventoryScan*). Вы можете запускать, останавливать, приостанавливать и возобновлять пользовательские задачи вручную и настраивать расписание запуска задач.

Вы можете просматривать список приложений, обнаруженных на устройстве в результате выполнения задачи Инвентаризация, с помощью команд управления контролем приложений.

Параметры задачи Инвентаризация

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

Параметры задачи Инвентаризация

Параметр	Описание	Значения
`ScanScripts`	Включение проверки скриптов.	`Yes` (значение по умолчанию) – проверять скрипты. `No` – не проверять скрипты.
`ScanBinaries`	Включение проверки бинарных файлов (elf, java и pyc).	`Yes` (значение по умолчанию) – проверять бинарные файлы. `No` – не проверять бинарные файлы.
`ScanAllExecutable`	Включение проверки файлов с исполняемым битом.	`Yes` (значение по умолчанию) – проверять файлы с исполняемым битом. `No` – не проверять файлы с исполняемым битом.
`CreateGoldenImage`	Добавление приложений, обнаруженных на устройстве задачей Инвентаризация, в категорию приложений "Золотой образ" ("Golden Image"). Если значение параметра `CreateGoldenImage=Yes`, то в правилах контроля приложений вы можете использовать категорию приложений "Золотой образ".	`Yes` – добавлять обнаруженные приложения в категорию приложений "Золотой образ". `No` (значение по умолчанию) – не добавлять обнаруженные приложения в категорию приложений "Золотой образ".
Секция **[ScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области инвентаризации, содержит дополнительную информацию об области инвентаризации. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: `All objects`.
`UseScanArea`	Включение проверки указанной области инвентаризации. Для выполнения задачи требуется включить проверку хотя бы одной области инвентаризации.	`Yes` (значение по умолчанию) – проверять указанную область инвентаризации. `No` – не проверять указанную область инвентаризации.

`AreaMask.item_#`	Ограничение области инвентаризации. В области инвентаризации приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области инвентаризации. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты).
`Path`	Путь к директории с проверяемыми объектами.	`<путь к локальной директории>` – проверять объекты в указанной директории. Значение по умолчанию: `/usr/bin`
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры.		
`AreaDesc`	Описание области исключения из инвентаризации, содержит дополнительную информацию об области инвентаризации.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из инвентаризации.	`Yes` (значение по умолчанию) – исключать указанную область. `No` – не исключать указанную область.
`AreaMask.item_#`	Ограничение области исключения из инвентаризации по маскам в формате shell. Если параметр не указан, приложение исключает все объекты в области инвентаризации. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (исключать все объекты).
`Path`	Путь к директории с исключаемыми объектами.	`<путь к локальной директории>` – исключать из проверки объекты в указанной директории. Для указания пути вы можете использовать маски.

		Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

Просмотр списка обнаруженных приложений

Чтобы просмотреть список приложений, обнаруженных на устройстве, выполните следующую команду:

```
kesl-control --get-app-list [--json]
```

где --json – выводить данные в формате JSON.

Kaspersky Endpoint Security отобразит следующую информацию об обнаруженных приложениях:

- **Дата и время инвентаризации**. Дата и время выполнения задачи Инвентаризация.
- **Количество приложений**. Количество приложений, обнаруженных на устройстве.

- Список приложений, содержащий следующую информацию:
  - **Путь**. Путь к приложению.
  - **Хеш**. Хеш-сумма приложения.
  - **Тип**. Тип приложения. Например: `Script`, `Executable`.
  - **Категории**. Категории, к которым принадлежит приложение (если они были созданы ранее). Вы можете просмотреть список созданных категорий приложений с помощью команды `kesl-control --get-categories`.

При добавлении новой категории информация о ней в списке приложений автоматически не обновляется. Для обновления списка приложений требуется повторный запуск задачи Инвентаризация.

Контроль устройств

Компонент *Контроль устройств* позволяет управлять доступом пользователей к устройствам, которые установлены на клиентском устройстве или подключены к нему (например, жестким дискам, камерам или модулям Wi-Fi). Управление доступом позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных.

Эта функциональность не поддерживается в KESL-контейнере.

Компонент Контроль устройств включается автоматически с параметрами по умолчанию при запуске приложения Kaspersky Endpoint Security.

Контроль устройств управляет доступом на следующих уровнях:

- **Тип устройства** по классификации компонента Контроль устройств (например, принтеры, съемные диски, CD/DVD-приводы). Для каждого типа устройств может применяться один из следующих режимов доступа:
  - *Разрешать* – предоставлять доступ к устройствам этого типа.
  - *Блокировать* – запрещать доступ к устройствам этого типа.
  - *В зависимости от шины подключения* – разрешать или запрещать доступ к устройствам в зависимости от режима доступа для шины, по которой подключено устройство.
  - *По правилам* – разрешать или запрещать доступ к устройствам в зависимости от правил доступа к устройствам. *Правило доступа к устройству* – это набор параметров, которые определяют, какие пользователи и в какое время могут получить доступ к устройствам, установленным на клиентском устройстве или подключенным к нему.

    При подключении устройства, доступ к которому запрещен, приложение запрещает указанным в правиле пользователям доступ к этому устройству и выводит уведомление. При попытке чтения и записи на этом устройстве приложение запрещает чтение/запись указанным в правиле пользователям без вывода уведомления.

    Если при попытке совершить операцию с устройством, для которого установлен режим доступа *По правилам*, не нашлось правила, активного на момент доступа, то операция с устройством будет запрещена.
- **Шина подключения**. *Шина подключения* – это интерфейс, с помощью которого устройства подключаются к клиентскому устройству (например, USB, FireWire). Для шин подключения может применяться один из следующих режимов доступа:
  - *Разрешать* – предоставлять доступ к устройствам, подключенным по этой шине подключения.
  - *Блокировать* – запрещать доступ к устройствам, подключенным по этой шине подключения.

  Например, может быть запрещен доступ ко всем устройствам, подключенным по шине USB.

По умолчанию для всех типов устройств выбран режим доступа *В зависимости от шины подключения*, для шин подключения выбран режим доступа *Разрешать*. В соответствии с этими параметрами Контроль устройств предоставляет пользователям полный доступ ко всем устройствам.

Блокировка устройств по типу устройства и по шине подключения через системный драйвер устройства не поддерживается на ядрах ОС Linux: 3.10, 5.14, 5.15, 5.17, 6.1. На этих ядрах, а также при режиме доступа *По правилам* блокируются только открытие файлов и чтение директорий (то есть получение имен файлов и директорий). На системах, не поддерживающих fanotify, не поддерживается блокировка чтения директорий.

При первом включении компонента Контроль устройств для всех обнаруженных устройств с известным типом устройства или шины формируется событие *Доступ к устройству разрешен*, а при следующих запусках повторные события для этих устройств не формируются, если не было изменений в параметрах контроля для этих устройств.

При выключении компонента Контроль устройств приложение разблокирует доступ к заблокированным устройствам.

Вы можете включать и выключать Контроль устройств, а также настраивать параметры работы компонента:

- Выбирать режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств: блокировать или только информировать о попытке доступа к устройству.
- Выбирать режим доступа к устройствам в зависимости от их типа.
- Выбирать режим доступа для шины, по которой подключаются устройства.
- Исключать отдельные устройства из области действия Контроля устройств, добавляя их в список доверенных устройств. *Доверенные устройства* – это устройства, к которым у пользователей есть полный доступ. Вы можете добавлять устройства в список доверенных по идентификатору или маске идентификатора устройства. Например, вы можете разрешить доступ к конкретным USB-устройствам или только к USB-накопителям, при этом доступ к остальным USB-устройства будет запрещен.

  Если вы управляете приложением с помощью командной строки, вы можете посмотреть идентификаторы подключенных устройств, выполнив на клиентском устройстве команду `kesl-control --get-device-list`.

  Если вы управляете приложением с помощью Kaspersky Security Center, информация об устройствах, установленных на клиентских устройствах или подключенных к ним, может передаваться на Сервер администрирования. Передача информации включена по умолчанию.

  > Информация об устройствах передается, если клиентское устройство находится под управлением активной политики и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в свойствах политики Агента администрирования, по умолчанию – каждые 15 минут).

- Настраивать расписание доступа для устройств (только для жестких дисков, съемных дисков, дискет и CD/DVD-приводов).

  > Если в общих параметрах приложения выключена блокировка доступа к файлам во время проверки, то заблокировать доступ к устройствам с помощью расписания доступа для устройств невозможно.

- Настраивать правила доступа к устройствам в зависимости от их типа. Вы можете разрешать или запрещать доступ для указанных пользователей в указанное время.

> Контроль устройств игнорирует исключение точек монтирования. Доступ к устройству, смонтированному в исключенной точке монтирования, может быть ограничен в соответствии с настроенными параметрами Контроля устройств.

Настройка контроля устройств в Web Console

В Web Console вы можете настраивать параметры контроля устройств в свойствах политики (**Параметры приложения → Контроль безопасности → Контроль устройств**).

Параметры компонента Контроль устройств

Параметр	Описание
Контроль устройств включен / выключен	Переключатель включает или выключает компонент Контроль устройств. По умолчанию переключатель включен.
Настроить доверенные устройства	По ссылке открывается окно **Доверенные устройства**. В этом окне вы можете добавлять устройства в список доверенных по идентификатору устройства или выбрав их из списка устройств, обнаруженных на клиентских устройствах.
Режим работы Контроля устройств	Режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств: • **Информировать**. При выборе этого варианта приложение Kaspersky Endpoint Security тестирует выбранный режим доступа и формирует событие об обнаружении попытки доступа к устройству. • **Блокировать** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security применяет режим доступа, заданный для устройства или шины.
Настроить параметры доступа для типов устройств	По ссылке открывается окно **Типы устройств**. В этом окне вы можете настроить параметры доступа к устройствам в зависимости от их типа.
Настроить параметры доступа для шин подключения	По ссылке открывается окно **Шины подключения**. В этом окне вы можете настроить параметры доступа для шин подключения.

Окно Доверенные устройства

Таблица содержит список доверенных устройств. По умолчанию таблица пустая.

Параметры доверенного устройства

Параметр	Описание
Идентификатор устройства	Идентификатор доверенного устройства.
Название устройства	Название доверенного устройства.
Тип устройства	Тип доверенного устройства (например, Жесткий диск или Устройство чтения смарт-карт).
Имя клиентского устройства	Имя клиентского устройства, к которому подключено доверенное устройство.
Комментарий	Комментарий, относящийся к доверенному устройству.

Вы можете добавить устройство в список доверенных устройств по идентификатору устройства или выбрав нужное устройство в списке устройств, обнаруженных на устройстве пользователя.

Доверенные устройства в таблице можно изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

Вы также можете импортировать список устройств из файла по кнопке **Импортировать** и экспортировать список добавленных устройств в файл по кнопке **Экспортировать**. При импорте вам будет предложено заменить список доверенных устройств или добавить устройства к уже существующему списку.

Окно Доверенное устройство (Идентификатор устройства)

В этом окне вы можете добавить устройство в список доверенных устройств по его идентификатору.

Добавление устройства по идентификатору

Параметр	Описание
Идентификатор устройства	Поле для ввода идентификатора или маски идентификатора устройства. Вы можете указать идентификатор вручную или скопировать идентификатор нужного устройства из списка **Устройства, обнаруженные на клиентских устройствах**. Для указания идентификатора вы можете использовать маски * (любая последовательность символов) или ? (один любой символ). Например, вы можете указать маску USBSTOR* для разрешения доступа ко всем USB-накопителям.
Комментарий	Поле ввода комментария (необязательное). Поле доступно после ввода идентификатора устройства и нажатия на кнопку **Далее**.

Окно Доверенное устройство (Список обнаруженных устройств)

В этом окне вы можете добавить устройство в список доверенных, выбрав его из списка устройств, обнаруженных на управляемых клиентских устройствах.

Информация о существующих устройствах доступна, если существует активная политика и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в свойствах политики Агента администрирования, по умолчанию – каждые 15 минут). При создании новой политики в отсутствие активной политики список будет пустым.

Добавление устройства из списка

Параметр	Описание
Тип устройства	В раскрывающемся списке вы можете выбрать тип устройств, которые будут отображаться в таблице **Устройства, обнаруженные на клиентских устройствах**.
Маска идентификатора устройства	Поле для ввода маски идентификатора устройства.
Комментарий	Поле ввода комментария (необязательное). Поле доступно после выбора устройств и нажатия на кнопку **Далее**.

При нажатии на кнопку **Фильтр** открывается окно, в котором вы можете настроить фильтрацию отображаемой информации об устройствах.

Окно Типы устройств

В этом окне вы можете настроить правила доступа для различных типов устройств.

Правила доступа для типов устройств

Параметр	Описание

Параметры доступа к устройствам хранения данных	Таблица содержит следующие столбцы:
	• **Тип** – тип устройств (например, Жесткие диски, Принтеры).
	• **Режим доступа** – режим доступа к устройствам этого типа. Вы можете выбрать один из следующих режимов доступа:
	  • **Разрешать** – предоставить доступ к устройствам этого типа.
	  • **Блокировать** – запретить доступ к устройствам этого типа.
	  • **Зависит от шины** (значение по умолчанию) – разрешить или запретить доступ к устройствам в зависимости от режима доступа для шины, используемой для подключения устройства.
	  • **По правилам** – разрешить или запретить доступ к устройствам в зависимости от правила доступа и расписания. Правило доступа и расписание для него можно настроить, выбрав нужный тип устройства.

Параметры доступа к другим устройствам	Таблица содержит следующие столбцы:
	• **Тип** – тип устройства (например, Устройства ввода, Звуковые адаптеры).
	• **Режим доступа** – режим доступа к устройствам этого типа. Вы можете выбрать один из следующих режимов доступа:
	  • **Разрешать** – предоставить доступ к устройствам этого типа.
	  • **Блокировать** – запретить доступ к устройствам этого типа. Для сетевых адаптеров невозможно выбрать режим доступа **Блокировать**.
	  • **Зависит от шины** (значение по умолчанию) – разрешить или запретить доступ к устройствам в зависимости от режима доступа для шины, используемой для подключения устройства.

Окно Параметры доступа к устройствам

В этом окне вы можете настроить режим доступа и правила доступа для выбранного типа устройств.

Параметры доступа к устройствам

Параметр	Описание
Режим доступа к	Режим доступа к устройствам выбранного типа: • **Разрешать** – разрешать доступ к устройствам выбранного типа.

устройствам	• **Блокировать** – запрещать доступ к устройствам выбранного типа. • **Зависит от шины** (значение по умолчанию) – разрешить или запретить доступ к устройствам в зависимости от правила доступа для шины, используемой для подключения устройства. • **По правилам** – разрешить или запретить доступ к устройствам в зависимости от правила доступа и расписания.

Правила доступа к устройствам	Таблица содержит список правил доступа и состоит из следующих столбцов:
	• **Расписание доступа** – названия существующих расписаний доступа.
	• **Пользователи и/или группы пользователей** – имена пользователей или названия групп пользователей, на которых будет распространяться правило доступа.
	• **Доступ** – режим доступа для расписания:
	  • **Разрешать** (предоставить доступ к устройствам выбранного типа).
	  • **Блокировать** (запретить доступ к устройствам выбранного типа).
	• **Статус** – статус работы правила доступа:
	  • **Включено** – правило включено, Контроль устройств применяет это правило во время работы.
	  • **Выключено** – правило выключено и не используется во время работы Контроля устройств.
	По умолчанию таблица содержит расписание доступа **Расписание по умолчанию**, которое обеспечивает полный доступ к устройствам для всех пользователей (выбран вариант **\Все** в списке пользователей и групп) в любое время, если для этого типа устройства разрешен доступ по шине подключения.
	Вы можете добавлять, изменять и удалять правила доступа.
	При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.
	Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно Правило доступа к устройствам

В этом окне вы можете настроить правило доступа к устройствам.

Правило доступа к устройствам

Параметр	Описание
Параметры правила доступа к устройствам	Режим доступа к устройствам выбранного типа: • **Разрешать** (значение по умолчанию) – разрешать доступ к устройствам выбранного типа. • **Блокировать** – запрещать доступ к устройствам выбранного типа.

Пользователи и/или группы пользователей	Имя пользователя или название группы пользователей, на которых будет распространяться правило доступа. По умолчанию указано **\Все** (все пользователи). Вы можете добавлять, изменять и удалять пользователей и группы пользователей. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент.
Статус	Статус работы правила доступа: • **Включено** – правило включено, Контроль устройств применяет это правило во время работы. • **Выключено** – правило выключено и не используется во время работы Контроля устройств.
Расписание доступа к устройствам	Расписание доступа указанных пользователей к устройствам. По умолчанию указано **Расписание по умолчанию**. Вы можете указать другое расписание.

Окно Выбор пользователя или группы

В этом окне вы можете указать локального или доменного пользователя или группу пользователей, для которых вы хотите настроить правило доступа.

Настройка правила доступа

Параметр	Описание
Вручную	Если выбран этот вариант, в поле ниже вам нужно ввести имя локального или доменного пользователя или название группы пользователей, на которых будет распространяться правило доступа к устройствам.
Список групп или пользователей	Если выбран этот вариант, в поле поиска вы можете ввести критерии поиска имени пользователя или названия группы пользователей, на которых будет распространяться правило доступа к устройствам, или выбрать название группы пользователей в списке ниже.

Окно Расписания

В этом окне вы можете указать расписание для выбранного правила доступа к устройствам.

Вы можете добавлять, изменять и удалять расписания доступа.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Расписание по умолчанию удалить невозможно.

Окно Расписание доступа

В этом окне вы можете настроить расписание доступа к устройствам. Расписания можно настраивать только для жестких дисков, съемных дисков, дискет и CD/DVD-приводов.

Если в разделе **Общие параметры → Параметры приложения** флажок **Блокировать доступ к файлам во время проверки** снят, то заблокировать доступ к устройствам с помощью расписания доступа невозможно.

Расписание доступа к устройствам

Параметр	Описание
Название	Поле для ввода названия расписания доступа. Название расписания должно быть уникальным.
Интервалы времени	Таблица, в которой вы можете выбрать интервалы времени для расписания (дни и часы). Интервалы, выделенные зеленым, включены в расписание. Чтобы исключить интервал из расписания, выберите соответствующие ячейки. Исключенные из расписания интервалы выделены серым цветом. По умолчанию в расписание включены все интервалы (24/7).

Окно Шины подключения

В этом окне вы можете настроить режим доступа для шин подключения.

Режим доступа для шин подключения

Параметр	Описание
Шина подключения	Шина подключения, по которой устройства подключаются к клиентскому устройству: • **FireWire** • **USB**
Режим доступа	Переключатель определяет режим доступа к устройствам, использующим эту шину для подключения: • **Разрешать** (значение по умолчанию) – предоставлять доступ к устройствам, подключенным по этой шине подключения. • **Блокировать** – запрещать доступ к устройствам, подключенным по этой шине подключения.

Настройка контроля устройств в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры контроля устройств в свойствах политики (**Контроль безопасности → Контроль устройств**).

Параметры компонента Контроль устройств

Параметр	Описание
Включить Контроль устройств	Флажок включает или выключает компонент Контроль устройств. По умолчанию флажок установлен.
Доверенные устройства	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные устройства**. В этом окне вы можете добавить устройство в список доверенных устройств по его идентификатору или выбрав его в списке устройств, обнаруженных на клиентских устройствах.
Режим работы Контроля устройств	Режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств: • **Информировать**. При выборе этого варианта приложение Kaspersky Endpoint Security тестирует выбранный режим доступа и формирует событие об обнаружении попытки доступа к устройству. • **Блокировать** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security применяет режим доступа, заданный для устройства или шины.
Параметры Контроля устройств	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить режим доступа к устройствам в зависимости от их типа и режим доступа для шин подключения.

Окно Доверенные устройства

Таблица содержит список доверенных устройств. По умолчанию таблица пустая.

Параметры доверенного устройства

Параметр	Описание
Идентификатор устройства	Идентификатор доверенного устройства.
Имя устройства	Имя доверенного устройства.
Тип устройства	Тип доверенного устройства (например, Жесткий диск или Устройство чтения смарт-карт).
Имя клиентского устройства	Имя клиентского устройства, к которому подключено доверенное устройство.
Комментарий	Комментарий, относящийся к доверенному устройству.

Вы можете добавить устройство в список доверенных устройств по идентификатору или маске или выбрав нужное устройство в списке устройств, обнаруженных на устройстве пользователя.

Доверенные устройства в таблице можно изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

Вы также можете импортировать список устройств из файла по кнопке **Дополнительно → Импортировать** и экспортировать список добавленных устройств в файл по кнопке **Дополнительно → Экспортировать выбранное** или **Дополнительно → Экспортировать все**. При импорте вам будет предложено заменить список доверенных устройств или добавить устройства к уже существующему списку.

Окно Доверенное устройство

В этом окне вы можете добавить устройство в список доверенных устройств по его идентификатору.

Добавление устройства по идентификатору

Параметр	Описание
Идентификатор устройства	Поле для ввода идентификатора или маски идентификатора устройства, которое вы хотите добавить в список доверенных устройств. Для указания идентификатора вы можете использовать маски * (любая последовательность символов) или ? (один любой символ). Например, вы можете указать маску USBSTOR* для разрешения доступа ко всем USB-накопителям.
Найти на устройствах	По нажатию на кнопку отображаются устройства, найденные по указанному идентификатору или маске на подключенных клиентских устройствах. Кнопка доступна, если поле **Идентификатор устройства** не пустое.
Найденные устройства	Таблица содержит следующие столбцы: • **Тип устройства** – тип найденного устройства (например, Жесткий диск или Устройство чтения смарт-карт). • **Идентификатор устройства** – идентификатор найденного устройства. • **Имя устройства** – имя найденного устройства. • **Имя клиентского устройства** – имя клиентского устройства, к которому подключено найденное устройство.
Комментарий	Поле ввода комментария к устройству, которое вы хотите добавить в список доверенных устройств (необязательное).

Окно Устройства на клиентских устройствах

В этом окне вы можете добавить устройство в список доверенных, выбрав его из списка устройств, обнаруженных на клиентских устройствах.

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 отсутствие активной политики список будет пустым.

Добавление устройства из списка

Параметр	Описание
Имя клиентского устройства	Поле ввода имени или маски имени управляемого устройства, для которого вы хотите найти подключенные устройства. По умолчанию указана маска * – все управляемые устройства.
Тип устройства	В раскрывающемся списке вы можете выбрать тип подключенного устройства для поиска (например, Жесткие диски или Устройства чтения смарт-карт). По умолчанию выбран элемент **Все устройства**.
Идентификатор устройства	Поле для ввода идентификатора или маски идентификатора устройства, которое вы хотите найти. По умолчанию указана маска * – все устройства.
Поиск на устройствах	По нажатию на кнопку приложение выполняет поиск устройства с указанными параметрами. Результаты поиска отображаются в таблице ниже.

Окно Тип устройства

В этом окне вы можете настроить режим доступа для различных типов устройств.

Режим доступа для типов устройств

Параметр	Описание
Тип устройства	Тип устройства (например, Жесткие диски, Принтеры).
Режим доступа	Режим доступа к устройству. При нажатии на правую кнопку мыши открывается контекстное меню, в котором вы можете выбрать один из следующих элементов: • **Разрешать** – разрешать доступ к устройствам выбранного типа. • **Блокировать** – запрещать доступ к устройствам выбранного типа. • **Зависит от шины** (значение по умолчанию) – разрешить или запретить доступ к устройствам в зависимости от режима доступа для шины подключения. • **По правилам** – разрешить или запретить доступ к устройствам в зависимости от правила доступа и расписания.

Вы можете настроить правила доступа и расписания доступа в окне **Настройка правила доступа к устройствам**, которое открывается двойным щелчком мыши по названию типа устройства.

Окно Настройка правила доступа к устройствам

В этом окне вы можете настроить правила доступа и расписания для выбранного типа устройств.

Окно открывается по двойному щелчку на названии типа устройства в окне **Тип устройства**.

Правила доступа и расписания для устройств

Параметр	Описание
Пользователи и/или группы пользователей	Список пользователей и групп, для которых можно настроить расписание доступа. По умолчанию таблица содержит элемент **\Все** (все пользователи). Вы можете добавлять, изменять и удалять пользователей и группы пользователей.
Правила для выделенной группы пользователей по расписаниям доступа	Таблица содержит расписания доступа для пользователей и групп и состоит из следующих столбцов: • **Расписание доступа** – названия существующих расписаний доступа. Флажок рядом с расписанием показывает, используется ли это расписание в работе компонента. • **Доступ** – тип доступа для расписания: **Разрешать** (предоставить доступ к устройствам выбранного типа) или **Блокировать** (запретить доступ к устройствам выбранного типа). Расписания можно настраивать только для жестких дисков, съемных дисков, дискет и CD/DVD-приводов. По умолчанию таблица содержит расписание доступа **По умолчанию**, которое обеспечивает полный доступ к устройствам для всех пользователей (выбран элемент **\Все** в списке **Пользователи и/или группы пользователей**) в любое время, если для этого типа устройства разрешен доступ по шине подключения. Вы можете добавлять, изменять и удалять расписания доступа для выбранных пользователей. Расписание **По умолчанию** невозможно изменить или удалить. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно Пользователь или группа

В этом окне вы можете указать пользователя или группу пользователей, на которых распространяется правило доступа к устройствам.

Настройка правила доступа к устройствам

Параметр	Описание
Тип	**Пользователь** или **Группа**, на которых распространяется правило.
Имя пользователя или группы	Имя пользователя или название группы пользователей, на которых распространяется правило.

Окно Расписание доступа

В этом окне вы можете настроить расписание доступа к устройствам.

Расписание доступа к устройствам

Параметр	Описание
Название	Поле для ввода названия расписания доступа.
Интервалы	Таблица, в которой вы можете выбрать интервалы времени для расписания (дни и часы).

времени	Интервалы, выделенные зеленым, включены в расписание. Чтобы исключить интервал из расписания, выберите соответствующие ячейки. Исключенные из расписания интервалы выделены серым цветом. По умолчанию в расписание включены все интервалы (24/7).

Окно Шины подключения

В этом окне вы можете настроить режим доступа для шин подключения.

Режим доступа для шин подключения

Параметр	Описание
Шина подключения	Шина подключения, по которой устройства подключаются к клиентскому устройству: • **FireWire** • **USB**
Режим доступа	Режим доступа для шины подключения. При нажатии на правую кнопку мыши открывается контекстное меню, в котором вы можете выбрать один из следующих элементов: • **Разрешать** (значение по умолчанию) – предоставлять доступ к устройствам, подключенным по этой шине подключения. • **Блокировать** – запрещать доступ к устройствам, подключенным по этой шине подключения.

Настройка Контроля устройств в командной строке

В командной строке вы можете управлять контролем устройств с помощью предустановленной задачи Контроль устройств (*Device_Control*).

Задача Контроль устройств по умолчанию не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры контроля устройств, изменяя параметры предустановленной задачи Контроль устройств.

Вы также можете просматривать список подключенных устройств с помощью команд управления Контролем устройств.

Параметры задачи Контроль устройств

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

Параметры задачи Контроль устройств

Параметр	Описание	Знач
OperationMode	Режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств.	`Block` (значение по умо применяет режим досту устройства или шины. `Notify` – приложение т режим доступа и форми обнаружении попытки д
Секция **[DeviceClass]** содержит режимы доступа к устройствам в зависимости от их типа.		
HardDrive	Режим доступа к жестким дискам, подключенным к клиентскому устройству.	`Allow` – пользователям жестким дискам. `DependsOnBus` (значени доступ к жесткому диск доступа для шины подкл подключен диск. `Block` – пользователям всем жестким дискам (з системных жестких дис устройств не блокирует `ByRule` – доступ к жест правил доступа.
RemovableDrive	Режим доступа к съемным дискам, подключенным к клиентскому устройству.	`Allow` – пользователям съемным дискам. `DependsOnBus` (значени доступ к съемному дис доступа для шины подкл подключен диск. `Block` – пользователям съемным дискам. `ByRule` – доступ к съем правил доступа.
FloppyDrive	Режим доступа к дискетам, подключенным к клиентскому устройству. Приложение не блокирует дискеты, подключенные к клиентскому устройству с помощью шины ISA.	`Allow` – пользователям дискетам. `DependsOnBus` (значени доступ к дискете зависи для шины подключения, дискета. `Block` – пользователям дискетам. `ByRule` – доступ к диск доступа.
OpticalDrive	Режим доступа к CD/DVD-приводам, подключенным к клиентскому устройству.	`Allow` – пользователям CD/DVD-приводам. `DependsOnBus` (значени доступ к CD/DVD-приво доступа для шины подкл подключен CD/DVD-при `Block` – пользователям CD/DVD-приводам.

		`ByRule` – доступ к CD/I от правил доступа.
SerialPortDevice	Режим доступа к устройствам, подключенным к клиентскому устройству через последовательный порт. Приложение не блокирует устройства, подключенные к клиентскому устройству через последовательный порт с помощью шины ISA.	`Allow` – пользователям устройствам, подключе последовательный порт `DependsOnBus` (значени доступ к устройству, по последовательный порт доступа для шины подкл `Block` – пользователям устройствам, подключе последовательный порт
ParallelPortDevice	Режим доступа к устройствам, подключенным к клиентскому устройству через параллельный порт.	`Allow` – пользователям устройствам, подключе параллельный порт. `DependsOnBus` (значени доступ к устройству, по параллельный порт, зави для шины подключения. `Block` – пользователям устройствам, подключе параллельный порт.
Printer	Режим доступа к принтерам, подключенным к клиентскому устройству.	`Allow` – пользователям принтерам. `DependsOnBus` (значени доступ к принтеру зави для шины подключения, принтер. `Block` – пользователям принтерам.
Modem	Режим доступа к модемам, подключенным к клиентскому устройству.	`Allow` – пользователям модемам. `DependsOnBus` (значени доступ к модему зависи для шины подключения, модем. `Block` – пользователям модемам.
TapeDrive	Режим доступа к стримерам, подключенным к клиентскому устройству.	`Allow` – пользователям стримерам. `DependsOnBus` (значени доступ к стримеру зави для шины подключения, стример. `Block` – пользователям стримерам.
MultifuncDevice	Режим доступа к мультифункциональным	`Allow` – пользователям мультифункциональным

	устройствам, подключенным к клиентскому устройству.	`DependsOnBus` (значени доступ к мультифункцио зависит от режима дост подключения, по которо устройство. `Block` – пользователям мультифункциональным
SmartCardReader	Режим доступа к устройствам чтения смарт-карт, подключенным к клиентскому устройству.	`Allow` – пользователям устройствам чтения см `DependsOnBus` (значени доступ к устройству чте зависит от режима дост подключения, по которо устройство. `Block` – пользователям устройствам чтения см
WiFiAdapter	Режим доступа к Wi-Fi-адаптерам, подключенным к клиентскому устройству.	`Allow` – пользователям Wi-Fi-адаптерам. `DependsOnBus` (значени доступ к Wi-Fi-адаптеру доступа для шины подкл `Block` – пользователям Wi-Fi-адаптерам.
NetworkAdapter	Режим доступа к внешним сетевым адаптерам, подключенным к клиентскому устройству.	`Allow` – пользователям внешним сетевым адапт `DependsOnBus` (значени доступ к внешнему сете от режима доступа для которой подключен ада Контроль устройств н запрещать доступ к в адаптерам, чтобы изб клиентского устройст
PortableDevice	Режим доступа к портативным устройствам, подключенным к клиентскому устройству.	`Allow` – пользователям портативным устройстве `DependsOnBus` (значени доступ к портативному режима доступа для ши которой подключено ус `Block` – пользователям портативным устройстве
BluetoothDevice	Режим доступа к Bluetooth-устройствам, подключенным к клиентскому устройству.	`Allow` – пользователям Bluetooth-устройствам `DependsOnBus` (значени доступ к Bluetooth-устр режима доступа для ши которой подключено ус

		`Block` – пользователям Bluetooth-устройствам
ImagingDevice	Режим доступа к устройствам обработки изображений, подключенным к клиентскому устройству.	`Allow` – пользователям устройствам обработки `DependsOnBus` (значени доступ к устройству об зависит от режима дост подключения, по которо устройство. `Block` – пользователям устройствам обработки
SoundAdapter	Режим доступа к звуковым адаптерам, подключенным к клиентскому устройству.	`Allow` – пользователям звуковым адаптерам. `DependsOnBus` (значени доступ к звуковому ада режима доступа для ши которой подключено ус `Block` – пользователям звуковым адаптерам.
InputDevice	Режим доступа к устройствам ввода, подключенным к клиентскому устройству (клавиатура, мышь, тачпад и другие).	`Allow` – пользователям устройствам ввода. `DependsOnBus` (значени доступ к устройству вво доступа для шины подкл подключено устройство `Block` – пользователям устройствам ввода.
Секция **[DeviceBus]** содержит режимы доступа для шин подключения.		
USB	Режим доступа для устройств, подключенных к клиентскому устройству через USB-интерфейс.	`Allow` (значение по умо пользователям разреше устройствам. `Block` – пользователям USB-устройствам.
FireWire	Режим доступа для устройств, подключенных к клиентскому устройству через интерфейс FireWire.	`Allow` (значение по умо пользователям разреше устройствам, подключе FireWire. `Block` – пользователям устройствам, подключе FireWire.
Секция **[TrustedDevices.item_#]** содержит доверенные устройства.		
DeviceId	Идентификатор или маска идентификатора доверенного устройства.	Вы можете использоват последовательность си любой символ), чтобы у устройства. Примеры: *Чтобы запретить дос устройствам, кроме у следующие параметр*

		В секции [DeviceBus USB=Block В секции [TrustedDe параметр DeviceId= нужного устройства *Чтобы запретить дос устройствам, но разр всем USB-накопителя следующие параметр В секции [DeviceBus USB=Block В секции [TrustedDe параметр DeviceId=
Comment	Комментарий к указанному доверенному устройству.	—
Секция **[Schedules.item_#]** содержит расписание доступа для устройств. Вы можете настраивать расписа дисков, съемных дисков, дискет и CD/DVD-приводов.		
ScheduleName	Название расписания. Название расписания должно быть уникальным.	Значение по умолчанию Расписание `Default` (п обеспечивает полный д для всех пользователей для соответствующего разрешен доступ по ши Расписание `Default` уд

DaysHours	Интервалы времени для расписания.	`All` (значение по умолч
		действует 24/7 (без огр
		
		`< день недели >` – дни
		использовать как полны
		недели, так и аббревиат
		понедельника можно ук
		`Monday`). Для дней неде
		либо интервалы, либо к
		начинается с воскресен
		
		`< час >` – часы [0:24]. Дл
		указывать только интер
		
		Примеры:
		Расписание schedule_
		воскресенья по суббо
		и с 16 до 24:
		`[Schedules.item_0`
		`ScheduleName=sche`
		`DaysHours=Su-Sa:0`
		Расписание schedule_
		четвергам с 12 до 14 и
		и с 16 до 24:
		`[Schedules.item_0`

		ScheduleName=sched DaysHours=Th:12..1 Расписание schedule_ часа 7 дней в неделю: [Schedules.item_0 ScheduleName=sched DaysHours=All
Секция **[HardDrivePrincipals.item_#]** содержит правила доступа к жестким дискам. Для жестких дисков должно быть включено хотя бы одно расписание. Вы можете назначить несколько прави диску. Также для пользователя или группы пользователей можно указать несколько расписаний. Если возник доступа для пользователя или группы, предоставляются минимальные права доступа.		
Principal	Пользователь или группа пользователей, к которым применяется правило доступа.	\Everyone (значение п правило доступа приме пользователей. < имя пользователя > для которого применяет @< название группы > пользователей, для кото правило доступа.
[HardDrivePrincipals.item_#.AccessRules.item_#]	Параметры правил доступа.	—
UseRule	Показывает, включено или выключено правило.	Yes (значение по умолч доступа включено. No – правило доступа в
ScheduleName	Расписание, указанное в секции [Schedules.item_#].	Значение по умолчанию
Access	Тип доступа.	Allow (значение по умо жестким дискам разреш Block – доступ к жестк
Секция **[RemovableDrivePrincipals.item_#]** содержит правила доступа к съемным дискам. Для съемных дисков должно быть включено хотя бы одно расписание. Вы можете назначить несколько прав диску. Также для пользователя или группы пользователей можно указать несколько расписаний. Если возник доступа для пользователя или группы, предоставляются минимальные права доступа.		
Principal	Пользователь или группа пользователей, к которым применяется правило доступа.	\Everyone (значение п правило доступа приме пользователей. < имя пользователя > для которого применяет @< название группы > пользователей, для кото правило доступа.
[RemovableDrivePrincipals.item_#.AccessRules.item_#]	Параметры правил доступа.	—
UseRule	Показывает, включено или выключено правило.	Yes (значение по умолч доступа включено. No – правило доступа в

ScheduleName	Расписание, указанное в секции [Schedules.item_#].	Значение по умолчани
Access	Тип доступа.	`Allow` (значение по умо съемным дискам разре `Block` – доступ к съемн
Секция **[FloppyDrivePrincipals.item_#]** содержит правила доступа к дискетам. Для дискет должно быть включено хотя бы одно расписание. Вы можете назначить несколько правил доступ пользователя или группы пользователей можно указать несколько расписаний. Если возникает конфликт пр пользователя или группы, предоставляются минимальные права доступа.		

Principal	Пользователь или группа пользователей, к которым применяется правило доступа.	`\Everyone` (значение п
		правило доступа приме
		пользователей.
		`<имя пользователя>`
		для которого применяет
		`@<название группы>`
		пользователей, для кото
		правило доступа.

[FloppyDrivePrincipals.item_#.AccessRules.item_#]	Параметры правил доступа.	—
UseRule	Показывает, включено или выключено правило.	`Yes` (значение по умолч доступа включено. `No` – правило доступа в
ScheduleName	Расписание, указанное в секции [Schedules.item_#].	Значение по умолчани
Access	Тип доступа.	`Allow` (значение по умо дискетам разрешен. `Block` – доступ к диске
Секция **[OpticalDrivePrincipals.item_#]** содержит правила доступа к CD/DVD-приводам. Для CD/DVD-приводов должно быть включено хотя бы одно расписание. Вы можете назначить несколько пр CD/DVD-приводу. Также для пользователя или группы пользователей можно указать несколько расписаний. конфликт правила доступа для пользователя или группы, предоставляются минимальные права доступа.		

Principal	Пользователь или группа пользователей, к которым применяется правило доступа.	`\Everyone` (значение п
		правило доступа приме
		пользователей.
		`<имя пользователя>`
		для которого применяет
		`@<название группы>`
		пользователей, для кото
		правило доступа.

[OpticalDrivePrincipals.item_#.AccessRules.item_#]	Параметры правил доступа.	—
UseRule	Показывает, включено или выключено правило.	`Yes` (значение по умолч доступа включено. `No` – правило доступа в
ScheduleName	Расписание, указанное	Значение по умолчани

	в секции [Schedules.item_#].	
Access	Тип доступа.	`Allow` (значение по умо CD/DVD-приводам разр `Block` – доступ к CD/D запрещен.

Просмотр списка подключенных устройств в командной строке

Только пользователи с ролями admin и audit могут просматривать список подключенных устройств.

Чтобы просмотреть список подключенных устройств, выполните следующую команду:

```
kesl-control [-D] --get-device-list
```

Kaspersky Endpoint Security отобразит следующую информацию о подключенных устройствах:

- **Тип устройства**. Тип подключенного устройства. Например, `OpticalDrive` или `HardDrive`.
- **Идентификатор**. Идентификатор подключенного устройства.
- **Название**. Название подключенного устройства.
- **Путь**. Путь к устройству в виртуальной операционной системе sysfs.
- **Системный диск**. Параметр показывает, является ли подключенное устройство системным диском (да или нет).
- **Шина**. Шина подключения. Возможные значения: `UnknownBus`, `USB`, `FireWire`.
- **Драйвер**. Название используемого драйвера, читаемое виртуальной операционной системой sysfs.

Веб-Контроль

Веб-Контроль управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть веб-сайт, доступ к которому ограничен Веб-Контролем, приложение Kaspersky Endpoint Security блокирует доступ или показывает сообщение-предупреждение о том, что веб-сайт не рекомендован для посещения.

Kaspersky Endpoint Security контролирует только HTTP- и HTTPS-трафик.

Веб-Контроль позволяет настраивать доступ к веб-сайтам следующими способами:

- По категориям содержания. Категоризацию содержания веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз приложения). Вы можете ограничить доступ пользователей, например, к категории содержания "Социальные сети" или другим категориям.

- По категориям типов данных. Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Приложение определяет тип данных по формату файла, а не по расширению.

  Приложение не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, приложение определит тип данных "Архивы", а не "Графические файлы".

- По веб-адресу. Вы можете указать веб-адрес или маску веб-адреса.

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к категории типов данных "Файлы офисных приложений" только для категории содержания "Веб-почта".

По умолчанию для всех веб-ресурсов выбрано *правило по умолчанию* **Разрешать**. В соответствии с этим правилом Веб-Контроль разрешает пользователям доступ к веб-ресурсам, если не заданы другие *правила доступа к веб-ресурсам*.

Вы можете изменить для Веб-Контроля правило по умолчанию, согласно которому приложение будет регулировать доступ к веб-ресурсам, которые не попадают под действие других правил, и задать *правило по умолчанию* **Блокировать**. В соответствии с этим правилом Веб-Контроль запрещает пользователям доступ к веб-ресурсам, если не заданы другие *правила доступа к веб-ресурсам*.

О правилах доступа к веб-ресурсам

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое приложение выполняет при посещении пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют задать веб-ресурсы, доступ к которым контролирует компонент Веб-Контроль.

Доступны следующие фильтры:

- **Фильтр по категориям содержания**. Веб-Контроль может распределять веб-ресурсы по категориям содержания. Вы можете контролировать доступ пользователей к веб-ресурсам, имеющим определенное этими категориями содержание. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории содержания, приложение выполняет действие, указанное в правиле.

- **Фильтр по категориям типов данных**. Веб-Контроль может распределять веб-ресурсы по категориям типов данных. Вы можете контролировать доступ пользователей к размещенным на веб-ресурсах данным, относящимся к определенным типам данных. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории типов данных, приложение выполняет действие, указанное в правиле.

- **Фильтр по адресам веб-ресурсов**. Вы можете контролировать доступ пользователей ко всем адресам веб-ресурсов или к отдельным адресам веб-ресурсов и/или группам адресов веб-ресурсов.

  Если задан и фильтр по категориям содержания и/или по категориям типов данных, и фильтр по адресам веб-ресурсов, и заданные адреса веб-ресурсов и/или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типов данных, приложение контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и/или категорий типов данных, а только к заданным адресам веб-ресурсов и/или группам адресов веб-ресурсов.

- **Фильтр по именам пользователей и групп пользователей**. Вы можете задавать пользователей и/или группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом. Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

- **Расписание работы правила**. Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда приложение контролирует доступ к веб-ресурсам, указанным в правиле. Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Для каждого правила вы можете задать действие, которое Веб-Контроль выполняет при посещении пользователем веб-ресурса, удовлетворяющего параметрам правила:

- *Разрешать.* Веб-Контроль разрешает доступ пользователя к веб-ресурсу.

- *Блокировать.* Веб-Контроль запрещает доступ пользователя к веб-ресурсу и выводит сообщение о запрете доступа. По ссылкам из сообщения о блокировке пользователь может отправить сообщение-жалобу администратору локальной сети организации об ошибочной блокировке и получить доступ к запрошенному веб-ресурсу.

- *Информировать.* Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может отправить сообщение-жалобу администратору локальной сети организации об ошибочном предупреждении. При этом доступ пользователя к веб-ресурсу не блокируется.

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к этому веб-сайту по правилу с высшим приоритетом. Например, приложение может определить корпоративный портал как социальную сеть. Чтобы ограничить доступ к социальным сетям и предоставить доступ к корпоративному веб-порталу, создайте два правила: запрещающее правило для категории содержания "Социальные сети" и разрешающее правило для корпоративного веб-портала. Правило доступа к корпоративному веб-порталу должно иметь приоритет выше, чем правило доступа к социальным сетям.

Если не создано ни одного запрещающего правила, расшифровка HTTPS-трафика не выполняется.

Настройка Веб-Контроля в Web Console

В Web Console вы можете настраивать параметры Веб-Контроля в свойствах политики (**Параметры приложения** → **Контроль безопасности** → **Веб-Контроль**).

Параметры компонента Веб-Контроль

Параметр	Описание
Веб-Контроль включен / выключен	Переключатель включает или выключает компонент Веб-Контроль. По умолчанию переключатель выключен.

Список правил	Таблица содержит список правил доступа к веб-ресурсам. В процессе работы Веб-Контроль применяет правила в том порядке, в котором они указаны в таблице.
	Таблица содержит следующие столбцы:
	• **Название правила**. Название правила доступа к веб-ресурсам.
	• **Статус**. Статус работы правила доступа к веб-ресурсам:
	  • *Включено* – правило включено, Веб-Контроль применяет это правило во время работы.
	  • *Выключено* – правило выключено и не используется во время работы Веб-Контроля.
	Вы можете включить или выключить переключатель в таблице, а также установить или снять флажок **Использовать это правило** в окне **Правило Веб-Контроля**.
	• **Действие**. Действие, которое приложение будет выполнять при обнаружении попытки доступа к веб-ресурсам, удовлетворяющим правилу.
	Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.
	При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.
	Кнопка доступна, если в таблице выбран только один элемент.
	При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.
	Кнопка доступна, если в таблице выбран только один элемент.
	При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.
	Кнопка доступна, если в таблице выбран хотя бы один элемент.
	Вы также можете импортировать список правил из файла по кнопке **Импортировать** и экспортировать список добавленных правил в файл по кнопке **Экспортировать**. При импорте вам будет предложено заменить список правил или добавить правила к уже существующему списку.

Правило по умолчанию	Вы можете выбрать правило по умолчанию, согласно которому приложение будет регулировать доступ к веб-ресурсам, которые не попадают под действие других правил: • **Разрешать все, что не указано в списке правил** (значение по умолчанию) – разрешать доступ к веб-ресурсам. • **Блокировать все, что не указано в списке правил** – блокировать доступ к веб-ресурсам.
Шаблоны	**Предупреждение**. Поле ввода содержит шаблон сообщения, которое появляется при

	срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу. **Сообщение о блокировке**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу. **Сообщение администратору**. Поле ввода содержит шаблон сообщения-жалобы для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ приложение Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие *Сообщение администратору о запрете доступа к веб-странице*. Описание события содержит сообщение администратору с подставленными переменными. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

Окно Правило Веб-Контроля

В этом окне вы можете настроить параметры правила доступа к веб-ресурсам.

Добавление правила доступа к веб-ресурсам

Параметр	Описание
Название правила	Поле ввода названия правила доступа к веб-ресурсам.
Статус	Вы можете выбрать статус работы правила доступа к веб-ресурсам: • *Включено* – правило включено, Веб-Контроль применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Веб-Контроля.
Действие	Вы можете выбрать действие, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсу, удовлетворяющему правилу: • **Разрешать** (значение по умолчанию) – разрешать доступ к веб-ресурсу. • **Блокировать** – блокировать доступ к веб-ресурсу и выводить сообщение о запрете доступа. • **Информировать** – выводить предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
Фильтровать по категориям содержания	Флажок включает или выключает использование фильтра по категориям содержания. Если флажок установлен, доступна ссылка **Категории содержания**, по нажатию на которую открывается окно, в котором вы можете выбрать нужные категории содержания. По умолчанию флажок снят.
Фильтровать по категориям типов данных	Флажок включает или выключает использование фильтра по категориям содержания. Если флажок установлен, доступна ссылка **Категории типов данных**, по нажатию на которую открывается окно, в котором вы можете выбрать нужные категории типов данных.

	По умолчанию флажок снят.
Адреса	Вы можете выбрать использование фильтра адресов веб-ресурса: • **Применять ко всем адресам** (значение по умолчанию). При выборе этого варианта фильтр адресов веб-ресурсов не используется, правило Веб-Контроля применяется ко всем адресам веб-ресурсов. • **Применять к указанным адресам и/или группам**. При выборе этого варианта становятся доступны таблица адресов веб-ресурсов, на которые распространяется правило, и кнопки **Добавить адрес**, по нажатию на которую открывается окно, в котором вы можете добавить нужный адрес веб-ресурса, и **Добавить группу**, по нажатию на которую открывается окно **Группы адресов**, в котором вы можете добавить группы адресов веб-ресурсов.
Пользователи	Вы можете выбрать использование фильтра пользователей, на которых распространяется правило доступа к веб-ресурсам: • **Применять ко всем пользователям** (значение по умолчанию). При выборе этого варианта фильтр пользователей не используется, правило Веб-Контроля применяется ко всем пользователям. • **Применять к указанным пользователям и/или группам**. При выборе этого варианта становятся доступны таблица пользователей и групп пользователей, на которые распространяется правило, и кнопка **Добавить**, по нажатию на которую открывается окно **Выбор пользователя или группы**, в котором вы можете добавить нужных пользователей и/или группы пользователей.
Расписание работы правила	Расписание работы правила Веб-Контроля. По умолчанию указано расписание **Всегда**. По ссылке **Всегда** открывается окно **Расписания**, в котором вы можете настроить другое расписание работы правила.

Окно Группы адресов

Таблица содержит группы адресов веб-ресурсов, доступ пользователей к которым контролирует компонент Веб-Контроль. По умолчанию таблица пустая.

Настройка правила доступа к веб-ресурсам

Параметр	Описание
Название группы	Название группы адресов веб-ресурсов, на которые распространяется правило.
Количество адресов в группе	Количество адресов в группе адресов.

Элементы в таблице можно добавлять, изменять и удалять.

Если вы хотите добавить новую группу адресов в список групп в этом окне, откройте окно **Группа**, нажав на кнопку **Добавить**, расположенную над таблицей.

Если вы хотите добавить группу адресов в список групп в окне **Правило Веб-Контроля**, установите флажок около названия группы в таблице и нажмите на кнопку **Добавить группы в правило**, расположенную под таблицей.

Окно Группа

В этом окне вы можете добавить группу адресов веб-ресурсов.

Настройка правила доступа к веб-ресурсам

Параметр	Описание
Название группы	Название новой группы адресов веб-ресурсов.
Адреса	Таблица адресов, входящих в группу адресов веб-ресурсов.

Элементы в таблице можно добавлять, изменять, и удалять.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Выбор пользователя или группы

В этом окне вы можете указать локального или доменного пользователя или группу пользователей, для которых вы хотите настроить правило доступа к веб-ресурсам.

Настройка правила доступа к веб-ресурсам

Параметр	Описание
Вручную	Если выбран этот вариант, в поле ниже вам нужно ввести имя локального или доменного пользователя или название группы пользователей, на которых будет распространяться правило доступа к веб-ресурсам.
Список групп или пользователей	Если выбран этот вариант, в поле поиска вы можете ввести критерии поиска имени пользователя или названия группы пользователей, на которых будет распространяться правило доступа к веб-ресурсам, или выбрать название группы пользователей в списке ниже.

Окно Расписания

В этом окне вы можете указать расписание для выбранного правила доступа к устройствам.

Вы можете добавлять, изменять и удалять расписания доступа.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Расписание по умолчанию **Всегда** невозможно удалить или изменить.

Окно Расписание доступа

В этом окне вы можете настроить расписание доступа к веб-ресурсам.

Расписание доступа к веб-ресурсам

Параметр	Описание
Название	Поле для ввода названия расписания доступа. Название расписания должно быть уникальным.
Интервалы времени	Таблица, в которой вы можете выбрать интервалы времени для расписания (дни и часы). Интервалы, выделенные зеленым, включены в расписание. Чтобы исключить интервал из расписания, выберите соответствующие ячейки. Исключенные из расписания интервалы выделены серым цветом. По умолчанию в расписание включены все интервалы (24/7).

Настройка Веб-Контроля в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры Веб-Контроля в свойствах политики (**Контроль безопасности** → **Веб-Контроль**).

Параметры компонента Веб-Контроль

Параметр	Описание
Включить Веб-Контроль	Флажок включает компонент Веб-Контроль. По умолчанию флажок снят.

Параметры Веб-Контроля	Таблица содержит список правил доступа к веб-ресурсам. В процессе работы Веб-Контроль применяет правила в том порядке, в котором они указаны в таблице.
	Таблица содержит следующие столбцы:
	• **Статус**. Статус работы правила доступа к веб-ресурсам:
	  • *Включено* – правило включено, Веб-Контроль применяет это правило во время работы.
	  • *Выключено* – правило выключено и не используется во время работы Веб-Контроля.
	Вы можете установить или снять флажок в таблице, а также установить или снять флажок **Использовать это правило** в окне Правило Веб-Контроля.
	• **Действие**. Действие, которое приложение будет выполнять при обнаружении попытки доступа к веб-ресурсам, удовлетворяющим правилу.
	• **Название**. Название правила доступа к веб-ресурсам.

	Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз. При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице. Кнопка доступна, если в таблице выбран только один элемент. При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице. Кнопка доступна, если в таблице выбран только один элемент. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Вы также можете импортировать список правил из файла по кнопке **Дополнительно → Импортировать** и экспортировать список добавленных правил в файл по кнопке **Дополнительно → Экспортировать выбранное** или **Дополнительно → Экспортировать все**. При импорте вам будет предложено заменить список правил или добавить правила к уже существующему списку.
Правило по умолчанию	В раскрывающемся списке вы можете выбрать правило по умолчанию, согласно которому приложение будет регулировать доступ к веб-ресурсам, которые не попадают под действие других правил: • **Разрешать** (значение по умолчанию) – разрешать доступ к веб-ресурсам. • **Блокировать** – блокировать доступ к веб-ресурсам.
Шаблоны сообщений	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Шаблоны сообщений**.

Окно Правило Веб-Контроля

В этом окне вы можете настроить параметры правила доступа к веб-ресурсам.

Добавление правила Веб-Контроля

Параметр	Описание
Название правила	Поле ввода названия правила доступа к веб-ресурсам.
Использовать правило	Флажок включает или выключает использование этого правила во время работы приложения. Если флажок установлен, правило включено, Веб-Контроль применяет это правило во время работы. Если флажок снят, правило выключено и не используется во время работы Веб-Контроля. В дальнейшем вы можете включить использование этого правила Веб-Контролем, установив флажок. По умолчанию флажок установлен.

Фильтровать содержимое	В раскрывающемся списке вы можете выбрать фильтр содержимого веб-ресурса: • **Не фильтровать** (значение по умолчанию). При выборе этого элемента списка фильтр содержимого веб-ресурсов не используется. • **По категориям содержания**. При выборе этого элемента списка становится доступна кнопка **Выбрать**, по нажатию на которую открывается окно **Выбор категории содержания**. • **По категориям типов данных**. При выборе этого элемента списка становится доступна кнопка **Выбрать**, по нажатию на которую открывается окно **Выбор категории типов данных**. • **По категориям содержания и типов данных**. При выборе этого элемента списка становятся доступны кнопки **Выбрать**, по нажатии на которые открываются окна, в которых вы можете выбрать нужные категории.
Фильтровать адрес	В раскрывающемся списке вы можете выбрать фильтр адреса веб-ресурса: • **Любой адрес** (значение по умолчанию). При выборе этого элемента списка фильтр адресов веб-ресурсов не используется, правило Веб-Контроля применяется ко всем адресам веб-ресурсов. • **Указанные адреса**. При выборе этого элемента списка становится доступна кнопка **Выбрать адреса**, по нажатию на которую открывается окно **Выбор адресов**, в котором вы можете выбрать нужные адреса веб-ресурсов.
Применять к пользователям	В раскрывающемся списке вы можете выбрать пользователей, на которых распространяется правило доступа к веб-ресурсам: • **Ко всем пользователям** (значение по умолчанию). При выборе этого элемента списка фильтр пользователей не используется, правило Веб-Контроля применяется ко всем пользователям. • **К выбранным пользователям**. При выборе этого элемента списка становится доступна кнопка **Выбрать пользователей**, по нажатию на которую открывается окно **Выбор пользователей**.
Расписание работы правила	В раскрывающемся списке вы можете настроить расписание работы правила доступа к веб-ресурсу: • **Всегда** (значение по умолчанию). При выборе этого элемента списка настраиваемое правило доступа к веб-ресурсу применяется без ограничений по времени, то есть в любое время. • **<Название расписания>**. При выборе этого элемента списка становятся доступны кнопки **Удалить** и **Изменить**, по нажатию на которые вы можете удалить или настроить это расписание. • **Добавить новое расписание**. При выборе этого элемента списка открывается окно **Расписание доступа**, в котором вы можете настроить новое расписание работы правила доступа к веб-ресурсу.
Действие правила	В раскрывающемся списке вы можете выбрать действие, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсу, удовлетворяющему правилу: • **Разрешать** (значение по умолчанию) – разрешать доступ к веб-ресурсу.

	• **Блокировать** – блокировать доступ к веб-ресурсу и выводить сообщение о запрете доступа. • **Информировать** – выводить предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

Окно Выбор категории содержания

В этом окне вы можете выбрать категории содержания, доступ к которым вы хотите контролировать.

Для этого установите флажки около нужных категорий.

По умолчанию все флажки сняты.

При установке флажков около всех вложенных категорий содержания флажок около основной категории содержания, содержащей вложенные, автоматически не устанавливается.

Окно Выбор категории типов данных

В этом окне вы можете выбрать категории типов, доступ к которым вы хотите контролировать.

Для этого установите флажки около нужных категорий.

По умолчанию все флажки сняты.

Окно Выбор адресов

В этом окне вы можете указать адреса веб-ресурсов, доступ пользователей к которым вы хотите контролировать. Вы можете указать несколько адресов, в этом случае указывайте каждый адрес в новой строке для удобства их копирования. Для указания адресов вы можете использовать маски.

Если вы хотите указать группу адресов, откройте окно **Выбор групп адресов**, нажав на кнопку **Добавить группу адресов**.

Окно Выбор групп адресов

Таблица содержит группы адресов веб-ресурсов, доступ пользователей к которым контролирует компонент Веб-Контроль.

Если вы хотите добавить группу адресов в список групп в окне **Выбор адресов**, установите флажок около названия группы в таблице и нажмите на кнопку **Добавить**, расположенную под таблицей.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Если вы хотите добавить новую группу адресов в список групп в этом окне, откройте окно **Добавление группы адресов**, нажав на кнопку **Добавить**, расположенную над таблицей.

По умолчанию таблица пустая.

Окно Добавление группы адресов

В этом окне вы можете указать группы адресов веб-ресурсов, доступ пользователей к которым вы хотите контролировать. Вы можете указать несколько адресов в группе адресов, в этом случае указывайте каждый адрес в новой строке для удобства их копирования. Для указания адресов вы можете использовать маски.

Окно Выбор пользователей

Таблица содержит имена и группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом.

Элементы в таблице можно добавлять, изменять и удалять

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Если вы хотите добавить новую пользователя и/или группу пользователей в список пользователей в этом окне, нажав на кнопку **Добавить**, расположенную над таблицей, откройте окно **Пользователь или группа**.

По умолчанию таблица пустая.

Окно Пользователь или группа

В этом окне вы можете указать пользователя или группу пользователей, на которых распространяется правило доступа к веб-ресурсам.

Настройка правила доступа к веб-ресурсам

Параметр	Описание
Тип	**Пользователь** или **Группа**, на которых распространяется правило.
Имя пользователя или группы	Имя пользователя или название группы пользователей, на которых распространяется правило.

Окно Расписание доступа

В этом окне вы можете настроить расписание доступа к веб-ресурсам.

Параметр	Описание
Название	Поле для ввода названия расписания доступа.
Интервалы времени	Таблица, в которой вы можете выбрать интервалы времени для расписания (дни и часы). Интервалы, выделенные зеленым, включены в расписание. Чтобы исключить интервал из расписания, выберите соответствующие ячейки. Исключенные из расписания интервалы выделены серым цветом. По умолчанию в расписание включены все интервалы (24/7).

Настройка шаблонов сообщений Веб-Контроля

В зависимости от действия, заданного в свойствах правил Веб-Контроля, при попытке пользователей получить доступ к веб-ресурсам приложение выводит сообщение (подменяет ответ HTTP-сервера HTML-страницей с сообщением) одного из следующих типов:

- Сообщение-предупреждение. Такое сообщение предупреждает пользователя о том, что посещение веб-ресурса не рекомендуется и/или не соответствует корпоративной политике безопасности. Приложение выводит сообщение-предупреждение, если в параметрах правила, описывающего этот веб-ресурс, выбрано действие **Информировать**.

  Если, по мнению пользователя, предупреждение ошибочно, по ссылке из предупреждения пользователь может отправить уже сформированное сообщение-жалобу администратору локальной сети организации.

- Сообщение о блокировке веб-ресурса. Приложение выводит сообщение о блокировке веб-ресурса, если в параметрах правила, которое описывает этот веб-ресурс, выбрано действие **Блокировать**.

  Если, по мнению пользователя, блокировка доступа к веб-ресурсу была ошибочна, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить уже сформированное сообщение-жалобу администратору локальной сети организации.

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и сообщения-жалобы для отправки администратору локальной сети организации предусмотрены шаблоны. Вы можете изменять их содержание.

Чтобы изменить шаблон сообщения в Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую устройства, на которых применяется политика. Для этого нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите группу администрирования в открывшемся окне.

   В списке отобразятся политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.

   Откроется окно свойств политики.

4. В окне свойств политики выберите **Параметры приложения** → **Контроль безопасности** → **Веб-Контроль**.

5. В блоке **Шаблоны** настройте шаблоны сообщений Веб-Контроля на следующих закладках:

- **Предупреждение**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу.

- **Сообщение о блокировке**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.

- **Сообщение администратору**. Поле ввода содержит шаблон сообщения-жалобы для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ приложение Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие *Сообщение администратору о запрете доступа к веб-странице*. Описание события содержит сообщение администратору с подставленными переменными. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

На закладках **Предупреждение** и **Сообщение о блокировке** вы можете добавлять переменные и ссылки в тексты сообщений для пользователя, используя кнопки **Добавить переменную** и **Добавить ссылку**. Вы можете восстановить текст шаблона сообщения, нажав на кнопку **По умолчанию**.

6. Нажмите на кнопку **ОК**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Чтобы изменить шаблон сообщения в Консоли администрирования:

1. В дереве Консоли администрирования в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.

2. В рабочей области выберите закладку **Политики**.

3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

   Вы также можете открыть окно свойств политики с помощью пункта **Свойства** контекстного меню политики или по ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

4. В окне политики выберите **Контроль безопасности** → **Веб-Контроль**.

5. В блоке **Шаблоны сообщений** нажмите на кнопку **Настроить**.

6. В открывшемся окне **Шаблоны сообщений** настройте шаблоны сообщений Веб-Контроля на следующих закладках:

   - **Предупреждение**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу.

   - **Сообщение о блокировке**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.

   - **Жалоба администратору**. Поле ввода содержит шаблон сообщения-жалобы для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ приложение Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие *Сообщение администратору о запрете доступа к веб-странице*. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером

администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

На закладках **Предупреждение** и **Сообщение о блокировке** вы можете добавлять переменные и ссылки в тексты сообщений для пользователя, используя кнопки **Переменная** и **Вставить ссылку**. Вы можете восстановить текст шаблона сообщения, нажав на кнопку **По умолчанию**.

7. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **Применить**.

Настройка Веб-Контроля в командной строке

В командной строке вы можете управлять Веб-Контролем с помощью предустановленной задачи Веб-Контроль (*Web_Control*).

Задача Веб-Контроль по умолчанию остановлена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры Веб-Контроля, изменяя параметры предустановленной задачи Веб-Контроль.

Вы также можете просматривать и настраивать параметры Веб-Контроля с помощью команд управления Веб-Контролем.

Параметры задачи Веб-Контроль

В таблице ниже описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Веб-Контроль.

Параметры задачи Веб-Контроль

Параметр	Описание	Значения
`WebControlDefaultAction`	Правило по умолчанию, то есть действие, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсам, которые не попадают под действие других правил.	`Allow` (значение по умолчани разрешать доступ к веб-ресур `Block` – запрещать доступ к в ресурсам.
`ComplaintRecipient`	Адрес электронной почты администратора для оправки ему сообщения об ошибочной блокировке веб-ресурса.	

Секция **[Rules.item_#]** содержит следующие параметры:

`Name`	Название правила доступа к веб-ресурсам.	
`WebControlAction`	Действие правила, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсу, удовлетворяющему правилу.	`Allow` (значение по умолчани разрешать доступ к веб-ресур `Block` – запрещать доступ к в ресурсу. `Notify` – выводить предупреждение о том, что ве ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
`Enabled`	Статус работы правила доступа к веб-ресурсам.	`Yes` – правило включено, Веб-Контроль применяет это прави во время работы. `No` (значение по умолчанию) – правило выключено и не используется во время работы Веб-Контроля.
`ScheduleId`	Идентификатор расписания, который используется в секции `[Schedules.item_#]`.	
`UseUrls`	Использование в правиле фильтра адресов веб-ресурса.	`Yes` – использовать в правиле фильтр адресов веб-ресурсов `No` (значение по умолчанию) – использовать фильтр адресов ресурсов, применять правило всем адресам веб-ресурсов.
`Urls.item_#`	Адрес веб-ресурса, доступ к которому регулирует правило.	Для указания адреса веб-ресу вы можете использовать маск
`UseCategories`	Использование в правиле фильтров по категориям содержания и по категориям типов данных.	`None` (значение по умолчанию использовать фильтр содержи веб-ресурсов. `ContentOnly` – использовать правиле фильтр по категориям содержания. `FormatOnly` – использовать в правиле фильтр категориям ти данных. `ContentAndFormat` – использовать в правиле фильт категориям содержания и категориям типов данных.
`[Rules.item_#.ContentCategories.item_#]`	Секция для указания категории	–

	содержания.	
ContentCategory	Категория содержания.	AdultContent, AlcoholTobaccoNarcotics, Violence, Profanity, Weap ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepsta InternetCommunicationMedi CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileShari AudioAndVideo, BankSites, Blogs, DatingSites, LegislationR LegislationGlobal, SexuallyExplicit, Sexuality, GenerativeAITo
[Rules.item_#.FormatCategories.item_#]	Секция для указания категории типов данных.	–
FormatCategories.item_#.FormatCategory	Категория типов данных.	Video – Видео Audio – Звуковые данные OfficeDocument – Файлы офисных приложений Executable – Исполняемые ф Archives – Архивы Images – Графические файлы Scripts – Скрипты
UsePrincipals	Использование фильтра пользователей, на которых распространяется правило доступа к веб-ресурсам.	Yes – использовать в правиле фильтр пользователей. No (значение по умолчанию) – использовать фильтр пользователей, применять пра ко всем пользователям.
[Rules.item_#.Principals.item_#]	Секция для указания пользователей, на которых распространяется	

	правило доступа к веб-ресурсам.	
`Name`	Пользователь или группа пользователей, на которых распространяется правило доступа к веб-ресурсам.	`<имя пользователя>` – имя пользователя, для которого применяется правило. `@<название группы>` – назв группы пользователей, для кот применяется правило. Значение по умолчанию: прав доступа к веб-ресурсам применяется для всех пользователей.
Секция **[UrlCategories.item_#]** содержит следующие параметры:		
`Name`	Название группы адресов веб-ресурсов, доступ к которым регулирует правило.	
`Urls.item_#`	Адрес веб-ресурса, входящего в группу.	Для указания адреса веб-ресу вы можете использовать маск
Секция **[Schedules.item_#]** содержит расписание работы правила.		
`Id`	Идентификатор расписания, который используется в секции `[Rules.item_#]`.	`1 – 999999` `0` – идентификатор расписани `Default` (по умолчанию), кото обеспечивает работу правила ограничений по времени, то ее любое время.
`Name`	Название расписания.	
`DaysHours`	Интервалы времени для расписания.	`<день недели>` – дни недели можете использовать как полн названия дней недели, так и аббревиатуры (например, для понедельника можно указать I `Mon` или `Monday`). Для дней не можно указывать либо интерв либо конкретные дни. Неделя начинается с воскресенья. `<час>` – часы [0:24]. Для часо можете указывать только интервалы.

Просмотр и изменение параметров Веб-Контроля

Чтобы просмотреть параметры Веб-Контроля, выполните следующую команду:

```
kesl-control --get-settings 26 [--file <путь к конфигурационному файлу>] [--json]
```

где:

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут выведены параметры.

`--json` – выводить данные в формате JSON.

Чтобы изменить параметры Веб-Контроля, выполните следующую команду:

```
kesl-control --set-settings 26 [--file <путь к конфигурационному файлу>] [--json]
```

где:

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

`--json` – импорт данных из файла в формате JSON.

Чтобы удалить настроенные параметры и восстановить значения параметров Веб-Контроля до правила по умолчанию, выполните следующую команду:

```
kesl-control --set-settings 26 --set-to-default
```

Правила формирования масок адресов веб-ресурсов

Использование *маски адреса веб-ресурса* (далее также "маски адреса") может быть удобно в случаях, когда в процессе создания правила доступа к веб-ресурсам требуется ввести множество схожих адресов веб-ресурсов. Одна грамотно сформированная маска адреса может заменить множество адресов веб-ресурсов.

При формировании маски адреса следует использовать следующие правила:

1. Символ `*` заменяет любую последовательность из нуля или более символов.

   Например, при вводе маски адреса `*abc*` правило доступа к веб-ресурсам применяется ко всем адресам, содержащим последовательность `abc`. Пример: `http://www.example.com/page_0-9abcdef.html`.

2. Последовательность символов `*.` позволяет выбрать все домены адреса – *маска домена*. Маска домена `*.` трактуется как любое имя домена, имя поддомена или пустая строка.

   Пример: под действие маски `*.example.com` попадают следующие адреса:

   - `http://pictures.example.com` – маска домена `*.` применена для `pictures.`.
   - `http://user.pictures.example.com` – маска домена `*.` применена для `pictures.` и `user.`.
   - `http://example.com` – маска домена `*.` трактуется как пустая строка.

3. Последовательность символов `www.` в начале маски адреса трактуется как последовательность `*.`.

   Пример: маска адреса `www.example.com` трактуется как `*.example.com`. Под действие маски попадают адреса `www2.example.com` и `www.pictures.example.com`.

4. Если маска адреса начинается не с символа `*`, то содержание маски адреса эквивалентно тому же содержанию с префиксом `*.`.

5. Если маска адреса заканчивается символом, отличным от `/` или `*`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

   Пример: под действие маски адреса `http://www.example.com` попадают адреса вида `http://www.example.com/abc`, где `a`, `b`, `c` – любые символы.

6. Если маска адреса заканчивается символом `/`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

7. Последовательность символов `/*` в конце маски адреса трактуется как `/*` или пустая строка.

8. Проверка адресов веб-ресурсов по маске адреса осуществляется с учетом схемы (http или https):

   - Если сетевой протокол в маске адреса отсутствует, то под действие маски адреса попадает адрес с любым сетевым протоколом.

     Пример: под действие маски адреса `example.com` попадают адреса `http://example.com` и `https://example.com`.

   - Если сетевой протокол в маске адреса присутствует, то под действие маски адреса попадают только адреса с таким же сетевым протоколом, как у маски адреса.

     Пример: под действие маски адреса `http://*.example.com` попадает адрес `http://www.example.com` и не попадает адрес `https://www.example.com`.

9. Маска адреса, заключенная в двойные кавычки, трактуется без учета каких-либо дополнительных подстановок, за исключением символа `*`, если он изначально включен в состав маски адреса. Для масок адреса, заключенных в двойные кавычки, не выполняются правила 5 и 7 (см. примеры 14 – 18 в таблице ниже).

10. При сравнении с маской адреса веб-ресурса не учитываются имя пользователя и пароль, порт соединения и регистр символов.

Примеры применения правил формирования масок адресов

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
1	*.example.com	http://www.123example.com	Нет	См. правило 1.
2	*.example.com	http://www.123.example.com	Да	См. правило 2.
3	*example.com	http://www.123example.com	Да	См. правило 1.
4	*example.com	http://www.123.example.com	Да	См. правило 1.
5	http://www.*.example.com	http://www.123example.com	Нет	См. правило 1.
6	www.example.com	http://www.example.com	Да	См. правила 3, 2, 1.
7	www.example.com	https://www.example.com	Да	См. правила 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 3, 4, 1.

9	www.example.com	http://www.example.com/abc	Да	См. правила 3, 5, 1.
10	example.com	http://www.example.com	Да	См. правила 3, 1.
11	http://example.com/	http://example.com/abc	Да	См. правила 6.
12	http://example.com/*	http://example.com	Да	См. правило 7.
13	http://example.com	https://example.com	Нет	См. правило 8.
14	"example.com"	http://www.example.com	Нет	См. правило 9.
15	"http://www.example.com"	http://www.example.com/abc	Нет	См. правило 9.
16	"*.example.com"	http://www.example.com	Да	См. правила 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Да	См. правила 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Да	См. правила 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Нет	Маска адреса содержит больше информации, чем адрес веб-ресурса.

Контроль целостности системы

Приложение Kaspersky Endpoint Security позволяет контролировать целостность операционной системы защищаемого устройства в режиме реального времени и по требованию.

- Компонент *Контроль целостности системы* позволяет в реальном времени отслеживать изменения в файлах и директориях, которые вы включили в область мониторинга в параметрах компонента. Вы можете отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве.

- С помощью задач *Проверка целостности системы* вы можете проверять наличие изменений в файлах и директориях, которые вы включили в область мониторинга, путем сравнения текущего состояния контролируемого объекта с ранее зафиксированным состоянием.

Для использования функциональности контроля целостности системы требуется лицензия, которая включает эту функцию.

Эта функциональность не поддерживается в KESL-контейнере.

Обнаружив изменения файлов и директорий из области мониторинга, приложение Kaspersky Endpoint Security формирует события об изменениях в списках контроля доступа к объектам. Компонент Контроль целостности системы не передает данные о том, какие именно изменения внесены. Задача *Проверка целостности системы* передает данные об измененных атрибутах и перемещенных файлах и директориях.

Контроль целостности системы в реальном времени

Компонент Контроль целостности системы позволяет определять каждое изменение объекта, включенного в область мониторинга, путем перехвата файловых операций в режиме реального времени.

Во время работы компонента Контроль целостности системы приложение контролирует изменение следующих параметров файлов:

- содержимое (write (), truncate (), etc.);

- метаданные (правообладание (chmod/chown));

- отметки времени (utimensat);

- расширенные атрибуты (setxattr) и другие.

Контрольная сумма файла не рассчитывается.

Технологические ограничения операционной системы Linux не позволяют приложению определять, какой пользователь или процесс внес изменение в файл.

По умолчанию Контроль целостности системы выключен. Вы можете включать и выключать Контроль целостности системы, а также настраивать параметры работы компонента:

- Настраивать области мониторинга для контроля целостности системы. Приложение отслеживает операции с файлами в областях мониторинга, указанных в параметрах компонента Контроль целостности системы. Для работы компонента требуется указать хотя бы одну область мониторинга. По умолчанию задана область мониторинга *Внутренние объекты "Лаборатории Касперского"* (/opt/kaspersky/kesl/).

  Вы можете указать несколько областей мониторинга. Вы можете изменять области мониторинга в режиме реального времени.

  > Приложение не отслеживает изменения файлов (атрибутов и содержимого) с жесткими ссылками, которые расположены вне области мониторинга.

- Настраивать исключение объектов из мониторинга по маске имени.

- Настраивать области исключения для контроля целостности системы. Исключения задаются для каждой отдельной области мониторинга и работают только для указанной области. Вы можете указать несколько областей исключения из мониторинга.

  Исключение имеет более высокий приоритет, чем область мониторинга, исключенный объект не проверяется, даже если находится в области мониторинга. Если область мониторинга задана на более низком уровне, чем директория, указанная в исключении, то приложение не отслеживает эту область мониторинга во время контроля целостности системы.

> При добавлении директории в область мониторинга или в область исключения приложение не проверяет, существует ли такая директория.

Настройка контроля целостности системы в Web Console

В Web Console вы можете настраивать параметры контроля целостности системы в свойствах политики (**Параметры приложения** → **Контроль безопасности** → **Контроль целостности системы**).

Параметры компонента Контроль целостности системы

Параметр	Описание
Контроль целостности системы включен / выключен	Переключатель включает или выключает компонент Контроль целостности системы. По умолчанию переключатель выключен.
Области мониторинга	По ссылке **Настроить области мониторинга** открывается окно **Области мониторинга**.
Области исключения	По ссылке **Настроить области исключения из мониторинга** открывается окно **Области исключения**.
Исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**.

Окно Области мониторинга

Таблица содержит области мониторинга компонента Контроль целостности системы. Приложение контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/).

Параметры области мониторинга Контроля целостности системы

Параметр	Описание
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно добавления области мониторинга

В этом окне вы можете добавить или настроить область мониторинга для компонента Контроля целостности системы.

Параметры области мониторинга

Параметр	Описание
Название области	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна **Области мониторинга**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение контролирует эту область мониторинга во время работы.

	Если флажок снят, приложение не контролирует эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Для указания пути вы можете использовать маски. Поле не должно быть пустым. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Области исключения

Таблица содержит области исключения из мониторинга для компонента Контроль целостности системы. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли приложение эту область из мониторинга при работе компонента.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения из мониторинга для компонента Контроль целостности системы.

Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы приложения. Если флажок установлен, приложение исключает эту область из мониторинга во время работы компонента. Если флажок снят, приложение контролирует эту область во время работы компонента. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски. Поле не должно быть пустым.

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек). Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение исключает из мониторинга. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Приложение не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Настройка контроля целостности системы в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры контроля целостности системы в свойствах политики (**Контроль безопасности** → **Контроль целостности системы**).

Параметры компонента Контроль целостности системы

Параметр	Описание
Включить Контроль целостности системы	Флажок включает или выключает Контроль целостности системы. По умолчанию флажок снят.
Области мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки**.
Исключения из мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске**.

Окно Области проверки

Таблица содержит области мониторинга для компонента Контроль целостности системы. Приложение 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 мониторинга

Параметр	Описание
Название области	Название области мониторинга.

Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить области мониторинга для компонента Контроль целостности системы.

Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение контролирует эту область мониторинга во время работы приложения. Если флажок снят, приложение не контролирует эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая	Поле ввода пути к локальной директории, которую вы хотите включить в область

система, протокол доступа и путь	мониторинга. Поле не должно быть пустым. По умолчанию указан путь /opt/kaspersky/kesl.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Области исключения

Таблица содержит области исключения из мониторинга для компонента Контроль целостности системы. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли приложение эту область из мониторинга при работе компонента.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно <Название области исключения>

В этом окне вы можете добавить или настроить область исключения из мониторинга для компонента Контроль целостности системы.

Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы приложения. Если флажок установлен, приложение исключает эту область из мониторинга во время работы компонента. Если флажок снят, приложение контролирует эту область во время работы компонента. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Поле не должно быть пустым. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение исключает из мониторинга. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки. Примеры: Маска `*.txt` – все текстовые файлы. Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Приложение не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Настройка контроля целостности системы в командной строке

В командной строке вы можете управлять контролем целостности системы в реальном времени с помощью предустановленной задачи Контроль целостности системы (*System_Integrity_Monitoring*). Тип задачи – *OAFIM*.

Задача Контроль целостности системы по умолчанию не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры контроля целостности системы на устройстве, изменяя параметры предустановленной задачи Контроль целостности системы.

Параметры задачи Контроль целостности системы при доступе

Параметр	Описание	Значения
`UseExcludeMasks`	Включение исключения из области мониторинга объектов, указанными параметром `ExcludeThreats.item_#`. Этот параметр работает, только если указано значение параметра `ExcludeMasks.item_#`.	`Yes` – исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга. `No` (значение по умолчанию) – не исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга.

`ExcludeMasks.item_#`	Исключение из мониторинга объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`. Вы можете указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом.	Значение по умолчанию не задано.
Секция **[ScanScope.item_#]** содержит области мониторинга для задачи Контроль целостности системы. Для задачи должна быть указана минимум одна область мониторинга. Вы можете указать несколько секций [ScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области мониторинга, содержит дополнительную информацию об области мониторинга.	Значение по умолчанию не задано.
`UseScanArea`	Включение мониторинга указанной области.	`Yes` (значение по умолчанию) – контролировать указанную область. `No` – не контролировать указанную область.
`Path`	Путь к директории для мониторинга.	Для указания пути вы можете использовать маски.

		Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Значение по умолчанию: /opt/kaspersky/kesl/
AreaMask.item_#	Ограничение области мониторинга. В области мониторинга приложение проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (контролировать все объекты).
Секция **[ExcludedFromScanScope.item_#]** содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#].Вы можете указать несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области исключения из мониторинга, содержит дополнительную информацию об области исключения из мониторинга.	Значение по умолчанию не задано.

`UseScanArea`	Исключение указанной области из мониторинга.	`Yes` (значение по умолчанию) – исключать указанную область из мониторинга. `No` – не исключать указанную область из мониторинга.
`Path`	Путь к директории с объектами, исключаемыми из мониторинга.	Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. Значение по умолчанию не задано.
`AreaMask.item_#`	Ограничение области исключения из мониторинга. В области исключения из мониторинга приложение исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (исключать из мониторинга все объекты).

Проверка целостности системы

Во время выполнения задачи *Проверка целостности системы* изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием. Сравнение может выполняться по следующим критериям:

- хеш файла;
- время изменения файла;
- размер файла.

Исходное состояние контролируемых объектов фиксируется в качестве *снимка состояния системы*. Снимок состояния системы содержит пути к контролируемым объектам и их метаданные.

Снимок состояния системы может содержать персональные данные.

Снимок состояния системы создается во время первого выполнения задачи проверки целостности системы на устройстве. Если вы создали несколько задач проверки целостности системы, для каждой задачи создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы содержит информацию об объектах, которые относятся к области мониторинга, настроенной для задачи. Если снимок состояния системы не соответствует области мониторинга, приложение Kaspersky Endpoint Security формирует событие о нарушении целостности системы.

Снимок состояния системы обновляется при изменении параметров задачи, например, при добавлении новой области мониторинга.

Приложение создает хранилище для снимков состояния системы на защищаемом устройстве. 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.

Вы можете удалить снимок состояния системы, удалив соответствующую задачу проверки целостности системы.

Вы можете запускать проверку целостности системы по требованию и настраивать параметры проверки:

- Включать и выключать обновление снимка состояния системы каждый раз после завершения задачи проверки целостности системы.
- Выбирать критерии, по которым выполняется сравнение текущего состояния контролируемого файла с исходным состоянием: использовать хеш и время изменения файла или только размер файла.
- Настраивать области мониторинга для проверки целостности системы.
- Настраивать области исключения из проверки целостности системы. Вы можете указывать пути к исключаемым файлам и директориям и исключать отдельные объекты по маске имени.

Проверка целостности системы в Web Console

В Web Console вы можете выполнять проверку целостности системы с помощью задачи *Проверка целостности системы*.

Вы можете создавать и запускать пользовательские задачи проверки целостности системы. Вы можете настраивать параметры проверки, изменяя параметры задач.

Параметры задачи Проверка целостности системы

Параметр	Описание
Обновлять снимок состояния системы при каждом запуске задачи	Флажок включает или выключает обновление снимка состояния системы при каждом запуске задачи *Проверка целостности системы*. По умолчанию флажок снят.
Использовать хеш SHA256 для проверки	Флажок включает или выключает использование хеша файла в качестве критерия для сравнения текущего состояния файла с исходным состоянием. Если флажок снят, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром). По умолчанию флажок снят.
Проверять директории в областях мониторинга	Флажок включает или выключает проверку директорий во время выполнения проверки целостности системы. По умолчанию флажок снят.
Отслеживать время последнего доступа к файлу	Флажок включает или выключает отслеживание времени доступа к файлу во время выполнения проверки целостности системы. По умолчанию флажок снят.
Области мониторинга	Таблица, содержащая области мониторинга, проверяемые задачей. По умолчанию таблица содержит область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/). Области мониторинга в таблице можно добавлять, настраивать, удалять, перемещать вверх и вниз. При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице. Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую. Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

При нажатии на название области проверки открывается окно **<Название области проверки>**. В этом окне вы можете изменить параметры выбранной области проверки.

При нажатии на кнопку **Добавить** открывается окно **<Новая область проверки>**. В этом окне вы можете задать новую область проверки.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область мониторинга для задачи Проверка целостности системы.

Параметры области мониторинга

Параметр	Описание
Название области	Поле ввода названия области мониторинга. Это название будет отображаться в таблице раздела **Параметры проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение контролирует эту область мониторинга во время работы приложения. Если флажок снят, приложение не контролирует эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Для указания пути вы можете использовать маски.

	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file*/` или `/dir/file**/`. Маску ** можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле не должно быть пустым. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Раздел Области исключения

В разделе **Области исключения** для задачи Проверка целостности системы вы можете настроить области исключения из проверки и исключения по маске.

Окно Области исключения

Таблица содержит области исключения из мониторинга для задачи Проверка целостности системы. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли приложение эту область из мониторинга при работе задачи.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения из мониторинга для задачи Проверка целостности системы.

Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы приложения. Если флажок установлен, приложение исключает эту область из мониторинга во время работы задачи. Если флажок снят, приложение контролирует эту область во время работы задачи. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски.

	Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. Поле не должно быть пустым. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение исключает из мониторинга. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Приложение не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Проверка целостности системы в Консоли администрирования

В Консоли администрирования вы можете выполнять проверку целостности системы с помощью задачи *Проверка целостности системы*.

Вы можете создавать и запускать пользовательские задачи проверки целостности системы. Вы можете настраивать параметры проверки, изменяя параметры задач.

В разделе **Параметры** в свойствах задачи Проверка целостности системы вы можете настроить параметры, приведенные в таблице ниже.

Параметры задачи Проверка целостности системы

Параметр	Описание
Обновлять снимок состояния системы при каждом запуске задачи	Флажок включает или выключает обновление снимка состояния системы при каждом запуске задачи Проверка целостности системы. По умолчанию флажок снят.
Использовать хеш (SHA256) для проверки	Флажок включает или выключает использование хеша файла в качестве критерия для сравнения текущего состояния файла с исходным состоянием. Если флажок снят, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром). По умолчанию флажок снят.
Проверять директории в областях мониторинга	Флажок включает или выключает проверку директорий в указанных областях мониторинга во время выполнения проверки целостности системы. По умолчанию флажок снят.
Отслеживать время последнего доступа к файлу	Флажок включает или выключает отслеживание времени доступа к файлу во время выполнения проверки целостности системы. По умолчанию флажок снят.
Области мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки**.

В разделе **Области исключения** в свойствах задачи Проверка целостности системы вы можете настроить области исключения из мониторинга и исключения по маске.

Окно Области проверки

Таблица содержит области мониторинга для задачи Проверка целостности системы. Приложение 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 мониторинга

Параметр	Описание
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Кнопка доступна, если в таблице выбран только один элемент.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить области мониторинга для задачи Проверка целостности системы.

Параметры области мониторинга

Параметр	Описание

Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение контролирует эту область мониторинга во время работы приложения. Если флажок снят, приложение не контролирует эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. Поле не должно быть пустым. По умолчанию указан путь /opt/kaspersky/kesl.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне. При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Раздел Области исключения

Параметры исключений из проверки

Блок параметров	Описание
Исключения из мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключений из мониторинга.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из мониторинга по маске имени.

Окно Области исключения

Таблица содержит области исключения из проверки для задачи Проверка целостности системы. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения из проверки задачи Проверка целостности системы

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, исключает ли приложение эту область из поверки при работе задачи.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Окно <Новая область исключения>

В этом окне вы можете добавить или настроить область исключения из мониторинга для задачи Проверка целостности системы.

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы приложения. Если флажок установлен, приложение исключает эту область из мониторинга во время работы задачи. Если флажок снят, приложение контролирует эту область во время работы задачи. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. Поле не должно быть пустым. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение исключает из мониторинга. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы один элемент. Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Приложение не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Проверка целостности системы в командной строке

В командной строке вы можете выполнять проверку целостности системы на устройстве с помощью пользовательских задач *Проверка целостности системы* (задач типа *ODFIM*).

Вы можете запускать, останавливать, приостанавливать и возобновлять пользовательские задачи вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки целостности системы, изменяя параметры этих задач.

Параметры задачи Проверка целостности системы

Параметр	Описание	Значения
`RebuildBaseline`	Включение обновления снимка состояния системы после завершения задачи *Проверка целостности системы*.	`Yes` – обновлять снимок состояния системы каждый раз после завершения задачи *Проверка целостности системы*. `No` (значение по умолчанию) – не обновлять снимок состояния системы каждый раз после завершения задачи *Проверка целостности системы*.
`CheckFileHash`	Использовать хеш файла (SHA256) в качестве критерия, по которому выполняется сравнение текущего состояния контролируемого файла с исходным состоянием.	`Yes` – проверять хеш. `No` (значение по умолчанию) – выключить проверку хеша. Если проверка выключена, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром).
`TrackDirectoryChanges`	Включение мониторинга директорий.	`Yes` – контролировать директории во время выполнения проверки целостности системы. `No` (значение по умолчанию) – не контролировать директории.
`TrackLastAccessTime`	Включение проверки времени последнего доступа к файлу. В операционных системах Linux это параметр `noatime`.	`Yes` – проверять время последнего доступа к файлу. `No` (значение по умолчанию) – не проверять время последнего доступа к файлу.
`UseExcludeMasks`	Включение исключения из области мониторинга объектов, указанными параметром `ExcludeMasks.item_#`. Этот параметр работает, только если указано значение параметра `ExcludeMasks.item_#`.	`Yes` – исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга. `No` (значение по умолчанию) – не исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга.
`ExcludeMasks.item_#`	Исключение из мониторинга объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`. Вы можете указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом.	Значение по умолчанию не задано.

Секция **[ScanScope.item_#]** содержит области мониторинга для задачи *Проверка целостности системы*. Для задачи должна быть указана минимум одна область мониторинга. Вы можете указать несколько секций [ScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.

Секция [ScanScope.item_#] содержит следующие параметры:

`AreaDesc`	Описание области мониторинга, содержит дополнительную информацию об области мониторинга.	Значение по умолчанию не задано.
`UseScanArea`	Включение мониторинга указанной области.	`Yes` (значение по умолчанию) – контролировать указанную область. `No` – не контролировать указанную область.
`Path`	Путь к директории для мониторинга.	Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. Значение по умолчанию: /opt/kaspersky/kesl/

`AreaMask.item_#`	Ограничение области мониторинга. В области мониторинга приложение проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (контролировать все объекты).
Секция **[ExcludedFromScanScope.item_#]** содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#]. Вы можете указать несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области исключения из мониторинга, содержит дополнительную информацию об области исключения из мониторинга.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из мониторинга.	`Yes` (значение по умолчанию) – исключать указанную область из мониторинга. `No` – не исключать указанную область из мониторинга.
`Path`	Путь к директории с объектами, исключаемыми из мониторинга.	Для указания пути вы можете использовать маски.

		Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Значение по умолчанию не задано.
AreaMask.item_#	Ограничение области исключения из мониторинга. В области исключения из мониторинга приложение исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов AreaMask.item_# в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: * (исключать из мониторинга все объекты).

Анализ поведения

Компонент Анализ поведения позволяет контролировать вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности Kaspersky Endpoint Security может завершать процесс приложения, осуществляющего вредоносную активность.

Эта функциональность не поддерживается в KESL-контейнере.

Компонент Анализ поведения включается автоматически с параметрами по умолчанию при запуске приложения Kaspersky Endpoint Security.

Вы можете включать и выключать Анализ поведения, а также настраивать параметры работы компонента:

- Выбирать действие, которое Kaspersky Endpoint Security будет выполнять при обнаружении вредоносной активности в операционной системе: информировать пользователя или блокировать приложение, осуществляющее вредоносную активность.
- Исключать активность процессов из проверки.

Если включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response, исключения по процессам не применяются при анализе поведения приложений в операционной системе.

По умолчанию на операционной системе СинтезМ-Клиент конфигурация службы auditd заблокирована против изменений, то есть находится в режиме работы `enabled 2`. Для корректной работы компонента Анализ поведения при интеграции Kaspersky Endpoint Security с решениями Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform требуется изменить режим работы auditd в конфигурационных файлах на режим без блокировки конфигурации `enabled 1` и перезагрузить операционную систему.

Настройка анализа поведения в Web Console

В Web Console вы можете настраивать параметры анализа поведения приложений в свойствах политики (**Параметры приложения** → **Продвинутая защита** → **Анализ поведения**).

Параметры компонента Анализ поведения

Параметр	Описание
Анализ поведения включен / выключен	Переключатель включает или выключает компонент Анализ поведения. По умолчанию переключатель включен.
Действие при обнаружении вредоносной активности	Действие, которое Kaspersky Endpoint Security будет выполнять при обнаружении вредоносной активности в операционной системе: • **Информировать** пользователя. Kaspersky Endpoint Security не завершает процесс, осуществляющий вредоносную активность, только записывает событие об обнаружении вредоносной активности в журнал событий. • **Блокировать** приложение, осуществляющее вредоносную активность (значение по умолчанию). Kaspersky Endpoint Security завершает процесс, осуществляющий

	вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности.
Исключения по процессам	По ссылке **Настроить исключения по процессам** открывается окно **Исключения по процессам**. В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса и файлов, изменяемых указанным процессом. По умолчанию таблица пуста.

Если включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response, исключения по процессам не применяются.

Параметры области исключения по процессам

Параметр	Описание
Исключать / Не исключать из проверки доверенные процессы	Переключатель включает или выключает использование настроенных исключений по процессам в работе компонента Анализ поведения. По умолчанию переключатель выключен.
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Вы также можете импортировать список исключений из файла по кнопке **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Экспортировать**. При импорте вам будет предложено заменить список исключений или добавить исключения к уже существующему списку.

Окно добавления области исключения по процессам

В этом окне вы можете добавить или настроить область исключения по процессам.

Параметры области исключения

Параметр	Описание
Название области	Поле ввода названия области исключения по процессам. Это название будет отображаться в таблице окна **Исключения по процессам**.

исключения по процессам	Поле ввода не должно быть пустым.
Использовать это исключение	Флажок включает или выключает исключение этой области во время работы приложения. По умолчанию флажок установлен.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки. Для указания пути вы можете использовать маски. Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле ввода не должно быть пустым.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром **Путь к исключаемому процессу**. По умолчанию флажок снят.

Настройка анализа поведения в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры анализа поведения приложений в свойствах политики (**Продвинутая защита** → **Анализ поведения**).

Параметры компонента Анализ поведения

Параметр	Описание
Включить Анализ поведения	Флажок включает или выключает компонент Анализ поведения. По умолчанию флажок установлен.
Действие при обнаружении вредоносной активности	Действие, которое Kaspersky Endpoint Security будет выполнять при обнаружении вредоносной активности в операционной системе: • **Блокировать** приложение, осуществляющее вредоносную активность (значение по умолчанию). Kaspersky Endpoint Security завершает процесс, осуществляющий вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности. • **Информировать** пользователя. Kaspersky Endpoint Security не завершает процесс, осуществляющий вредоносную активность, только записывает событие об обнаружении вредоносной активности в журнал событий.

Использовать исключения по процессам	Флажок включает или выключает использование исключений по процессам в работе компонента Анализ поведения. По умолчанию флажок снят. По кнопке **Настроить** открывается окно **Исключения по процессам**. В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Исключения по процессам

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса из проверки. По умолчанию таблица пуста.

Если включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response, исключения по процессам не применяются.

Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно → Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно → Экспортировать выбранное** или **Дополнительно → Экспортировать все**. При импорте вам будет предложено заменить список исключений или добавить исключения к уже существующему списку.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Исключения по процессам**.
Путь к исключаемому	Полный путь к процессу, который вы хотите исключить из проверки. Для указания пути вы можете использовать маски.

процессу	Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file. Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/. Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска. Вы можете использовать символ ? вместо любого одного символа в имени файла или директории. Поле ввода не должно быть пустым.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром **Путь к исключаемому процессу**. По умолчанию флажок снят.
Использовать эту область	Флажок включает или выключает исключение этой области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область во время работы. Если флажок снят, приложение включает эту область во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.

Настройка анализа поведения в командной строке

В командной строке вы можете управлять анализом поведения приложений в операционной системе с помощью предустановленной задачи Анализ поведения (*Behavior_Detection*).

Задача Анализ поведения по умолчанию запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры анализа поведения, изменяя параметры предустановленной задачи Анализ поведения.

Параметры задачи Анализ поведения

Параметр	Описание	Значения
TaskMode	Действие, выполняемое приложением при обнаружении вредоносной активности в операционной системе.	Block (значение по умолчанию) – завершать процесс приложения, осуществляющего вредоносную активность. Notify – не завершать процесс, осуществляющий вредоносную активность, только регистрировать обнаружение вредоносной активности в журнале событий.
UseTrustedPrograms	Исключение процессов	Yes – исключать из проверки активность

	из проверки.	указанных процессов. `No` (значение по умолчанию) – проверять все процессы.
Секция **[TrustedPrograms.item_#]** содержит процессы, которые исключаются из проверки. Приложение Kaspersky Endpoint Security не контролирует активность указанных процессов.		
`ProgramPath`	Путь к исключаемому процессу.	`<полный путь к процессу>` – исключать из проверки процесс в указанной локальной директории. Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.
`ApplyToDescendants`	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром `ProgramPath`.	`Yes` – исключать из проверки указанный процесс и все его дочерние процессы. `No` (значение по умолчанию) – исключать из проверки только указанный процесс, не исключать из проверки дочерние процессы.
`ProgramDesc`	Описание исключаемого процесса.	
`UseTrustedProgram`	Включение исключения указанного процесса из проверки.	`Yes` (значение по умолчанию) – включить исключение активности указанного процесса из проверки. `No` – не включать исключение активности указанного процесса из проверки.

Использование Kaspersky Security Network

Функциональность KSN будет недоступна в приложении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

Для повышения эффективности защиты устройств и данных пользователей приложение Kaspersky Endpoint Security может использовать облачную базу знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения – Kaspersky Security Network (KSN). Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции на различные угрозы, высокую производительность компонентов защиты и снижение количества ложных срабатываний.

Использование Kaspersky Security Network является добровольным. Вы можете включить или выключить использование KSN в любой момент.

Функциональность KSN не поддерживается в KESL-контейнере.

Инфраструктурные решения Kaspersky Security Network

Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network (KSN)* – это решение, которое позволяет получать информацию от "Лаборатории Касперского", а также отправлять в "Лабораторию Касперского" данные об объектах, обнаруженных на устройствах пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.

- *Kaspersky Private Security Network (KPSN)* – это решение, которое позволяет пользователям устройств с установленным приложением Kaspersky Endpoint Security получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих устройств. KPSN разработан для корпоративных клиентов, не имеющих возможности использовать Kaspersky Security Network, например, по следующим причинам:

  - отсутствие подключения локальных рабочих мест к интернету;

  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

После активации приложения по новой лицензии для использования KPSN требуется предоставить поставщику услуг информацию о новом лицензионном ключе. В противном случае обмен информацией с KPSN будет невозможен из-за ошибки аутентификации.

Варианты использования Kaspersky Security Network

Существует два варианта использования KSN:

- **Расширенный режим KSN** – вы можете получать информацию из базы знаний "Лаборатории Касперского", при этом приложение Kaspersky Endpoint Security автоматически отправляет в Kaspersky Security Network статистическую информацию, полученную в результате своей работы. Также приложение может отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или

части файлов), которые злоумышленники могут использовать для нанесения вреда устройству или данным.

- **Стандартный режим KSN** – вы можете получать информацию из базы знаний "Лаборатории Касперского", при этом приложение Kaspersky Endpoint Security не отправляет анонимную статистику и данные о типах и источниках угроз.

Вы можете в любой момент выбрать другой вариант использования Kaspersky Security Network.

Сбор, обработка и хранение персональных данных пользователя не производится. Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского". Файл с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Облачный режим работы Kaspersky Endpoint Security

Облачный режим – это режим работы приложения Kaspersky Endpoint Security, при котором используется облегченная версия баз вредоносного ПО. Это позволяет снизить нагрузку на оперативную память устройства.

Работу приложения с облегченными базами вредоносного ПО обеспечивает Kaspersky Security Network.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме и вы используете KSN в работе приложения, вы можете включать облачный режим работы приложения.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, работа с облегченными базами вредоносного ПО не поддерживается. Приложение получает от Сервера защиты специальные базы, необходимые для работы Легкого агента.

Kaspersky Endpoint Security переходит к использованию облегченной версии баз вредоносного ПО после включения облачного режима и выполнения очередного обновления баз и модулей приложения. Если облачный режим выключается, Kaspersky Endpoint Security загружает полную версию баз приложения с серверов "Лаборатории Касперского" в ходе очередного обновления баз и модулей приложения.

Если вы не используете KSN или облачный режим выключен, Kaspersky Endpoint Security использует полную версию баз приложения.

Облачный режим выключается автоматически, если выключено использование KSN.

Использование службы прокси-сервера KSN

Устройства пользователей, работающие под управлением Сервера администрирования, могут взаимодействовать с KSN напрямую или при помощи службы прокси-сервера KSN.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, взаимодействие с инфраструктурой KSN обеспечивает служба прокси-сервера KSN. Взаимодействие с KSN напрямую не поддерживается. Если прокси-сервер KSN недоступен, KSN не используется в работе приложения.

Прокси-сервер KSN предоставляет следующие возможности:

- Устройство пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение устройством пользователя запрошенной информации.

Параметры прокси-сервера KSN вы можете настроить в свойствах Сервера администрирования. Подробнее о прокси-сервере KSN см. в справке Kaspersky Security Center.

Настройка использования Kaspersky Security Network в Web Console

В Web Console вы можете настраивать использование Kaspersky Security Network в работе приложения Kaspersky Endpoint Security в свойствах политики (**Параметры приложения** → **Продвинутая защита** → **Kaspersky Security Network**).

Текст Положения о Kaspersky Security Network вы можете прочитать в окне **Положение о Kaspersky Security Network**, которое можно открыть по ссылке **Положение о Kaspersky Security Network**.

Информация о доступности KSN отображается в Kaspersky Security Center с помощью статуса клиентского устройства (*OK, Критический, Предупреждение*) в списке управляемых устройств на закладке **Активы (Устройства)**.

Параметры использования Kaspersky Security Network

Параметр	Описание
Не использовать KSN	Выбирая этот вариант, вы отказываетесь от использования Kaspersky Security Network.
Расширенный режим KSN	Выбирая этот вариант, вы принимаете условия использования 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 в "Лабораторию Касперского" будет отправляться анонимная статистика и данные о типах и источниках различных угроз.
Стандартный режим KSN	Выбирая этот вариант, вы принимаете условия использования Kaspersky Security Network. Вы сможете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения.
Включить облачный режим	Флажок включает или выключает режим работы, при котором приложение Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО. Флажок доступен, если включено использование KSN. Флажок установлен, если при создании политики вы приняли условия Положения о Kaspersky Security Network и используете расширенный режим KSN. Режим включается или выключается после следующего обновления баз приложения. Параметр применяется, только если приложение используется в стандартном режиме.
Использовать	Флажок включает или выключает возможность взаимодействовать с серверами KSN

серверы KSN, если прокси-сервер KSN недоступен	напрямую, когда служба прокси-сервера KSN недоступна. По умолчанию флажок установлен. Параметр применяется, только если приложение используется в стандартном режиме.
Положение о Kaspersky Security Network	По ссылке открывается окно **Положение о Kaspersky Security Network**, в котором вы можете прочитать текст Положения о Kaspersky Security Network.

Положение о Kaspersky Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Security Network и принять его условия.

Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите использовать Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Security Network.
Я не принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите использовать Kaspersky Security Network.

Положение о Kaspersky Private Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Private Security Network и принять его условия.

Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите использовать Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Private Security Network.
Я не принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите использовать Kaspersky Security Network.

Настройка использования Kaspersky Security Network в Консоли администрирования

В Консоли администрирования вы можете настраивать использование Kaspersky Security Network в работе приложения Kaspersky Endpoint Security в свойствах политики (**Продвинутая защита → Kaspersky Security Network**).

Текст Положения о Kaspersky Security Network вы можете прочитать в окне **Положение о Kaspersky Security Network**, которое можно открыть по ссылке **Положение о Kaspersky Security Network**.

Информация о доступности KSN отображается в Kaspersky Security Center с помощью статуса клиентского устройства (*OK, Критический, Предупреждение*) в списке управляемых устройств на закладке **Устройства**.

Параметры использования Kaspersky Security Network

Параметр	Описание
Положение о Kaspersky Security Network	По ссылке открывается окно **Положение о Kaspersky Security Network**. В этом окне вы можете просмотреть текст Положения о Kaspersky Security Network.
Kaspersky Security Network (KSN)	В блоке отображается информация о режиме использования KSN или о том, что KSN не используется в работе Kaspersky Endpoint Security. По кнопке **Изменить** открывается окно, в котором вы можете настроить использование Kaspersky Security Network.
Включить облачный режим	Флажок включает или выключает режим работы, при котором приложение Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО. Флажок доступен, если включено использование KSN. Флажок установлен, если при создании политики вы приняли условия Положения о Kaspersky Security Network и используете расширенный режим KSN. Режим включается или выключается после следующего обновления баз приложения. Параметр применяется, только если приложение используется в стандартном режиме.
Использовать серверы KSN, если прокси-сервер KSN недоступен	Флажок включает или выключает возможность взаимодействовать с серверами KSN напрямую, когда служба прокси-сервера KSN недоступна. По умолчанию флажок установлен. Параметр применяется, только если приложение используется в стандартном режиме.

Параметры Kaspersky Security Network

В этом окне вы можете настроить параметры использования Kaspersky Security Network.

Параметры Kaspersky Security Network

Параметр	Описание
Подробнее...	По ссылке открывается веб-сайт "Лаборатории Касперского".
Не использовать	Выбирая этот вариант, вы отказываетесь от использования Kaspersky Security Network.

Kaspersky Security Network	
Стандартный режим KSN	Выбирая этот вариант, вы принимаете условия использования Kaspersky Security Network. Вы можете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения.
Расширенный режим KSN	Выбирая этот вариант, вы принимаете условия использования Kaspersky Security Network. Вы можете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Кроме того, для улучшения работы Kaspersky Security Network в "Лабораторию Касперского" будет отправляться анонимная статистика и данные о типах и источниках различных угроз.
Положение о Kaspersky Security Network	По ссылке открывается окно **Положение о Kaspersky Security Network**, **в котором** вы можете прочитать текст Положения о Kaspersky Security Network.

Положение о Kaspersky Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Security Network и принять его условия.

Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите использовать Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Security Network. Вариант доступен, если в окне **Параметры Kaspersky Security Network** вы выбрали вариант **Стандартный режим KSN** или **Расширенный режим KSN**.
Я не принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите использовать Kaspersky Security Network. Вариант доступен, если в окне **Параметры Kaspersky Security Network** вы выбрали вариант **Стандартный режим KSN** или **Расширенный режим KSN**.

Положение о Kaspersky Private Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Private Security Network и принять его условия.

Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите использовать Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Private Security Network.
Я не принимаю условия Положения	Выбирая этот вариант, вы подтверждаете, что вы не хотите

о Kaspersky Security Network	использовать Kaspersky Security Network.

Настройка использования Kaspersky Security Network в командной строке

В командной строке вы можете включать и выключать использование Kaspersky Security Network с помощью параметра `UseKSN` из общих параметров приложения.

Вы можете изменять значение параметра `UseKSN` с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Чтобы включить использование Kaspersky Security Network с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

где:

- `<Extended/Basic>` – режим использования Kaspersky Security Network.
- `--accept-ksn` – ключ, означающий, что вы соглашаетесь с условиями, изложенными в Положении о Kaspersky Security Network. Вы подтверждаете, что полностью прочитали, понимаете и принимаете условия Положения о Kaspersky Security Network.

Файл ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network находится в директории /opt/kaspersky/kesl/doc/.

Чтобы выключить использование Kaspersky Security Network с помощью ключей командной строки, 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> [--json] [--
accept-ksn]
```

где:

- `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу с общими параметрами приложения, в котором настроено нужное значение параметра `UseKSN`.
- `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.
- `--accept-ksn` – ключ, означающий, что вы соглашаетесь с условиями, изложенными в Положении о Kaspersky Security Network. Ключ требуется указать, если вы включаете использование Kaspersky Security Network.

Если приложение Kaspersky Endpoint Security, установленное на клиентском устройстве, работает под управлением политики, которая была назначена в Kaspersky Security Center, значение параметра `UseKSN` можно изменить только в Kaspersky Security Center. Когда приложение Kaspersky Endpoint Security, установленное на клиентском устройстве, прекращает работать под управлением политики, параметру присваивается значение `UseKSN=No`.

Проверка подключения к Kaspersky Security Network с помощью командной строки

Чтобы проверить подключение к Kaspersky Security Network, выполните следующую команду:

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

В строке **Использование Kaspersky Security Network** отображается статус подключения к Kaspersky Security Network:

- Если отображается статус `Расширенный режим KSN`, приложение Kaspersky Endpoint Security использует Kaspersky Security Network, можно получать информацию из базы знаний, отправляется анонимная статистика и информация о типах и источниках угроз.
- Если отображается статус `Стандартный режим KSN`, приложение Kaspersky Endpoint Security использует Kaspersky Security Network, можно получать информацию из базы знаний, но анонимная статистика и информация о типах и источниках угроз не отправляется.
- Если отображается статус `Выключен`, приложение Kaspersky Endpoint Security не использует Kaspersky Security Network.

В строке **Инфраструктура Kaspersky Security Network** отображается информация об инфраструктурном решении, которое используется для работы с репутационными базами "Лаборатории Касперского": `Kaspersky Security Network` или `Kaspersky Private Security Network`.

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Устройство пользователя не подключено к интернету.
- Использование Kaspersky Security Network не включено.
- Приложение не активировано, или срок действия лицензии истек.
- Выявлены проблемы, связанные с лицензионным ключом. Например, ключ находится в списке запрещенных ключей.

Включение и выключение облачного режима с помощью командной строки

Облачный режим – это режим работы приложения Kaspersky Endpoint Security, при котором используется облегченная версия баз вредоносного ПО.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, работа с облегченными базами вредоносного ПО не поддерживается. Приложение получает от Сервера защиты специальные базы, необходимые для работы Легкого агента.

В командной строке вы можете включать и выключать облачный режим с помощью параметра `CloudMode=Yes/No` из общих параметров приложения.

Вы можете изменять значение параметра `CloudMode` с помощью конфигурационного файла, который содержит все общие параметры приложения, или с помощью ключей командной строки.

Облачный режим работы приложения доступен, если включено использование Kaspersky Security Network.

Дополнительные параметры работы приложения

Вы можете настраивать следующие дополнительные параметры работы приложения:

- Использование прокси-сервера в работе приложения.
- Глобальные исключения – исключение точек монтирования из перехвата файловых операций для компонентов Защита от файловых угроз, Защита от шифрования, Мониторинг контейнеров и задач Поиск вредоносного ПО, Проверка важных областей, Проверка контейнеров и Проверка съемных дисков.
- Исключение памяти процессов из проверки.
- Режим перехвата файловых операций.
- Обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
- Отслеживание стабильности работы приложения.
- Параметры запуска приложения.
- Ограничение на использование памяти и ресурсов процессора для задач проверки.
- Ограничение на использование резидентной памяти приложением.
- Ограничение на количество задач выборочной проверки, которые может одновременно запустить непривилегированный пользователь.
- Параметры отправки информации в хранилище Kaspersky Security Center.
- Разрешения на управление задачами.

Настройка прокси-сервера

Вы можете настроить параметры прокси-сервера, если доступ пользователей с клиентских устройств в интернет осуществляется через прокси-сервер. Приложение Kaspersky Endpoint Security может использовать прокси-сервер для подключения к серверам "Лаборатории Касперского", например, при обновлении баз и модулей приложения или при взаимодействии с Kaspersky Security Network и Kaspersky Endpoint Detection and Response (KATA).

По умолчанию использование прокси-сервера выключено.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование прокси-сервера для подключения к Kaspersky Security Network, к SVM и к Серверу интеграции.

Настройка параметров прокси-сервера в Web Console

В Web Console вы можете настраивать использование прокси-сервера в свойствах политики (**Параметры приложения → Общие параметры → Параметры прокси-сервера**).

Параметры прокси-сервера

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, прокси-сервер не используется в работе приложения.
Использовать указанные параметры прокси-сервера	Если выбран этот вариант, приложение использует указанные параметры прокси-сервера, например для интеграции с Kaspersky Endpoint Detection and Response (KATA).
Адрес	Поле для ввода IP-адреса или доменного имени прокси-сервера. Поле доступно, если выбран вариант **Использовать указанные параметры прокси-сервера**.
Порт	Поле для ввода порта прокси-сервера. Значение по умолчанию: 3128. Поле доступно, если выбран вариант **Использовать указанные параметры прокси-сервера**.
Использовать аутентификацию на прокси-сервере	Включает или выключает аутентификацию с помощью имени пользователя и пароля при доступе к прокси-серверу. Флажок доступен, если выбран вариант **Использовать указанные параметры прокси-сервера**. По умолчанию флажок снят. Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.
Имя пользователя	Поле ввода имени пользователя для его аутентификации на прокси-сервере. Поле ввода доступно, если установлен флажок **Использовать аутентификацию на прокси-сервере**.
Изменить	Позволяет указать пароль пользователя для авторизации на прокси-сервере. Поле **Пароль** недоступно для редактирования. По умолчанию пароль пустой. Чтобы указать пароль, нажмите на кнопку **Изменить**, в открывшемся окне введите пароль и нажмите на кнопку **OK**. Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев. При нажатии на кнопку **Показать** в окне ввода пароля пароль отображается в открытом виде. Кнопка доступна, если установлен флажок **Использовать аутентификацию на прокси-сервере**.
Использовать Kaspersky Security Center в качестве	Флажок включает или выключает использование Kaspersky Security Center в качестве прокси-сервера при активации приложения.

прокси-сервера для активации приложения	Если флажок установлен, Kaspersky Endpoint Security использует Kaspersky Security Center в качестве прокси-сервера при активации приложения. По умолчанию флажок снят. Параметр применяется, только если приложение используется в стандартном режиме. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, информацию о лицензии предоставляет Сервер защиты.

Настройка параметров прокси-сервера в Консоли администрирования

В Консоли администрирования вы можете настраивать использование прокси-сервера в свойствах политики (**Общие параметры** → **Параметры прокси-сервера**).

Параметры прокси-сервера

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, прокси-сервер не используется в работе приложения.
Использовать указанные параметры прокси-сервера	Если выбран этот вариант, приложение использует указанные параметры прокси-сервера, например для интеграции с Kaspersky Endpoint Detection and Response (KATA).
Адрес и порт	Поля для ввода IP-адреса или доменного имени прокси-сервера и порта прокси-сервера. Порт по умолчанию: 3128. Поля доступны, если выбран вариант **Использовать указанные параметры прокси-сервера**.
Использовать аутентификацию на прокси-сервере	Флажок включает или выключает аутентификацию с помощью имени пользователя и пароля при доступе к прокси-серверу. Флажок доступен, если выбран вариант **Использовать указанные параметры прокси-сервера**. По умолчанию флажок снят. Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.
Имя пользователя	Поле ввода имени пользователя для его аутентификации на прокси-сервере. Поле ввода доступно, если установлен флажок **Использовать аутентификацию на прокси-сервере**.
Пароль	Поле для ввода пароля пользователя для авторизации на прокси-сервере.

	Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев. При нажатии на кнопку **Показать** пароль пользователя отображается в поле **Пароль** в открытом виде. По умолчанию пароль пользователя скрыт и отображается в виде точек. Поле ввода и кнопка доступны, если установлен флажок **Использовать аутентификацию на прокси-сервере**.
Использовать Kaspersky Security Center в качестве прокси-сервера для активации приложения	Флажок включает или выключает использование Kaspersky Security Center в качестве прокси-сервера при активации приложения. Если флажок установлен, Kaspersky Endpoint Security использует Kaspersky Security Center в качестве прокси-сервера при активации приложения. По умолчанию флажок снят. Параметр применяется, только если приложение используется в стандартном режиме. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, информацию о лицензии предоставляет Сервер защиты.

Настройка параметров прокси-сервера в командной строке

В командной строке вы можете включать и выключать использование прокси-сервера компонентами приложения с помощью параметров `UseProxy` и `ProxyServer` из общих параметров приложения.

Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `UseProxy` может принимать следующие значения:

- `Yes` – включить использование прокси-сервера.
- `No` – выключить использование прокси-сервера.

Параметр `ProxyServer` позволяет задавать параметры прокси-сервера в формате `[<пользователь>[:<пароль>]@]<адрес прокси-сервера>[:<порт>]`, где:

- `<пользователь>` – имя пользователя для аутентификации на прокси-сервере.
- `<пароль>` – пароль пользователя для авторизации на прокси-сервере.
- `<адрес прокси-сервера>` – IP-адрес или доменное имя прокси-сервера.
- `<порт>` – порт прокси-сервера.

Если для подключения к прокси-серверу не требуется аутентификация, параметр `ProxyServer` указывать не нужно.

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

Настройка глобальных исключений

Вы можете настраивать исключение точек монтирования из перехвата файловых операций для компонентов Защита от файловых угроз и Защита от шифрования, а также из проверки задачами Поиск вредоносного ПО, Проверка важных областей и Проверка контейнеров. Исключение точек монтирования позволяет исключать из перехвата файловых операций локальные или удаленные директории, смонтированные на устройстве. Кроме того, глобальные исключения влияют на работу компонента Мониторинг контейнеров и задачи Проверка съемных дисков.

Настройка глобальных исключений в Web Console

В Web Console вы можете настраивать глобальные исключения в свойствах политики (**Параметры приложения** → **Общие параметры** → **Глобальные исключения**).

Таблица в разделе **Глобальные исключения** содержит точки монтирования, которые будут исключены из перехвата файловых операций.

В столбце **Путь** отображается путь к исключенным точкам монтирования. По умолчанию таблица пустая.

Элементы в таблице можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно добавления исключения точки монтирования

Параметры точки монтирования

Параметр	Описание
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные точки монтирования. • **Смонтированная** – удаленные директории, смонтированные на устройстве по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол	В раскрывающемся списке вы можете выбрать протокол удаленного доступа:

доступа	• **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.
Путь	Поле ввода пути к точке монтирования, которую вы хотите добавить в исключения из перехвата файловых операций. Для указания пути вы можете использовать маски. Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек). Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из перехвата файловых операций. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке **Протокол доступа** выбран элемент **Пользовательский**.

Настройка глобальных исключений в Консоли администрирования

В Консоли администрирования вы можете настраивать глобальные исключения в свойствах политики (**Общие параметры** → **Глобальные исключения**).

Блок параметров **Исключенные точки монтирования** содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключенные точки монтирования**.

Список в окне содержит пути к исключенным точкам монтирования. По умолчанию список пуст.

Элементы в списке можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы.

Кнопка доступна, если в таблице выбран хотя бы один элемент.

Окно Путь к точке монтирования

Параметры точки монтирования

Параметр	Описание
Файловая система, протокол доступа и путь	Блок параметров позволяет задать расположение точки монтирования. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные точки монтирования. • **Смонтированная** – удаленные директории, смонтированные на устройстве по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – все ресурсы файловой системы устройства, указанной в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к точке монтирования, которую вы хотите добавить в исключения из перехвата файловых операций. Для указания пути вы можете использовать маски.

	Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории. Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`. Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`. Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска. Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек). Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из перехвата файловых операций. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.

Настройка глобальных исключений в командной строке

В командной строке вы можете настраивать исключения точек монтирования с помощью параметра `ExcludedMountPoint.item_#` из общих параметров приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `ExcludedMountPoint.item_#` может принимать следующие значения:

- `AllRemoteMounted` – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протоколов SMB и NFS.
- `Mounted:NFS` – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протокола NFS.
- `Mounted:SMB` – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протокола SMB.
- `Mounted:<тип файловой системы>` – исключать из перехвата файловых операций все смонтированные директории с указанным типом файловой системы.

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

- `<путь, содержащий маску /mnt/user* или /mnt/**/user_share>` – исключать из перехвата объекты, находящиеся в точках монтирования, имена которых содержат указанную маску.

  Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

  Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

  Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

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

  Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек).

  Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`.

  Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Вы можете указать несколько точек монтирования, которые вы хотите исключить из проверки.

Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды `mount`.

Исключение памяти процессов из проверки

Вы можете настраивать исключения из проверки памяти процессов. Приложение не будет проверять память указанных процессов.

Настройка исключений в Web Console

В Web Console вы можете настраивать исключения памяти процессов из проверки в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры приложения**).

По ссылке **Настроить исключение памяти процессов из проверки** в блоке **Исключение памяти процессов из проверки** открывается окно **Исключение памяти процессов из проверки**, в котором вы можете сформировать список исключений.

Список в окне **Исключение памяти процессов из проверки** содержит пути к процессам, которые приложение исключает из проверки памяти процессов. Для указания пути вы можете использовать маски. По умолчанию список пуст.

Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

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

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

Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек).

Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir.

Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

Элементы в списке можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранный путь к процессу из списка.

Кнопка доступна, если в списке выбран хотя бы один путь к процессу.

При нажатии на кнопку **Изменить** открывается окно, в котором вы можете изменить путь к процессу. Kaspersky Endpoint Security исключает из проверки память указанного процесса.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете ввести полный путь к процессу. Kaspersky Endpoint Security исключает из проверки память указанного процесса.

Настройка исключений в Консоли администрирования

В Консоли администрирования вы можете настраивать исключения памяти процессов из проверки в свойствах политики (**Общие параметры** → **Исключение памяти процессов**).

По кнопке **Настроить** в блоке **Исключение памяти процессов из проверки** открывается окно, в котором вы можете сформировать список исключений.

Список в окне **Исключение памяти процессов из проверки** содержит пути к процессам, которые приложение исключает из проверки памяти процессов. Для указания пути вы можете использовать маски. По умолчанию список пуст.

Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/*/*/file.

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

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

Для исключения точки монтирования /dir требуется указывать именно /dir (без звездочек).

Маска /dir/* исключает все точки монтирования на уровень ниже от /dir, но не саму точку монтирования /dir. Маска /dir/** исключает все точки монтирования на любом уровне вложенности под /dir, но не саму точку монтирования /dir.

Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

Элементы в списке можно добавлять, изменять и удалять.

При нажатии на кнопку **Удалить** Kaspersky Endpoint Security удаляет выбранный путь к процессу из списка.

Кнопка доступна, если в списке выбран хотя бы один путь к процессу.

При нажатии на кнопку **Изменить** открывается окно, в котором вы можете изменить путь к процессу. Kaspersky Endpoint Security исключает из проверки память указанного процесса.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете ввести полный путь к процессу. Kaspersky Endpoint Security исключает из проверки память указанного процесса.

Настройка исключений в командной строке

В командной строке вы можете настраивать исключение памяти процессов из проверки с помощью параметра MemScanExcludedProgramPath.item_# в общих параметрах приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр MemScanExcludedProgramPath.item_# содержит полный путь к процессу в локальной директории. Для указания пути вы можете использовать маски.

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

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

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Вы можете указать несколько процессов, память которых требуется исключить из проверки.

Выбор режима перехвата файловых операций

Режим перехвата файловых операций влияет на работу компонентов Защита от файловых угроз и Контроль устройств.

- Приложение может блокировать на время проверки доступ к файлам, которые проверяет компонент Защита от файловых угроз. По умолчанию доступ блокируется: любое обращение к проверяемому файлу ожидает результатов проверки. Если в результате проверки в файле не обнаружены угрозы, приложение разрешает доступ к файлу. При обнаружении зараженных объектов приложение выполняет действия, указанные в параметрах **Первое действие** (`FirstAction`) и **Второе действие** (`SecondAction`) компонента Защита от файловых угроз.

  Вы можете выключить блокировку доступа к файлам, которые проверяет компонент Защита от файловых угроз. В этом случае проверка выполняется в асинхронном режиме.

- Приложение может блокировать доступ к файлам на устройстве на время, пока компонент Контроль устройств определяет возможность предоставления доступа к устройству. По умолчанию доступ блокируется: любое обращение к файлам на контролируемом устройстве ожидает результатов проверки. Приложение разрешает доступ к файлам, если в результате проверки Контроль устройств разрешает доступ к устройству с файлами.

  Вы можете выключить блокировку доступа к файлам на устройстве, которое контролирует компонент Контроль устройств. В этом случае Контроль устройств определяет возможность предоставления доступа к устройству в асинхронном режиме.

Настройка в Web Console

В Web Console вы можете настраивать режим перехвата файловых операций в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Режим перехвата файловых операций**).

Флажок **Блокировать доступ к файлам во время проверки** включает или выключает блокировку доступа к файлам на время проверки компонентами Защита от файловых угроз и Контроль устройств.

По умолчанию флажок установлен.

Если флажок снят, на время проверки обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать режим перехвата файлов в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Режим перехвата файловых операций**).

Флажок **Блокировать доступ к файлам во время проверки** включает или выключает блокировку доступа к файлам на время проверки компонентами Защита от файловых угроз и Контроль устройств.

По умолчанию флажок установлен.

Если флажок снят, на время проверки обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.

Настройка в командной строке

В командной строке вы можете настраивать режим перехвата файловых операций с помощью параметра `FileBlockDuringScan` в общих параметрах приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `FileBlockDuringScan` может принимать следующие значения:

- `Yes` (значение по умолчанию) – блокировать доступ к файлам на время проверки компонентами Защита от файловых угроз и Контроль устройств.
- `No` – не блокировать доступ к файлам на время проверки. Обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.

  Такой режим перехвата файловых операций оказывает меньшее влияние на производительность системы во время работы, но есть риск, что угроза в файле не будет вылечена или удалена, если во время проверки этот файл сможет, например, изменить свое имя до принятия приложением решения о статусе этого файла.

Настройка обнаружения приложений, которые злоумышленники могут использовать для нанесения вреда

Вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.

Настройка в Web Console

В Web Console вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным, в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Параметры проверки**).

Флажок **Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным** включает или выключает обнаружение легальных приложений, через которые злоумышленники могут навредить устройству или данным пользователя.

По умолчанию флажок снят.

Настройка в Консоли администрирования

В Консоли администрирования вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным, в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Параметры проверки**).

Флажок **Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным** включает или выключает обнаружение легальных приложений, через которые злоумышленники могут навредить устройству или данным пользователя.

По умолчанию флажок снят.

Настройка в командной строке

В командной строке вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным, с помощью параметра `DetectOtherObjects` в общих параметрах приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `DetectOtherObjects` может принимать следующие значения:

- `Yes` – включить обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
- `No` – не включать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.

Включение мониторинга стабильности работы приложения

Вы можете включать и выключать мониторинг стабильности работы приложения Kaspersky Endpoint Security, который позволяет отслеживать количество нештатных остановок приложения и уведомлять администратора о нестабильной работе приложения.

Настройка в Web Console

В Web Console вы можете включать и выключать мониторинг стабильности работы приложения в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Дополнительные параметры приложения**).

Флажок **Включить мониторинг стабильности работы приложения** включает или выключает отслеживание состояния работы приложения Kaspersky Endpoint Security.

По умолчанию флажок снят.

Для применения параметра требуется перезапустить приложение.

Если приложение работает нестабильно, в свойствах устройства с установленным приложением отображается сообщение: *<Количество> нештатных остановок приложения начиная с <дата и время>*.

Настройка в Консоли администрирования

В Консоли администрирования вы можете включать и выключать мониторинг стабильности работы приложения в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Дополнительные параметры приложения**).

Флажок **Включить мониторинг стабильности работы приложения** включает или выключает отслеживание состояния работы приложения Kaspersky Endpoint Security.

По умолчанию флажок снят.

Для применения параметра требуется перезапустить приложение.

Если приложение работает нестабильно, в свойствах устройства с установленным приложением отображается сообщение: *<Количество> нештатных остановок приложения начиная с <дата и время>*.

Настройка в командной строке

В командной строке вы можете настроить мониторинг стабильности работы приложения с помощью параметров `TrackProductCrashes`, `ProductHealthLogFile`, `WarnThreshold`, `WarnAfter_#_crash` и `WarnRemovingThreshold` в конфигурационном файле kesl.ini.

Параметр `TrackProductCrashes` позволяет включить или выключить мониторинг стабильности работы приложения. Параметр может принимать следующие значения:

- `Yes/true` – включить мониторинг стабильности работы приложения.
- `No/false` – не включать мониторинг стабильности работы приложения.

Параметр `ProductHealthLogFile` позволяет задать путь к файлу, с помощью которого осуществляется мониторинг стабильности приложения. Значение по умолчанию: /var/opt/kaspersky/kesl/private/kesl_health.log.

Параметр `WarnThreshold` позволяет задать интервал времени (в секундах), за который приложение должно посчитать количество нештатных остановок, прежде чем вывести уведомление о нестабильной работе. Значение по умолчанию: 3600 секунд.

Параметр `WarnRemovingThreshold` позволяет задать интервал времени (в секундах), по истечении которого статус о нестабильной работе приложения будет снят. Значение по умолчанию: 86400 секунд.

Параметр `WarnAfter_#_crash` позволяет задать количество нештатных остановок приложения, необходимых для отображения уведомления о нестабильной работе приложения. Параметр может принимать значения от 0 до 10. Значение по умолчанию: 10. Если указано значение 0, уведомление о нестабильной работе приложения не отображается.

Настройка параметров запуска приложения

Вы можете настраивать параметры запуска приложения.

Настройка ограничения в Web Console

В Web Console вы можете настраивать параметры запуска приложения в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Параметры запуска приложения**).

Параметры запуска приложения

Параметр	Описание
Максимальное количество неудачных последовательных попыток запуска приложения	Поле ввода максимального количества неудачных последовательных попыток запуска приложения. Значение по умолчанию: 5.
Максимальное время ожидания запуска приложения (мин.)	Поле ввода максимального времени ожидания запуска приложения (в минутах), после которого процесс kesl будет перезапущен. Значение по умолчанию: 3.

Настройка ограничения в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры запуска приложения в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Параметры запуска приложения**).

В блоке **Параметры запуска приложения** по нажатию на кнопку **Настроить** открывается окно **Параметры запуска приложения**, в котором вы можете настроить параметры запуска приложения (см. таблицу ниже).

Параметры запуска приложения

Параметр	Описание
Максимальное количество неудачных последовательных попыток запуска приложения	Поле ввода максимального количества неудачных последовательных попыток запуска приложения. Значение по умолчанию: 5.
Максимальное время ожидания запуска приложения (мин.)	Поле ввода максимального времени ожидания запуска приложения (в минутах), после которого процесс kesl будет перезапущен. Значение по умолчанию: 3.

Настройка ограничения в командной строке

В командной строке вы можете настраивать параметры запуска приложения с помощью параметров `MaxRestartCount` и `StartupTimeout` в конфигурационном файле kesl.ini.

Параметр `MaxRestartCount` позволяет задать максимальное количество неудачных последовательных попыток запуска приложения. Параметр может принимать значения от 1 до 10. Значение по умолчанию: 5.

Параметр `StartupTimeout` позволяет задать максимальное время ожидания запуска приложения (в минутах), после которого процесс kesl будет перезапущен. Параметр может принимать значения от 1 до 60. Значение по умолчанию: 3.

Ограничение на использование памяти и ресурсов процессора

Вы можете настраивать ограничение на использование ресурсов процессора для задач проверки. По умолчанию ограничение не установлено. Также вы можете настраивать ограничение на использование памяти для задач проверки. По умолчанию установлено ограничение 8192 мегабайт.

Настройка ограничения в Web Console

В Web Console вы можете включать и выключать ограничение на использование ресурсов процессора и настраивать ограничение на использование памяти для задач проверки в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Производительность**).

Параметры

Параметр	Описание
Ограничение на использование памяти для задач проверки (МБ)	Поле ввода ограничения на использование памяти для задач проверки (в мегабайтах). Значение по умолчанию: 8192.
Ограничить потребление ресурсов процессора для задач проверки	Флажок включает или выключает ограничение на использование ресурсов процессора для задач Поиск вредоносного ПО, Проверка важных областей, Инвентаризация и Проверка контейнеров. Если флажок установлен, максимальная нагрузка на все ядра процессора при работе этих задач не превышает значения, указанного в поле **Максимальное значение (%)**. По умолчанию флажок снят.

Настройка ограничения в Консоли администрирования

В Консоли администрирования вы можете включать и выключать ограничение на использование ресурсов процессора и настраивать ограничение на использование памяти для задач проверки в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Производительность**).

В блоке **Производительность** по нажатию на кнопку **Настроить** открывается окно **Потребление ресурсов процессора и памяти**, в котором вы можете настроить ограничения (см. таблицу ниже).

Параметры

Параметр	Описание
Ограничить потребление ресурсов процессора для задач проверки (%)	Флажок включает или выключает ограничение на использование ресурсов процессора для задач Поиск вредоносного ПО, Проверка важных областей, Инвентаризация и Проверка контейнеров. Если флажок установлен, максимальная нагрузка на все ядра процессора при работе этих задач не превышает значения, указанного в поле справа (в процентах). По умолчанию флажок снят.

Ограничение на использование памяти для задач проверки (МБ)	Поле ввода ограничения на использование памяти для задач проверки (в мегабайтах). Значение по умолчанию: 8192.

Настройка ограничения в командной строке

В командной строке вы можете настраивать ограничение на использование ресурсов процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan* с помощью параметров `UseOnDemandCPULimit` и `OnDemandCPULimit` в общих параметрах приложения.

Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `UseOnDemandCPULimit` может принимать следующие значения:

- `Yes` – включить ограничение потребления ресурсов процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan*.
- `No` – выключить ограничение потребления ресурсов процессора для задач.

Параметр `OnDemandCPULimit` позволяет задать максимальное значение нагрузки на все ядра процессора (в процентах) при работе задач типа *ODS*, *ContainerScan* и *InventoryScan*. Параметр может принимать значения от 10 до 100. Значение по умолчанию 100.

В командной строке вы можете настраивать ограничение на использование памяти для задач типа *ODS*, *ContainerScan* и *InventoryScan* с помощью параметра `ScanMemoryLimit` в конфигурационном файле kesl.ini. Значение по умолчанию: 8192.

Ограничение на использование резидентной памяти приложением

Вы можете настраивать ограничение на использование резидентной памяти приложением. По умолчанию установлено автоматическое ограничение.

Настройка ограничения в Web Console

В Web Console вы можете настраивать ограничение на использование резидентной памяти приложением в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Дополнительные параметры приложения**).

В блоке **Дополнительные параметры приложения** по ссылке **Настроить использование памяти** открывается окно, в котором вы можете настроить ограничение на использование резидентной памяти (см. таблицу ниже).

Параметры

Параметр	Описание
Использование резидентной памяти приложением	В раскрывающемся списке вы можете выбрать способ ограничения на использование резидентной памяти: • **Не ограничено**. При выборе этого элемента списка использование резидентной памяти не ограничивается.

	• **Ограничено значением в процентах от общего объема**. При выборе этого элемента списка становится доступно поле **Ограничение на использование памяти (%)**, в котором вы можете указать нужное значение в процентах. • **Ограничено значением в мегабайтах**. При выборе этого элемента списка становится доступно поле **Ограничение на использование памяти (МБ)**, в котором вы можете указать нужное значение в мегабайтах. • **Ограничено наименьшим из указанных значений (%, МБ)**. При выборе этого элемента списка становятся доступны поля **Ограничение на использование памяти (%)** и **Ограничение на использование памяти (МБ)**, в которых вы можете указать нужные значения. • **Ограничено наибольшим из указанных значений (%, МБ)**. При выборе этого элемента списка становятся доступны поля **Ограничение на использование памяти (%)** и **Ограничение на использование памяти (МБ)**, в которых вы можете указать нужные значения. • **Ограничивается автоматически (рекомендуется)**. При выборе этого элемента списка использование резидентной памяти ограничивается автоматически (значение по умолчанию).
Ограничение на использование памяти (%)	Поле ввода ограничения на использование памяти (в процентах). Значение по умолчанию: 50.
Ограничение на использование памяти (МБ)	Поле ввода ограничения на использование памяти (в мегабайтах). Значение по умолчанию: 2000.

Настройка ограничения в Консоли администрирования

В Консоли администрирования вы можете настраивать ограничение на использование резидентной памяти приложением в свойствах политики (**Общие параметры** → **Параметры приложения**).

В блоке **Дополнительные параметры приложения** по нажатию на кнопку **Настроить** открывается окно **Дополнительные параметры**, в котором вы можете настроить ограничение на использование резидентной памяти (см. таблицу ниже).

Параметры

Параметр	Описание
Использование памяти приложением	В раскрывающемся списке вы можете выбрать способ ограничения на использование резидентной памяти: • **Не ограничено**. При выборе этого элемента списка использование резидентной памяти не ограничивается. • **Ограничивается автоматически (рекомендуется)**. При выборе этого элемента списка использование резидентной памяти ограничивается автоматически (значение по умолчанию). • **Ограничено значением в процентах от общего объема**. При выборе этого элемента списка становится доступно поле **Ограничение на использование памяти (%)**, в котором вы можете указать нужное значение в процентах.

	• **Ограничено значением в мегабайтах**. При выборе этого элемента списка становится доступно поле **Ограничение на использование памяти (МБ)**, в котором вы можете указать нужное значение в мегабайтах. • **Ограничено наименьшим из указанных значений (%, МБ)**. При выборе этого элемента списка становятся доступны поля **Ограничение на использование памяти (%)** и **Ограничение на использование памяти (МБ)**, в которых вы можете указать нужные значения. • **Ограничено наибольшим из указанных значений (%, МБ)**. При выборе этого элемента списка становятся доступны поля **Ограничение на использование памяти (%)** и **Ограничение на использование памяти (МБ)**, в которых вы можете указать нужные значения.
Ограничение на использование памяти (%)	Поле ввода ограничения на использование памяти (в процентах). Значение по умолчанию: 50.
Ограничение на использование памяти (МБ)	Поле ввода ограничения на использование памяти (в мегабайтах). Значение по умолчанию: 2000.

Настройка ограничения в командной строке

В командной строке вы можете настраивать ограничение на использование резидентной памяти приложением с помощью параметра `MaxMemory` в конфигурационном файле kesl.ini.

Параметр `MaxMemory` может принимать следующие значения:

- `off` – использование резидентной памяти не ограничено.
- `< значение >%` – значение от 1 до 100 в процентах от объема памяти.
- `< значение >MB` – значение в мегабайтах.
- `lowest/< значение >%/< значение >MB` – наименьшее значение между значением в процентах и значением в мегабайтах.
- `highest/< значение >%/< значение >MB` – наибольшее значение между значением в процентах и значением в мегабайтах.
- `auto` – до 50% доступной памяти, но не менее 2 ГБ и не более 16 ГБ.

Значение по умолчанию: `auto`.

Ограничение на количество задач выборочной проверки

Вы можете настраивать ограничение на количество задач выборочной проверки, которые может одновременно запустить на устройстве непривилегированный пользователь. Количество задач, которые может запустить пользователь с root-правами, не ограничивается.

Вы можете включать и выключать ограничение на количество одновременно запущенных задач выборочной проверки в командной строке с помощью параметра `LimitNumberOfScanFileTasks` из общих параметров приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `LimitNumberOfScanFileTasks` может принимать значения от 0 до 4294967295. Значение по умолчанию: 0.

Если задано значение 0, непривилегированный пользователь не может запускать задачи выборочной проверки.

Если во время установки приложения вы установили пакет графического интерфейса, для параметра `LimitNumberOfScanFileTasks` по умолчанию используется значение `5`.

Настройка отправки информации в хранилище Kaspersky Security Center

В Kaspersky Security Center вы можете включать и выключать отправку в хранилище Kaspersky Security Center информации о необработанных файлах и о подключенных устройствах.

Информация о необработанных файлах отображается в списке активных угроз в Web Console (**Операции** → **Хранилища** → **Активные угрозы**) и в Консоли администрирования (**Дополнительно** → **Хранилища** → **Активные угрозы**).

Информация об устройствах, установленных на клиентском устройстве или подключенных к нему, отображается в списке оборудования в Web Console (**Операции** → **Хранилища** → **Оборудование**) и в Консоли администрирования (**Дополнительно** → **Хранилища** → **Оборудование**). Информация передается, если включен Контроль устройств.

Включение и выключение отправки информации в Web Console

В Web Console вы можете включать и выключать отправку информации в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры Хранилища**).

Параметры отправки информации в хранилище Kaspersky Security Center

Параметр	Описание
Информирование о необработанных файлах включено / выключено	Переключатель включает или выключает отправку уведомлений о файлах, необработанных во время проверки, на Сервер администрирования. По умолчанию переключатель включен.
Информирование об установленных устройствах включено / выключено	Переключатель включает или выключает передачу на Сервер администрирования информации об устройствах, установленных на клиентском устройстве или подключенных к нему. По умолчанию переключатель включен.

Включение и выключение отправки информации в Консоли администрирования

В Консоли администрирования вы можете включать и выключать отправку информации в свойствах политики (**Общие параметры** → **Параметры Хранилища**).

Параметры отправки информации в хранилище Kaspersky Security Center

Параметр	Описание
Информировать о необработанных файлах	Флажок включает или выключает отправку уведомлений о файлах, необработанных во время проверки, на Сервер администрирования. По умолчанию флажок установлен.
Информировать об установленных устройствах	Флажок включает или выключает передачу на Сервер администрирования информации об устройствах, установленных на клиентском устройстве или подключенных к нему. По умолчанию флажок установлен.

Настройка разрешений на управление задачами

В Kaspersky Security Center вы можете настраивать следующие разрешения для пользователей:

- разрешение на просмотр задач, созданных в приложении Kaspersky Endpoint Security;
- разрешение на просмотр на клиентских устройствах задач, созданных в Kaspersky Security Center.

Настройка в Web Console

В Web Console вы можете настраивать разрешение на просмотр задач в свойствах политики (**Параметры приложения** → **Локальные задачи** → **Управление задачами**).

Параметры управления задачами

Параметр	Описание
Разрешить пользователям просмотр и управление локальными задачами	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в приложении Kaspersky Endpoint Security, и управление этими задачами на управляемых клиентских устройствах. По умолчанию флажок снят.
Разрешить пользователям просмотр и управление задачами, созданными через KSC	Флажок разрешает или запрещает пользователям просмотр задач, созданных через Kaspersky Security Center Web Console, и управление этими задачами на управляемых клиентских устройствах. По умолчанию флажок снят.

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать разрешение на просмотр задач в свойствах политики (**Локальные задачи** → **Управление задачами**).

Параметры управления задачами

Параметр	Описание
Разрешить пользователям просмотр и управление локальными задачами	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в приложении Kaspersky Endpoint Security, и управление этими задачами на управляемых клиентских устройствах. По умолчанию флажок снят.
Разрешить пользователям	Флажок разрешает или запрещает пользователям просмотр задач,

просмотр и управление задачами, созданными через KSC	созданных через Kaspersky Security Center, и управление этими задачами на управляемых клиентских устройствах. По умолчанию флажок снят.

Резервное хранилище

Если во время проверки защищенного устройства Kaspersky Endpoint Security обнаруживает в файле вредоносный код, приложение может заблокировать этот файл, присвоить ему статус *Заражен*, поместить его копию в резервное хранилище и попытаться провести лечение файла.

Резервное хранилище – это хранилище резервных копий файлов, которые были удалены или изменены в процессе лечения. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Если файл удается вылечить, то статус резервной копии файла изменяется на *Вылечен*. Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете попытаться восстановить файл из его вылеченной копии в директорию исходного размещения файла.

Рекомендуется восстанавливать файлы из резервных копий только в том случае, если им присвоен статус *Вылечен*. Восстановление зараженных объектов может привести к заражению устройства.

Резервные копии файлов в резервном хранилище могут содержать персональные данные. Для доступа к объектам резервного хранилища требуются root-права.

Вы можете настраивать следующие параметры резервного хранилища:

- Время хранения объектов в резервном хранилище. По умолчанию объекты хранятся 90 суток.
- Максимальный размер резервного хранилища. По умолчанию размер резервного хранилища не ограничен.
- Путь к резервному хранилищу. По умолчанию резервное хранилище расположено в директории /var/opt/kaspersky/kesl/common/objects-backup/.

По истечении заданного времени или при достижении максимального размера резервного хранилища приложение автоматически удаляет из резервного хранилища резервные копии файлов с любым статусом.

Также вы можете самостоятельно удалить резервную копию как восстановленного, так и невосстановленного файла.

Общий список файлов, помещенных в резервное хранилище приложениями "Лаборатории Касперского" на клиентских устройствах, формируется в Kaspersky Security Center и доступен в Консоли администрирования (**Дополнительно** → **Хранилища** → **Резервное хранилище**) и в Web Console (**Операции** → **Хранилища** → **Резервное хранилище**). Вы можете просматривать свойства файлов, находящихся в резервных хранилищах на защищенных устройствах, запускать проверку на наличие вредоносного ПО в резервном хранилище и удалять из него файлы. Kaspersky Security Center не копирует файлы из резервных хранилищ на Сервер администрирования, все файлы размещаются в резервных хранилищах на защищенных устройствах. Восстановление файлов выполняется на защищенном устройстве.

Настройка параметров резервного хранилища в Web Console

В Web Console вы можете настраивать параметры резервного хранилища в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры Хранилища**).

Параметры резервного хранилища

Параметр	Описание
Информирование о файлах в резервном хранилище включено / выключено	Переключатель включает или выключает отправку уведомлений о файлах в резервном хранилище на Сервер администрирования. По умолчанию переключатель включен.
Хранить объекты не более (дней)	Поле ввода для указания периода хранения объектов в резервном хранилище. Доступные значения: 0–3653. Значение по умолчанию: 90. Если задано значение 0, период хранения объектов в резервном хранилище не ограничен.
Ограничить размер резервного хранилища до (МБ)	Поле ввода для указания максимального размера резервного хранилища (в мегабайтах). Доступные значения: 0–999999. Значение по умолчанию: 0 (размер резервного хранилища не ограничен).

Настройка параметров резервного хранилища в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры резервного хранилища в свойствах политики (**Общие параметры** → **Параметры Хранилища**).

Параметры резервного хранилища

Параметр	Описание
Информировать о файлах в резервном хранилище	Флажок включает или выключает отправку уведомлений о файлах в резервном хранилище на Сервер администрирования. По умолчанию флажок установлен.
Хранить объекты не более (дней)	Флажок включает или выключает ограничение срока хранения объектов в резервном хранилище заданным интервалом времени. Доступные значения: 0–3653. Значение по умолчанию: 90. Если задано значение 0, период хранения объектов в резервном хранилище не ограничен.
Ограничить размер резервного хранилища до (МБ)	Флажок включает или выключает ограничение максимального размера резервного хранилища заданным значением (в мегабайтах). Доступные значения: 0–999999. Значение по умолчанию: 0 (размер резервного хранилища не ограничен).

Настройка параметров резервного хранилища в командной строке

В командной строке вы можете настраивать параметры резервного хранилища с помощью предустановленной задачи Управление резервным хранилищем (*Backup*).

Задача Управление резервным хранилищем по умолчанию запущена. Вы не можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры резервного хранилища, изменяя параметры предустановленной задачи Управление резервным хранилищем.

Параметр	Описание	Значение
`DaysToLive`	Интервал времени, в течение которого объекты хранятся в резервном хранилище (в сутках). Чтобы снять ограничение на время хранения объектов в резервном хранилище, укажите значение 0.	0 – время хранения объектов в резервном хранилище не ограничено. Значение по умолчанию: 90.
`BackupSizeLimit`	Максимальный размер резервного хранилища (в мегабайтах). При достижении максимального размера резервного хранилища, приложение удаляет самые старые объекты. Чтобы снять ограничение на размер резервного хранилища, укажите значение 0.	0 – 999999 0 – размер резервного хранилища не ограничен. Значение по умолчанию: 0.
`BackupFolder`	Путь к директории резервного хранилища. Вы можете указать в качестве резервного хранилища пользовательскую директорию, отличную от директории, заданной по умолчанию. В качестве резервного хранилища можно использовать директории на любых устройствах. Не рекомендуется указывать директории, расположенные на удаленных устройствах, например смонтированных по протоколам Samba и NFS. Kaspersky Endpoint Security начинает перемещать объекты в выбранную директорию после изменения параметров и перезапуска приложения. Если указанной директории не существует или она недоступна, приложение использует директорию, заданную по умолчанию.	Значение по умолчанию: /var/opt/kaspersky/kesl/common/objects-backup/ Для доступа к заданной по умолчанию директории резервного хранилища требуются root-права.

Работа с объектами резервного хранилища в командной строке

В командной строке с помощью команд управления резервным хранилищем вы можете выполнять следующие действия с объектами резервного хранилища:

- Просматривать информацию об объектах резервного хранилища.
- Удалять из резервного хранилища все или только указанные объекты.
- Восстанавливать объекты из резервного хранилища.

Восстановление зараженных объектов может привести к заражению устройства.

Просмотр информации об объектах резервного хранилища

Чтобы просмотреть информацию об объектах резервного хранилища, выполните следующую команду:

```
kesl-control -B --query ["<условия фильтра>"] [-n <количество>] [--json]
```

где:

- `<условия фильтра>` – одно или несколько логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса. Если вы не укажете условия фильтра, приложение выведет информацию обо всех объектах резервного хранилища.
- `<количество>` – количество последних объектов из хранилища, которые нужно вывести. Если вы не укажете ключ `-n`, будут выведены последние 30 объектов. Чтобы показать все объекты, укажите значение 0.
- `--json` – выводить данные в формате JSON.

В строке `ObjectId` отобразится числовой идентификатор, который приложение присвоило объекту при помещении в резервное хранилище. Этот идентификатор используется для выполнения действий над объектом, таких как восстановление или удаление объекта из резервного хранилища.

Восстановление объектов из резервного хранилища

Чтобы восстановить объект с исходным именем в исходное местоположение, выполните следующую команду:

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

где `<идентификатор объекта>` – числовой идентификатор, который приложение присвоило объекту при помещении в резервное хранилище.

Чтобы восстановить объект с новым именем в указанную директорию, выполните следующую команду:

```
kesl-control --restore <идентификатор объекта> --file <путь к файлу>
```

где `--file <путь к файлу>` – новое имя файла и путь к директории, в которой вы хотите его сохранить. Если указанной директории не существует, приложение создает ее.

Удаление объектов из резервного хранилища

Чтобы удалить выбранные объекты из резервного хранилища, выполните следующую команду:

```
kesl-control --mass-remove --query "<условия фильтра>"
```

где <условия фильтра> – одно или несколько логических выражений в формате <поле> <операция сравнения> '<значение>', скомбинированных с помощью логического оператора and, для ограничения результатов запроса.

Примеры:
Чтобы удалить объект с ID=15:

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

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 резервного хранилища, выполните следующую команду:

```
kesl-control -B --mass-remove
```

Интеграция с решениями Detection and Response

Решения Detection and Response от "Лаборатории Касперского" представляют собой системы безопасности, предназначенные для обнаружения сложных угроз и признаков атак на разных уровнях инфраструктуры организации. Решения Detection and Response предоставляют вам информацию об обнаруженной угрозе и позволяют управлять действиями по реагированию на обнаружения.

Приложение Kaspersky Endpoint Security может взаимодействовать со следующими решениями Detection and Response от "Лаборатории Касперского":

- Kaspersky Anti Targeted Attack Platform (компонент Kaspersky Endpoint Detection and Response). Интеграцию с Kaspersky Endpoint Detection and Response (KATA) обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response (KATA) (далее также EDR (KATA)).

- Kaspersky Endpoint Detection and Response Optimum. Интеграцию обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response Optimum (далее также EDR Optimum).

- Kaspersky Managed Detection and Response. Интеграцию обеспечивает компонент приложения Kaspersky Endpoint Security – Managed Detection and Response (далее также MDR).

При интеграции приложения Kaspersky Endpoint Security с решениями Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform в журнал systemd может записываться большое количество событий. Если вы хотите выключить запись событий аудита в systemd, вам нужно отключить сокет systemd-journald-audit и перезагрузить операционную систему.

Чтобы отключить сокет systemd-journald-audit, выполните следующие команды:

```
systemctl stop systemd-journald-audit.socket

systemctl disable systemd-journald-audit.socket

systemctl mask systemd-journald-audit.socket
```

По умолчанию на операционной системе СинтезМ-Клиент конфигурация службы auditd заблокирована против изменений, то есть находится в режиме работы `enabled 2`. Для корректной работы компонента Анализ поведения при интеграции Kaspersky Endpoint Security с решениями Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform требуется изменить режим работы auditd в конфигурационных файлах на режим без блокировки конфигурации `enabled 1` и перезагрузить операционную систему.

Об ответных действиях по командам от решений Detection and Response

Приложение Kaspersky Endpoint Security может выполнять ответные действия, направленные на обеспечение функций безопасности:

- При взаимодействии с компонентом решения Kaspersky Anti Targeted Attack Platform – Kaspersky Endpoint Detection and Response (KATA).

- При взаимодействии с решением Kaspersky Endpoint Detection and Response Optimum.

Параметры ответных действий Kaspersky Anti Targeted Attack Platform и Kaspersky Endpoint Detection and Response Optimum отличаются.

Приложение Kaspersky Endpoint Security может выполнять следующие ответные действия:

- Получать файлы с устройств.

  Действие выполняется с помощью задачи *Получить файл* (Get file task). Например, вы можете настроить получение файла журнала событий, который создает сторонняя программа.

- Удалять файлы с устройств.

  Действие выполняется с помощью задачи *Удалить файл* (Delete file task).

- Удаленно запускать процессы на устройствах.

  Действие выполняется с помощью задачи *Запустить процесс* (Run process).

  Например, вы можете удаленно запустить утилиту, которая создает файл с конфигурацией устройства, а затем получить созданный файл с помощью задачи *Получить файл*.

- Удаленно завершать процессы на устройствах.

  Действие выполняется с помощью задачи *Завершить процесс* (Terminate process).

  Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи запуска процесса.

- Обнаруживать *индикаторы компрометации* на устройствах и выполнять действия по реагированию на угрозы.

  Действие выполняется с помощью задачи *Поиск IOC* (IOC Scan).

  При выполнении задачи *Поиск IOC* проверка по IOC-терминам (свойствам IOC-объекта, например, хеш-сумме файла) выполняется только в основном пространстве имен операционной системы. Задача *Поиск IOC* не вычисляет хеш-суммы файлов размером более 200 МБ.

- Включать и выключать сетевую изоляцию устройства.

  При взаимодействии Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Optimum вы можете:

  - Включать и выключать сетевую изоляцию в Web Console.
  - Выключать сетевую изоляцию в командной строке.
  - Настроить автоматическое выключение сетевой изоляции в Web Console.

  При взаимодействии Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA) вы можете:

  - Выключать сетевую изоляцию в командной строке.
  - Включать и выключать сетевую изоляцию на стороне решения Kaspersky Endpoint Detection and Response (KATA).

    Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

Ограничения сетевой изоляции

При использовании сетевой изоляции настоятельно рекомендуется ознакомиться с ограничениями, описанными ниже.

Для работоспособности сетевой изоляции требуется, чтобы приложение Kaspersky Endpoint Security было запущено. Во время сбоя в работе приложения Kaspersky Endpoint Security (когда приложение не запущено), блокировка трафика при включении сетевой изоляции решением Kaspersky Anti Targeted Attack Platform или Kaspersky Endpoint Detection and Response Optimum не гарантируется.

Транзитный трафик при включенной сетевой изоляции поддерживается с ограничениями и может фильтроваться.

DHCP и DNS в исключения из сетевой изоляции автоматически не добавляются, поэтому если сетевой адрес какого-то ресурса был изменен во время сетевой изоляции, приложение Kaspersky Endpoint Security не сможет получить к нему доступ. Это же относится к узлам отказоустойчивого сервера KATA. Не рекомендуется менять их адреса, чтобы приложение Kaspersky Endpoint Security не потеряло с ними связь.

Прокси-сервер также в исключения из сетевой изоляции автоматически не добавляется, поэтому требуется добавить его в исключения вручную, чтобы приложение Kaspersky Endpoint Security не потеряло связь с сервером KATA.

Добавление процесса в сетевую изоляцию и исключение процесса из сетевой изоляции по имени не поддерживается.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме, при использовании сетевой изоляции рекомендуется:

- Использовать прокси-сервер KSN для взаимодействия с Kaspersky Security Network.
- Использовать Kaspersky Security Center в качестве прокси-сервера для активации приложения.

  В случае невозможности использования Kaspersky Security Center в качестве прокси-сервера настройте параметры нужного прокси-сервера и добавьте его в исключения.
- Указать Kaspersky Security Center в качестве источника обновлений баз.

Эти рекомендации неприменимы, если приложение Kaspersky Endpoint Security используется в режиме Легкого агента.

Интеграция с Kaspersky Endpoint Detection and Response (KATA)

Kaspersky Endpoint Detection and Response (KATA) – компонент в составе решения Kaspersky Anti Targeted Attack Platform. Интеграцию с компонентом Kaspersky Endpoint Detection and Response (KATA) обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response (KATA) (далее также EDR (KATA)).

Приложение Kaspersky Endpoint Security совместимо с решением Kaspersky Anti Targeted Attack Platform, которое предназначено для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats (далее также "APT"). Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

Эта функциональность не поддерживается в KESL-контейнере.

При взаимодействии с Kaspersky Endpoint Detection and Response (KATA) приложение Kaspersky Endpoint Security может выполнять следующие функции:

- Отправлять данные о событиях на устройствах (телеметрию) на сервер Kaspersky Anti Targeted Attack Platform с компонентом Central Node (далее также сервер KATA). Приложение Kaspersky Endpoint Security передает на сервер KATA данные наблюдения за процессами, открытыми сетевыми соединениями и изменяемыми файлами, а также данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

- Выполнять ответные действия, направленные на обеспечение функций безопасности, по командам, полученным от Kaspersky Anti Targeted Attack Platform.

Для интеграции с Kaspersky Endpoint Detection and Response (KATA) должен быть включен компонент Анализ поведения.

Интеграция приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA) возможна, только если компонент Анализ поведения включен. В противном случае необходимые данные телеметрии не передаются.

Дополнительно Kaspersky Endpoint Detection and Response (KATA) может использовать данные, полученные от следующих компонентов:

- Защита от файловых угроз.

- Защита от сетевых угроз.

- Защита от веб-угроз.

Во время интеграции с Kaspersky Endpoint Detection and Response (KATA), устройства с Kaspersky Endpoint Security устанавливают защищенные соединения с сервером KATA по протоколу HTTPS. Для обеспечения безопасности соединения используются следующие сертификаты, выданные сервером KATA:

- Сертификат сервера KATA. Соединение шифруется с помощью TLS-сертификата сервера. Вы можете повысить уровень безопасности соединения, включив проверку сертификата сервера на стороне Kaspersky Endpoint Security. Для этого вам нужно добавить сертификат сервера интеграции перед включением интеграции с Kaspersky Endpoint Detection and Response (KATA).

- Сертификат клиента. Этот сертификат используется для дополнительной защиты подключения с помощью двусторонней аутентификации (проверки устройств с Kaspersky Endpoint Security сервером KATA). Один и тот же сертификат клиента может использоваться несколькими устройствами. По умолчанию сервер KATA не выполняет проверку сертификатов клиентов, но двусторонняя аутентификация может быть включена на стороне Kaspersky Anti Targeted Attack Platform. В этом случае вам нужно включить двустороннюю аутентификацию в параметрах интеграции с Kaspersky Endpoint Detection and Response (KATA) и добавить сертификат клиента (криптоконтейнер с сертификатом и закрытым ключом).

Сертификаты для защиты соединения с сервером KATA предоставляет администратор Kaspersky Anti Targeted Attack Platform.

Для подключения к серверу KATA используется прокси-сервер, если использование прокси-сервера настроено в общих параметрах приложения Kaspersky Endpoint Security.

По умолчанию интеграция с Kaspersky Endpoint Detection and Response (KATA) выключена. Вы можете включать и выключать интеграцию, а также настраивать следующие параметры интеграции с помощью командной строки, Web Console и Консоли администрирования:

- Настраивать общие параметры подключения к серверам KATA.
- Добавлять и удалять сертификаты серверов KATA.
- Настраивать двустороннюю аутентификацию при подключении к серверам KATA и добавлять сертификаты клиента.
- Настраивать параметры отправки событий.
- Включать и выключать отправку телеметрии.

  Если включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response, исключения по процессам не применяются при отправке телеметрии.

Управление параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA) через Kaspersky Security Center Cloud Console не поддерживается.

Настройка интеграции с Kaspersky Endpoint Detection and Response (KATA) в Web Console

В Web Console вы можете включать и выключать интеграцию приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA) и настраивать параметры интеграции в свойствах политики (**Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response (KATA)**).

Управление параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA) через Kaspersky Security Center Cloud Console не поддерживается.

Параметры интеграции с Kaspersky Endpoint Detection and Response (KATA)

Параметр	Описание
Endpoint Detection and Response (KATA) включен / выключен	Включает или выключает интеграцию приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA). По умолчанию интеграция выключена.
Параметры подключения к серверам	По ссылке **Настроить** открывается окно, в котором вы можете настроить общие параметры подключения к серверам KATA, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверам KATA.
Серверы KATA	Таблица содержит список серверов KATA, к которым настроено подключение. По кнопке **Добавить** открывается окно, в котором вы можете настроить подключение к серверу KATA. С помощью кнопок над таблицей вы можете изменять и удалять ранее настроенные параметры подключения.
Максимальная задержка отправки событий (сек.)	Максимальная задержка отправки событий на сервер KATA в секундах. Значение по умолчанию: `30`.

Включить регулирование количества событий	Включает или выключает регулирование количества событий, отправляемых на сервер KATA.
Максимальное количество событий в час	Максимальное количество событий в час. Значение по умолчанию: `3000`.
Процент превышения лимита событий	Процент превышения лимита событий. Передача событий ограничивается, если соотношение событий одного типа (например, событий изменений в реестре) к общему количеству событий превышает установленное ограничение в процентах. Значение по умолчанию: `15`.

Окно настройки параметров подключения к серверам

В этом окне вы можете настроить общие параметры подключения к серверам KATA, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверам KATA.

Параметры подключения к серверу KATA

Параметр	Описание
Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)	Периодичность отправки запросов на синхронизацию на сервер KATA в минутах. Значение по умолчанию: `5`.
Максимальное время ожидания соединения с сервером (сек.)	Максимальное время ожидания соединения с сервером KATA в секундах. Значение по умолчанию: `10`.
Максимальное время ожидания ответа от сервера (сек.)	Максимальное время ожидания ответа от сервера KATA в секундах. Значение по умолчанию: `10`.
Разрешить отправку телеметрии	Включает или выключает отправку данных о событиях на устройствах (телеметрии) на сервер KATA. По умолчанию отправка телеметрии включена.
Сертификат сервера	После добавления сертификата сервера отображается информация о сертификате: • серийный номер сертификата; • субъект сертификата; • издатель сертификата; • дата начала срока действия сертификата; • дата окончания срока действия сертификата.
Выбрать	Открывает стандартное окно выбора файла, в котором вы можете указать путь к сертификату сервера KATA.

	Если сертификат сервера добавлен, выполняется проверка сертификата сервера на стороне Kaspersky Endpoint Security, это позволяет повысить уровень безопасности соединения.
Удалить	Удаляет ранее добавленный сертификат сервера. Кнопка отображается только если сертификат сервера добавлен.
Дополнительная защита подключения	Блок параметров позволяет включить или выключить двустороннюю аутентификацию при подключении к серверу KATA и добавить сертификат клиента.
Использовать двустороннюю аутентификацию	Включает или выключает использование двусторонней аутентификации для дополнительной защиты соединения с сервером KATA. Двусторонняя аутентификация должна быть включена на стороне сервера KATA. Чтобы использовать двустороннюю аутентификацию, вам нужно добавить сертификат клиента.
Добавить сертификат клиента	Открывает стандартное окно выбора файла, в котором вы можете указать путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ. Кнопка доступна, если установлен флажок **Использовать двустороннюю аутентификацию**.
Изменить	Позволяет указать пароль криптоконтейнера с сертификатом клиента. Поле **Пароль криптоконтейнера** недоступно для редактирования. По умолчанию пароль пустой. Чтобы указать пароль, нажмите на кнопку **Изменить**, в открывшемся окне введите пароль и нажмите на кнопку **ОК**. При нажатии на кнопку **Показать** в окне ввода пароля пароль отображается в открытом виде. Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев. Кнопка доступна, если установлен флажок **Использовать двустороннюю аутентификацию**.

Окно добавления параметров подключения к серверу KATA

В этом окне вы можете указать параметры подключения к серверу KATA.

Параметры подключения к серверу KATA

Параметр	Описание
Адрес	Адрес сервера KATA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером KATA не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера. Значение по умолчанию: `127.0.0.1`.

Порт	Порт для подключения к серверу KATA. Значение по умолчанию: 443.

Настройка интеграции с Kaspersky Endpoint Detection and Response (KATA) в Консоли администрирования

В Консоли администрирования вы можете включать и выключать интеграцию приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA) и настраивать параметры интеграции в свойствах политики (**Detection and Response → Endpoint Detection and Response (KATA)**).

Параметры интеграции с Kaspersky Endpoint Detection and Response (KATA)

Параметр	Описание
Интеграция с Endpoint Detection and Response (KATA)	Включает или выключает интеграцию приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA). По умолчанию интеграция выключена.
Серверы KATA	По кнопке **Настроить** открывается окно **Серверы KATA**. В этом окне вы можете настраивать подключение к серверам KATA, а также просматривать список серверов, к которым настроено подключение.
Параметры подключения к серверам	По кнопке **Настроить** открывается окно, в котором вы можете настроить общие параметры подключения к серверам KATA, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверам KATA.
Параметры передачи данных	По кнопке **Настроить** открывается окно, в котором вы можете настроить параметры передачи данных на серверы KATA.

Окно Серверы KATA

В этом окне в таблице отображается список параметров подключения к серверам KATA. Для каждого сервера, к которому настроено подключение, в таблице указывается IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера и порт.

С помощью кнопок и меню над таблицей вы можете выполнить следующие действия:

- Добавить параметры подключения к серверу KATA.
- Изменить или удалить ранее настроенные параметры подключения.
- Экспортировать или импортировать список настроенных параметров подключения.

Окно добавления параметров подключения к серверу KATA

В этом окне вы можете указать параметры подключения к серверу KATA.

Параметры подключения к серверу KATA

Параметр	Описание

Адрес	Адрес сервера KATA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером KATA не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера. Значение по умолчанию: `127.0.0.1`.
Порт	Порт для подключения к серверу KATA. Значение по умолчанию: `443`.

Окно настройки параметров подключения к серверам

В этом окне вы можете настроить общие параметры подключения к серверам KATA.

Параметры подключения к серверам KATA

Параметр	Описание
Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)	Периодичность отправки запросов на синхронизацию на сервер KATA в минутах. Значение по умолчанию: 5.
Максимальное время ожидания соединения с сервером (сек.)	Максимальное время ожидания соединения с сервером KATA в секундах. Значение по умолчанию: `10`.
Максимальное время ожидания ответа от сервера (сек.)	Максимальное время ожидания ответа от сервера KATA в секундах. Значение по умолчанию: `10`.
Разрешить отправку телеметрии	Включает или выключает отправку данных о событиях на устройствах (телеметрии) на сервер KATA. По умолчанию отправка телеметрии включена.
Использовать двустороннюю аутентификацию	Включает или выключает использование двусторонней аутентификации для дополнительной защиты соединения с сервером KATA. Чтобы использовать двустороннюю аутентификацию, вам нужно добавить сертификат клиента. Двусторонняя аутентификация должна быть включена на стороне сервера KATA.
Добавить (сертификат клиента)	Открывает окно добавления сертификата клиента для дополнительной защиты соединения с сервером KATA. Кнопка отображается, если сертификат клиента еще не добавлен. Если вы хотите настроить дополнительную защиту соединения, вам нужно включить проверку сертификатов клиентов на стороне сервера KATA и установить флажок **Использовать двустороннюю аутентификацию** в этом окне.

Удалить (сертификат клиента)	Удаляет сертификат клиента. Кнопка отображается, если сертификат клиента добавлен.
Добавить (сертификат сервера)	Открывает окно добавления сертификата сервера. Кнопка отображается, если сертификат сервера еще не добавлен.
Удалить (сертификат сервера)	Удаляет сертификат сервера. Кнопка отображается, если сертификат сервера добавлен.

Окно добавления сертификата сервера

В этом окне вы можете добавить сертификат сервера KATA одним из следующих способов:

- Указать путь к файлу сертификата в поле **Добавить из файла**. По кнопке **Обзор** открывается стандартное окно для выбора файла. Укажите путь к файлу, содержащему сертификат формата DER или PEM.
- Скопировать содержимое файла сертификата в поле **Ввести данные сертификата**.

Если сертификат сервера добавлен, выполняется проверка сертификата сервера на стороне Kaspersky Endpoint Security, это позволяет повысить уровень безопасности соединения.

Окно добавления сертификата клиента

В этом окне вы можете добавить сертификат клиента для дополнительной защиты соединения с сервером KATA.

Если вы хотите настроить дополнительную защиту соединения, вам нужно включить проверку сертификатов клиентов на стороне сервера KATA и установить флажок **Использовать двустороннюю аутентификацию** в окне настройки параметров подключения к серверам.

Чтобы добавить сертификат клиента, укажите путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ. По кнопке **Обзор** открывается стандартное окно для выбора файла. Если архив защищен паролем, введите пароль в поле **Пароль криптоконтейнера**.

Окно Параметры передачи данных

В этом окне вы можете настроить параметры передачи данных на серверы KATA.

Параметры передачи данных на серверы KATA

Параметр	Описание
Максимальная задержка отправки событий (сек.)	Максимальная задержка отправки событий на сервер KATA в секундах. Значение по умолчанию: `30`.
Включить регулирование количества событий	Включает или выключает регулирование количества событий, отправляемых на сервер KATA.

Максимальное количество событий в час	Максимальное количество событий в час. Значение по умолчанию: `3000`.
Процент превышения лимита событий	Процент превышения лимита событий. Передача событий ограничивается, если соотношение событий одного типа (например, событий изменений в реестре) к общему количеству событий превышает установленное ограничение в процентах. Значение по умолчанию: `15`.

Настройка интеграции с Kaspersky Endpoint Detection and Response (KATA) в командной строке

В командной строке вы можете управлять интеграцией приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA) с помощью предустановленной задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA) (*KATAEDR*).

По умолчанию задача Интеграция с Kaspersky Endpoint Detection and Response (KATA) не запущена. Вы можете запускать и останавливать эту задачу вручную.

Вы можете настраивать параметры интеграции с Kaspersky Endpoint Detection and Response (KATA), изменяя параметры предустановленной задачи.

С помощью команд управления параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA) вы можете управлять сертификатами, которые используются для подключения к серверам KATA.

Параметры задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA)

В таблице ниже описаны все доступные параметры и значения по умолчанию для всех параметров, которые вы можете указать для задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA).

Параметры задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA)

Параметр	Описание	Значение
`Address`	Адрес сервера KATA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером KATA не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу KATA.	Значение по умолчанию: `443`.
`UseClientPinnedCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу KATA.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты

	Если двусторонняя аутентификация включена на стороне сервера KATA, вам нужно включить двустороннюю аутентификацию в параметрах задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA) и добавить сертификат клиента перед запуском задачи.	подключения к серверу KATA. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`SynchronizationPeriod`	Периодичность отправки запросов на синхронизацию на сервер KATA в минутах.	Значение по умолчанию: `5`.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером KATA в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера KATA в секундах.	Значение по умолчанию: `10`.
`MaximumDataTransferTime`	Максимальная задержка отправки событий на сервер KATA в секундах.	Значение по умолчанию: `30`.
`UseRequestCountLimits`	Включение и выключение регулирования количества событий, отправляемых на сервер KATA.	`Yes` (значение по умолчанию) – регулировать количество отправляемых событий. `No` – не регулировать количество событий.
`MaximumNumberOfEventsInHour`	Максимальное количество событий в час.	Значение по умолчанию: `3000`.
`EventLimitExceededPercentage`	Процент превышения лимита событий. Передача событий ограничивается, если соотношение событий одного типа к общему количеству событий превышает установленное ограничение в процентах.	Значение по умолчанию: `15`.
`EnableTelemetry`	Включение и выключение отправки данных о событиях на устройствах (телеметрии) на сервер KATA.	`Yes` (значение по умолчанию) – отправлять телеметрию на сервер KATA. `No` – не отправлять телеметрию.

Управление сертификатами для подключения к серверам KATA

Для управления сертификатами требуются root-права.

Вы можете управлять сертификатами, которые используются для подключения к серверам KATA, с помощью команд. Вы можете выполнять следующие действия с сертификатами:

- добавлять или заменять сертификат сервера;
- выводить информацию о сертификате сервера;
- удалять сертификат сервера;
- добавлять или заменять сертификат клиента;
- выводить информацию о сертификате клиента;
- удалять сертификат клиента.

Чтобы добавить или заменить сертификат сервера, выполните следующую команду:

```
kesl-control [-R] --add-kataedr-server-certificate <путь к файлу>
```

где `<путь к файлу>` – путь к файлу, содержащему сертификат сервера.

Чтобы добавить или заменить сертификат клиента:

1. Выполните команду:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <путь к файлу>
   ```

   где `<путь к файлу>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

2. Если криптоконтейнер защищен паролем, введите пароль по запросу.

Сертификат клиента используется для дополнительной защиты соединения с сервером KATA, если в параметрах сервера KATA включена проверка сертификата клиента и в параметрах задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA) для параметра `UseClientPinnedCertificate` установлено значение `yes`.

Чтобы вывести информацию о сертификате, выполните следующую команду:

- для сертификата сервера:

  ```
  kesl-control [-R] --query-kataedr-server-certificate
  ```

- для сертификата клиента:

  ```
  kesl-control [-R] --query-kataedr-client-certificate
  ```

  В результате выполнения команды выводится следующая информация о сертификате:

- серийный номер сертификата;
- субъект сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;

- SHA1 и SHA256 отпечатки сертификата.

Чтобы удалить сертификат сервера, выполните следующую команду:

```
kesl-control [-R] --remove-kataedr-server-certificate
```

Чтобы удалить сертификат клиента, выполните следующую команду:

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Если использование сертификата настроено в параметрах задачи Интеграция с Kaspersky Endpoint Detection and Response (KATA) и задача запущена, удаление этого сертификата завершается с ошибкой.

Интеграция с Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum – решение, предназначенное для защиты IT-инфраструктуры организации от таких угроз, как эксплойты (англ. exploits), программы-вымогатели (англ. ransomware), бесфайловые атаки (англ. fileless attacks) и использование злоумышленниками законных системных инструментов для нанесения вреда устройствам или данным.

Kaspersky Endpoint Detection and Response Optimum выполняет мониторинг и анализ развития угрозы, а также предоставляет сотруднику службы безопасности или администратору информацию о потенциальной атаке, необходимую для принятия своевременных действий по реагированию.

Интеграцию приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Optimum обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response Optimum (далее также EDR Optimum).

Приложение Kaspersky Endpoint Security 12.1 для Linux совместимо с решением Kaspersky Endpoint Detection and Response Optimum версии 3.0.

В составе Kaspersky Endpoint Security для Linux версии ниже 12.1 компонент EDR Optimum отсутствует.

Kaspersky Endpoint Detection and Response Optimum использует следующие средства анализа угроз (Threat Intelligence):

- Инфраструктура облачных служб Kaspersky Security Network (далее также KSN), предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-сайтов и программного обеспечения.
- Интеграция с порталом Kaspersky Threat Intelligence Portal, который содержит и отображает информацию о репутации файлов и веб-сайтов.
- База угроз "Лаборатории Касперского" Kaspersky Threats.

При взаимодействии с Kaspersky Endpoint Detection and Response Optimum приложение Kaspersky Endpoint Security может выполнять следующие функции:

- Отправлять в Kaspersky Security Center данные о событиях на устройствах. Приложение Kaspersky Endpoint Security передает в Kaspersky Security Center данные наблюдения за процессами, открытыми

сетевыми соединениями и изменяемыми файлами, а также данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

- Выполнять ответные действия, направленные на обеспечение функций безопасности, по командам, полученным от Kaspersky Security Center.

Интеграция с Kaspersky Endpoint Detection and Response Optimum состоит из следующих этапов:

1. **Включение необходимых компонентов Kaspersky Endpoint Security**

   Убедитесь, что следующие компоненты Kaspersky Endpoint Security включены и работают:

   - Защита от файловых угроз.
   - Защита от веб-угроз.
   - Анализ поведения.

2. **Включение средств анализа угроз**

   Убедитесь, что включен Kaspersky Security Network в стандартном или расширенном режиме.

   > Для наиболее эффективной работы Kaspersky Endpoint Detection and Response Optimum рекомендуется использовать Kaspersky Security Network в расширенном режиме.

3. **Активация компонента EDR Optimum**

   Убедитесь, что соблюдено одно из следующих условий:

   - Вы используете приложение Kaspersky Endpoint Security по лицензии, которая включает функциональность Kaspersky Endpoint Detection and Response Optimum.
   - Вы приобрели отдельную лицензию на использование функциональности Kaspersky Endpoint Detection and Response Optimum и добавили в приложение дополнительный лицензионный ключ EDR Optimum.

4. **Включение интеграции с решением Kaspersky Endpoint Detection and Response Optimum**

   По умолчанию интеграция Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Optimum выключена. Вы можете включать и выключать интеграцию, а также настраивать параметры интеграции:

   - с помощью Web Console;
   - с помощью командной строки.

     > Управление компонентом EDR Optimum с помощью Консоли администрирования Kaspersky Security Center не поддерживается.

   Вы можете проверить статус работы компонента EDR Optimum:

   - С помощью *Отчета о статусе компонентов приложения* в Web Console.

     В список компонентов Kaspersky Endpoint Security добавлен компонент **Endpoint Detection and Response Optimum**. Подробную информацию о работе с отчетами см. в справке Kaspersky Security Center.
   - В свойствах устройства в Web Console.

- С помощью командной строки.

5. **Включение передачи данных на Сервер администрирования**

   Для использования всех возможностей Kaspersky Endpoint Detection and Response Optimum вам нужно включить следующие параметры:

   - **Информирование о файлах в резервном хранилище включено/выключено**.

     Вы можете включить этот параметр в свойствах политики в разделе **Параметры приложения** → **Общие параметры** → **Параметры Хранилища**.

     Включив этот параметр, вы разрешите передачу в Kaspersky Security Center информации о файлах, помещенных приложением Kaspersky Endpoint Security в резервное хранилище на устройстве.

   - **Показать EDR-алерты**.

     Вы можете включить этот параметр в главном окне Web Console в разделе **Параметры** → **Параметры интерфейса**.

     Включив этот параметр, вы разрешите отображение списка алертов.

     Параметр **Показать EDR-алерты** отсутствует в Web Console версии ниже 15.1.

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum

Вы можете включать и выключать интеграцию с Kaspersky Endpoint Detection and Response Optimum:

- с помощью Web Console;
- с помощью командной строки.

Управление параметрами интеграции с Kaspersky Endpoint Detection and Response Optimum через Консоль администрирования не поддерживается.

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console

В Web Console вы можете включать и выключать интеграцию приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Optimum и настраивать параметры интеграции:

- в свойствах политики (**Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response Optimum**);
- в свойствах устройства (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → **Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response Optimum**).

Включение и выключение интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Optimum в свойствах устройства недоступно, если на устройство распространяется действие политики.

Параметры интеграции с Kaspersky Endpoint Detection and Response Optimum

Параметр	Описание
Endpoint Detection and Response Optimum включен/ выключен	Включает или выключает интеграцию приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Optimum. По умолчанию интеграция выключена.
Сетевая изоляция	По ссылке **Настроить разблокировку устройства** открывается окно **Настройка разблокировки устройства,** в котором вы можете настроить длительность блокировки устройства.
Исключения	По ссылке **Исключения** открывается окно **Исключения**, в котором вы можете настроить исключения сетевой изоляции.

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в командной строке

В командной строке вы можете включать и выключать интеграцию с Kaspersky Endpoint Detection and Response Optimum с помощью параметра `UseEdrOptimum` в общих параметрах приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Чтобы включить интеграцию с Kaspersky Endpoint Detection and Response Optimum с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

Чтобы выключить интеграцию с Kaspersky Endpoint Detection and Response Optimum с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-app-settings UseEdrOptimum=No
```

Просмотр статуса интеграции с Kaspersky Endpoint Detection and Response Optimum

Просмотр статуса интеграции в Web Console

Вы можете посмотреть статус интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console, выбрав раздел **Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → **Общие** → **Компоненты**.

Просмотр статуса интеграции в командной строке

Вы можете посмотреть статус интеграции с Kaspersky Endpoint Detection and Response Optimum с помощью командной строки, выполнив команду `kesl-control --app-info`.

Статусы интеграции

Для компонента EDR Optimum отображается один из следующих статусов:

- *Выполняется*.

  Этот статус отображается при одновременном соблюдении следующих условий:

  - добавлен лицензионный ключ, необходимый для работы EDR Optimum;
  - текущая дата не превышает дату окончания срока действия лицензии;
  - один или несколько компонентов Kaspersky Endpoint Security, необходимых для работы EDR Optimum, включены;
  - на устройстве включена интеграция с Kaspersky Endpoint Detection and Response Optimum.

- *Остановлена*.

  Этот статус отображается в следующих случаях:

  - интеграция с Kaspersky Endpoint Detection and Response Optimum выключена;
  - приложение Kaspersky Endpoint Security остановлено.

- *Не поддерживается лицензией*.

  Этот статус отображается в следующих случаях:

  - текущая дата превышает дату окончания срока действия лицензии;
  - действующая лицензия не включает функциональность EDR Optimum.

- *Ошибка*.

  Этот статус отображается при одновременном соблюдении следующих условий:

  - текущая дата не превышает дату окончания срока действия лицензии;
  - в работе одного или нескольких компонентов Kaspersky Endpoint Security, необходимых для работы EDR Optimum, произошла ошибка.

Просмотр информации об обнаруженной угрозе и действиях по реагированию

Для просмотра всей информации об обнаруженной угрозе и выполнения действий по реагированию на эту угрозу вы можете воспользоваться окном с деталями алерта, которое содержит:

- граф цепочки развития угрозы;
- рекомендации по реагированию на угрозу с возможностью выполнения выбранного действия;

- общую информацию об обнаружении угрозы (например, о режиме обнаружения);
- информацию о защищаемом устройстве;
- информацию об обнаруженном объекте;
- историю появления файлов на устройстве;
- информацию о выполненных приложением действиях по реагированию на обнаруженную угрозу.

Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum.

Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет старые записи.

Поиск индикаторов компрометации

Вы можете выполнять поиск индикаторов компрометации на устройстве, а также выполнять действия по реагированию на угрозы с помощью задачи *Поиск IOC*.

Для поиска индикаторов компрометации Kaspersky Endpoint Security использует IOC-файлы, подготовленные пользователем. IOC-файлы должны соответствовать требованиям к IOC-файлам.

Вы можете создавать и запускать задачу *Поиск IOC*, а также изменять ее параметры в Web Console:

- в разделе **Активы (Устройства)** → **Задачи**;
- в разделе **Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → **Задачи**;
- в окне с деталями алерта.

Вы не можете создавать, запускать или настраивать задачу *Поиск IOC* с помощью командной строки. Просмотр задачи *Поиск IOC*, созданной в Web Console, недоступен по команде `kesl-control --get-task-list` в командной строке.

Для этой задачи функция Wake-on-LAN в параметрах расписания недоступна. Убедитесь, что устройство включено для выполнения задачи.

Параметры задачи *Поиск IOC*

Параметр	Описание
Переопределить IOC-файлы	При нажатии на кнопку открывается панель **Переопределить IOC-файлы**. При нажатии на кнопку **Добавить IOC-файлы**, расположенную в панели **Переопределить IOC-файлы**, открывается окно, с помощью которого вы можете выбрать на устройстве и загрузить IOC-файлы, необходимые для поиска индикаторов компрометации. После загрузки IOC-файлов вы можете просмотреть список индикаторов из IOC-файлов.
Экспортировать IOC-коллекцию	При нажатии на кнопку выполняется скачивание IOC-файлов на устройство.
Применять	Флажок включает или выключает применение действий по реагированию при

действия по реагированию при обнаружении IOC	обнаружении индикаторов компрометации. Если флажок установлен, то при обнаружении индикаторов компрометации приложение выполняет выбранные вами действия: • **Изолировать устройство от сети**. Если флажок установлен, то при обнаружении индикаторов компрометации приложение изолирует устройство от сети для предотвращения распространения угрозы. Вы можете настроить время изоляции. • **Запускать проверку важных областей**. Если флажок установлен, то при обнаружении индикаторов компрометации приложение запускает задачу *Проверка важных областей*. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы. Если флажок снят, то при обнаружении индикаторов компрометации приложение не выполняет действия по реагированию. Информация об обнаружении индикаторов компрометации отображается в окне с деталями алерта и в свойствах задачи.
Области проверки	Отображаются области проверки файлов: важные области системных дисков и путь из IOC.

Не рекомендуется добавлять или удалять IOC-файлы после запуска задачи. Это может привести к некорректному отображению результатов поиска IOC для предыдущих запусков задачи. Для поиска индикаторов компрометации по новым IOC-файлам рекомендуется добавлять новые задачи.

Результат выполнения задачи *Поиск IOC* можно посмотреть в разделе **Активы (Устройства)** → **Задачи** → <название задачи> → **Параметры приложения** → **Результаты поиска IOC**.

Таблица в разделе **Результаты поиска IOC** содержит список устройств, на которых выполнена задача *Поиск IOC*, а также результаты выполнения задачи. В раскрывающемся списке **Устройство** вы можете выбрать результаты выполнения задачи для всех управляемых устройств группы администрирования или для конкретного устройства.

Таблица содержит следующие столбцы:

- **Статус**.

  Статус обнаружения индикаторов компрометации, отображающийся в виде значка.

- **Устройство**.

  Имя устройства, на котором выполнена задача *Поиск IOC*.

- **Время**.

  Дата и время выполнения задачи *Поиск IOC*.

- **Результаты**.

  Информация о результате выполнения задачи *Поиск IOC*. В результате выполнения задачи может отображаться один из следующих статусов:

  - *обнаружены IOC*;

    Этот статус отображается в виде ссылки, при переходе по которой открывается окно с деталями алерта.

  - *IOC не обнаружены*.

Также результат выполнения задачи можно посмотреть в разделе **Активы (Устройства)** → **Задачи** → <название задачи> на закладке **Результаты** в столбце **Описание**.

Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет старые записи.

Требования к IOC-файлам

При создании задач поиска IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- Приложение поддерживает IOC-файлы с расширением IOC и XML открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- Семантические ошибки и неподдерживаемые IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов приложение фиксирует отсутствие совпадения.
- Идентификаторы всех IOC-файлов, которые используются в одной задаче поиска IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи *Поиск IOC*.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC.

ЗАГРУЗИТЬ ФАЙЛ IOC TERMS.XLSX

Особенности и ограничения поддержки стандарта OpenIOC приложением приведены в таблице ниже.

Особенности и ограничения поддержки стандарта OpenIOC версий 1.0 и 1.1

Поддерживаемые условия	OpenIOC 1.0: • `is` • `isnot` (как исключение из множества) • `contains` • `containsnot` (как исключение из множества) OpenIOC 1.1: • `is` • `contains` • `starts-with` • `ends-with`

	• `matches` • `greater-than` • `less-than`
Поддерживаемые атрибуты условий	OpenIOC 1.1: • `preserve-case` • `negate`
Поддерживаемые операторы	`AND` `OR`
Поддерживаемые типы данных	`"date"`: дата (применимые условия: `is`, `greater-than`, `less-than`) `"int"`: целое число (применимые условия: `is`, `greater-than`, `less-than`) `"string"`: строка (применимые условия: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: продолжительность в секундах (применимые условия: `is`, `greater-than`, `less-than`)

Особенности интерпретации типов данных	Типы данных `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` интерпретируются как строка (string).
	Приложение поддерживает интерпретацию параметра `Content` для типов данных `int` и `date`, заданного в виде промежутков:
	• OpenIOC 1.0:
	С использованием оператора `TO` в поле `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	• OpenIOC 1.1:
	• С помощью условий `greater-than` и `less-than`
	• С использованием оператора `TO` в поле `Content`
	Приложение поддерживает интерпретацию типов данных `date` и `duration`, если индикаторы заданы в формате `ISO 8601, Zulu time zone, UTC`.

Включение и выключение сетевой изоляции устройства

Вы можете включать сетевую изоляцию устройства следующими способами:

- С помощью задачи *Поиск IOC*.

  Если при создании и настройке параметров задачи *Поиск IOC* в блоке **Действия при обнаружении IOC** вы установили флажки **Применять действия по реагированию при обнаружении IOC** и **Изолировать устройство от сети**, то включение сетевой изоляции происходит автоматически при обнаружении приложением индикаторов компрометации (IOC).

- В окне с деталями алерта.

- В свойствах устройства в Web Console.

> Включение сетевой изоляции доступно только при условии, что включена интеграция с решением Kaspersky Endpoint Detection and Response Optimum и компонент EDR Optimum находится в статусе *Выполняется*.

Вы можете выключать сетевую изоляцию устройства следующими способами:

- Вручную в свойствах устройства в Web Console.
- Вручную в командной строке.
- В окне с деталями алерта.
- Настроив автоматическое выключение в свойствах устройства или в свойствах политики.

> Выключение сетевой изоляции в свойствах устройства и в командной строке доступно вне зависимости от того, включена ли интеграция с решением Kaspersky Endpoint Detection and Response Optimum и активирован ли компонент EDR Optimum, а также вне зависимости от того, распространяется ли на устройство действие политики.

Вы можете настраивать исключения для сетевых соединений, которые не нужно изолировать при включении сетевой изоляции.

Вы можете проверять статус сетевой изоляции в командной строке.

После включения сетевой изоляции приложение разрывает все активные и блокирует все новые сетевые соединения TCP/IP на устройстве, кроме следующих:

- соединений, указанных в исключениях из сетевой изоляции;
- соединений, инициированных службами Kaspersky Endpoint Security;
- соединений, инициированных Агентом администрирования Kaspersky Security Center;
- соединений с SVM и Сервером интеграции, если приложение используется в режиме Легкого агента.

Изолированному устройству EDR Optimum автоматически присваивает тег **ISOLATED FROM NETWORK**. После выключения сетевой изоляции этот тег автоматически снимается.

Общую информацию о получении списка изолированных устройств по тегу см. в справке Kaspersky Endpoint Detection and Response Optimum.

Включение и выключение сетевой изоляции устройства вручную в Web Console

Чтобы включить или выключить сетевую изоляцию устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и в открывшемся окне выберите группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. В списке найдите нужное устройство и нажмите на его имя.

4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.

5. В списке приложений, установленных на устройстве, нажмите на название приложения **Kaspersky Endpoint Security 12.1 для Linux**.

   Откроется окно свойств приложения.

6. Перейдите на закладку **Параметры приложения**.

7. Перейдите в раздел **Detection and Response → Endpoint Detection and Response Optimum**.

8. В блоке параметров **Сетевая изоляция** выполните одно из следующих действий:

   - чтобы включить сетевую изоляцию устройства, нажмите на кнопку **Изолировать устройство от сети**;
   - чтобы выключить сетевую изоляцию устройства, нажмите на кнопку **Разблокировать изолированное устройство**.

Если вы включили сетевую изоляцию устройства, то Kaspersky Endpoint Security присвоит устройству тег **ISOLATED FROM NETWORK**. Если вы выключили сетевую изоляцию устройства, то Kaspersky Endpoint Security снимет этот тег с устройства.

Настройка автоматического выключения сетевой изоляции

Вы можете настроить автоматическое выключение сетевой изоляции по истечении заданного периода времени:

- В свойствах устройства.

  Настройка автоматического выключения сетевой изоляции в свойствах устройства недоступна, если на устройство распространяется действие политики.

- В свойствах политики.

  Параметры автоматического выключения сетевой изоляции, указанные в свойствах политики, применяются только к тем устройствам, которые были изолированы в результате обнаружения индикаторов компрометации (IOC) при выполнении задачи *Поиск IOC*.

По умолчанию приложение выключает сетевую изоляцию через 5 часов с момента включения. После выключения сетевой изоляции устройство может работать в сети без ограничений.

Настройка автоматического выключения сетевой изоляции в свойствах устройства

Чтобы настроить автоматическое выключение сетевой изоляции устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Найдите нужное устройство в списке и нажмите на его имя.

4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.

5. В списке приложений, установленных на устройстве, нажмите на название приложения **Kaspersky Endpoint Security 12.1 для Linux**.

   Откроется окно свойств приложения.

6. Перейдите на закладку **Параметры приложения**.

7. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response Optimum**.

8. В блоке параметров **Сетевая изоляция** нажмите на ссылку **Настроить разблокировку устройства**.

9. В открывшемся окне **Настроить разблокировку устройства** задайте параметры разблокировки устройства.

   Параметры разблокировки устройства

Параметр	Описание
Разблокировать автоматически изолированное устройство через	Флажок включает или выключает автоматическую разблокировку изолированного устройства по истечении временного периода, указанного в поле ввода ниже. По умолчанию флажок установлен.

10. Сохраните внесенные изменения.

Настройка автоматического выключения сетевой изоляции в свойствах политики

Чтобы настроить автоматическое выключение сетевой изоляции устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую устройства, на которых применяется политика. Для этого нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите группу администрирования в открывшемся окне.

   В списке отобразятся политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.

   Откроется окно свойств политики.

4. Перейдите на закладку **Параметры приложения**.
5. Перейдите в раздел **Detection and Response → Endpoint Detection and Response Optimum**.
6. В блоке параметров **Сетевая изоляция** нажмите на ссылку **Настроить разблокировку устройства**.
7. В открывшемся окне **Настроить разблокировку устройства** задайте параметры разблокировки устройства.

Параметры разблокировки устройства

Параметр	Описание
Разблокировать автоматически изолированное устройство через	Флажок включает или выключает автоматическую разблокировку изолированного устройства по истечении временного периода, указанного в поле ввода ниже. По умолчанию флажок установлен.

8. Сохраните внесенные изменения.

Выключение сетевой изоляции устройства в командной строке

Чтобы выключить сетевую изоляцию устройства с помощью командной строки, выполните следующую команду:

```
kesl-control [-R] --isolation-off
```

Вы можете проверить статус сетевой изоляции и просмотреть список исключений из сетевой изоляции с помощью следующей команды:

```
kesl-control [-R] --isolation-stat
```

Для сетевой изоляции в командной строке отображается один из следующих статусов:

- *Сетевая изоляция включена.*
- *Сетевая изоляция выключена.*

Настройка исключений из сетевой изоляции

Вы можете настраивать исключения:

- в свойствах политики;
- в свойствах устройства.

Сетевые соединения, на которые распространяются заданные правила, не будут заблокированы на устройстве после включения сетевой изоляции.

По умолчанию из сетевой изоляции исключаются сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент.

Исключения, заданные в свойствах политики, применяются, только если сетевая изоляция включена приложением автоматически, в результате реагирования на обнаружение индикаторов компрометации (IOC).

Исключения, заданные в свойствах устройства, применяются, только если сетевая изоляция включена вручную в свойствах устройства или в окне с деталями алерта.

Активная политика не блокирует применение исключений из сетевой изоляции, заданных в свойствах устройства.

Вы можете просматривать перечень исключений из сетевой изоляции:

- в свойствах политики (**Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response Optimum** → ссылка **Исключения**);
- в свойствах устройства (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → ссылка <название приложения Kaspersky Endpoint Security> → **Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response Optimum** → ссылка **Исключения**);
- в командной строке.

Добавление и удаление исключений из сетевой изоляции в свойствах политики в Web Console

В Web Console вы можете добавлять и удалять исключения из сетевой изоляции в свойствах политики (**Параметры приложения** → **Detection and Response** → **Endpoint Detection and Response Optimum** → ссылка **Исключения**).

В окне **Исключения** с помощью кнопок над таблицей вы можете выполнить следующие действия:

- добавить информацию об исключаемом сетевом соединении одним из следующих способов:
  - нажать на кнопку **Добавить**, а затем ввести информацию о сетевом соединении;
  - нажать на кнопку **Добавить из профиля**, а затем выбрать сетевой профиль из словаря;
- удалить информацию о сетевом соединении.

Добавление и удаление исключения из сетевой изоляции в свойствах устройства

Добавление и удаление исключений из сетевой изоляции в свойствах устройства недоступно, если на устройство распространяется действие политики.

Чтобы добавить или удалить исключение из сетевой изоляции в свойствах устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Найдите нужное устройство в списке и нажмите на его имя.

4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.

5. В списке приложений, установленных на устройстве, нажмите на название приложения **Kaspersky Endpoint Security 12.1 для Linux**.

   Откроется окно свойств приложения.

6. Перейдите на закладку **Параметры приложения**.

7. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response Optimum**.

8. В блоке параметров **Сетевая изоляция** по ссылке **Исключения** откройте окно **Исключения**.

9. В открывшемся окне с помощью кнопок над таблицей выполните необходимое действие:

   - Если вы хотите добавить информацию об исключаемом сетевом соединении, сделайте это одним из следующих способов:
     - нажмите на кнопку **Добавить** и ввести информацию о сетевом соединении;
     - нажмите на кнопку **Добавить из профиля** и выбрать сетевой профиль из словаря.
   - Если вы хотите удалить информацию об исключаемом сетевом соединении, установите флажок напротив удаляемого сетевого соединения и нажмите на кнопку **Удалить**;

10. Сохраните внесенные изменения.

Окно добавления исключения из сетевой изоляции

В этом окне вы можете ввести информацию о сетевом соединении, которое не нужно блокировать после включения сетевой изоляции.

Параметры сетевого соединения

Параметр	Описание
Название	Название сетевого соединения.
Направление	Направление сетевого соединения.
Протокол	Протокол, используемый сетевым соединением.
Номер	Номер сетевого соединения.
Локальный порт(ы) / диапазон(ы)	Номер локального порта(ов) или диапазон(ы) локальных портов.

Удаленный порт(ы) / диапазон(ы)	Номер удаленного порта(ов) или диапазон(ы) удаленных портов.
Удаленный адрес	IP-адрес удаленного устройства.

Окно Словарь сетевых профилей

В этом окне вы можете выбрать профиль исключаемого сетевого соединения.

Профили сетевых соединений

Профиль сетевого соединения	Описание
DNS-сервер	Служба, обеспечивающая разрешение DNS-имен, отвечая на запросы получения IP-адресов и запросы обновления DNS-записей.
DNS-клиент	Служба, обеспечивающая разрешение DNS-имен, выполняя запросы DNS-имен.
Службы сертификатов Active Directory	Службы, используемые для создания, проверки и отзыва сертификатов открытых ключей для внутреннего пользования в организации.
Службы федерации Active Directory	Службы, используемые для предоставления пользователям доступа к нескольким веб-службам или сетевым ресурсам при помощи единых наборов учетных данных, хранящихся централизованно.
Службы Active Directory облегченного доступа к каталогам	Службы с теми же функциями, что и доменные службы Active Directory, но не требующие создания доменов или контроллеров домена.
Службы управления правами Active Directory	Службы, используемые для управления доступом пользователей к документам.
DHCP	Служба, использующая протокол динамической конфигурации узлов (DHCP) для автоматического распределения IP-адресов.
Протокол передачи файлов (FTP)	Стандартный сетевой протокол, используемый для передачи файлов между клиентом и сервером в сети.
Центр распространения ключей Kerberos	Сетевая служба, используемая для предоставления тикетов (TGS) и временных ключей сеанса пользователям и устройствам в домене Active Directory.
Безопасная оболочка (SSH)	Протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений.
Системные компоненты Linux	Системные компоненты Linux.

Запуск процесса

Вы можете удаленно запускать необходимые процессы и исполняемые файлы на устройствах с помощью задачи *Запуск процесса*.

Например, вы можете запускать:

- Процессы, остановленные в результате вредоносной активности на устройстве.
- Процессы, остановленные вами.

  Например, вы можете удаленно запустить процесс, который был завершен вами с помощью задачи *Завершение процесса*.
- Скрипты.

  Например, вы можете запустить скрипт, чтобы собрать с устройства данные, необходимые для расследования возникновения угрозы.
- Утилиты.

  Например, вы можете запустить утилиту, которая сохраняет информацию о конфигурации устройства в файл.
- Приложения.

Если в вашей операционной системе установлена система SELinux в режиме `Enforcing`, то для запуска задачи *Запуск процесса* вам нужно дополнительно настроить систему SELinux.

Вы можете создавать и запускать задачу *Запуск процесса*, а также изменять ее параметры в Web Console.

Вы не можете создавать, запускать или настраивать задачу *Запуск процесса* с помощью командной строки. Просмотр задачи *Запуск процесса*, созданной в Web Console, недоступен по команде `kesl-control --get-task-list` в командной строке.

Параметры задачи Запуск процесса

Параметр	Описание
Исполняемая команда	Поле ввода команды запуска процесса. Например, если вы хотите запустить утилиту `klnagchk`, которая предназначена для проверки подключения к Серверу администрирования, вам нужно ввести `/<абсолютный путь к директории с утилитой>/klnagchk`, а затем, если необходимо, заполнить остальные поля, описанные в этой таблице ниже.
Аргументы командной строки (необязательно)	Поле ввода аргументов командной строки для передачи дополнительной информации в скрипт, утилиту или приложение при запуске. Например, вы можете ввести аргумент `-logfile /tmp/klnagchk.log`. Этот аргумент указывает утилите, что результат работы нужно сохранить в файл с именем `klnagchk.log` в директории `/tmp`. Если вам нужно передать несколько аргументов, требуется разделять их пробелами. Например, вы можете ввести аргументы `-logfile /tmp/klnagchk.log -savecert /home/user/certificate.cer`. Эти аргументы указывают утилите, что нужно сохранить результат работы в файл с именем `klnagchk.log` в директории `/tmp`, а также сохранить сертификат, используемый для проверки доступа к Серверу администрирования, в файле `certificate.cer` в директории `/home/user/`.
Путь к рабочей директории (необязательно)	Поле ввода пути к рабочей директории, в которой выполняется команда из поля **Исполняемая команда**. Например, вы можете ввести значение `/tmp` и запустить утилиту `klnagchk` с аргументами `-logfile klnagchk.log -savecert certificate.cer`. В этом случае оба файла будут созданы в директории `/tmp`.

Результат выполнения задачи можно посмотреть в разделе **Активы (Устройства)** → **Задачи** → <название задачи> на закладке **Результаты** в столбце **Описание**.

Завершение процесса

Вы можете удаленно завершать процессы на устройстве с помощью задачи *Завершение процесса*.

Например, вы можете завершать:

- Процессы, запущенные на устройстве в результате вредоносной активности.
- Процессы, запущенные вами.

  Например, вы можете удаленно завершить процесс, который был запущен вами с помощью задачи *Запуск процесса*.
- Скрипты.

  Например, вы можете удаленно завершить работу скрипта, который был запущен вами с помощью задачи *Запуск процесса*.
- Утилиты.

  Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена вами с помощью задачи *Запуск процесса*.
- Приложения.

Завершать процессы критически важных системных объектов (англ. System Critical Object, SCO) невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Endpoint Security.

Вы можете создавать и запускать задачу *Завершение процесса*, а также изменять ее параметры в Web Console. Вы не можете создавать, запускать или настраивать задачу *Завершение процесса* с помощью командной строки. Просмотр задачи *Завершение процесса*, созданной из Web Console, недоступен по команде `kesl-control --get-task-list` в командной строке.

Параметры задачи Завершение процесса

Параметр	Описание
Укажите файл, процессы которого требуется завершить	В раскрывающемся списке вы можете выбрать способ указания пути к файлу: • **По пути к директории и контрольной сумме**. • **По полному пути**. • **По PID**. Значение **По PID** отображается в раскрывающемся списке только для задач, создаваемых в свойствах устройства.
Полный путь к файлу	Поле ввода полного пути к файлу. Это поле отображается, только если в раскрывающемся списке **Укажите файл, процессы которого требуется завершить** вы выбрали значение **По полному пути**.

Тип контрольной суммы	В раскрывающемся списке вы можете выбрать тип контрольной суммы файла: • **MD5**. • **SHA256**. Этот раскрывающийся список отображается, если в раскрывающемся списке **Укажите файл, процессы которого требуется завершить** вы выбрали значение **По пути к директории и контрольной сумме**.
Контрольная сумма файла	Поле ввода контрольной суммы файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, процессы которого требуется завершить** вы выбрали значение **По пути к директории и контрольной сумме**, а в раскрывающемся списке **Тип контрольной суммы** значение **MD5**.
Путь к директории	Поле ввода пути к директории файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, процессы которого требуется завершить** вы выбрали значение **По пути к директории и контрольной сумме**.
Идентификатор процесса	Поле ввода идентификатора процесса (PID). Это поле отображается, если в раскрывающемся списке **Укажите файл, процессы которого требуется завершить** вы выбрали значение **По PID**.

Результат выполнения задачи можно посмотреть в разделе **Активы (Устройства)** → **Задачи** → <название задачи> на закладке **Результаты** в столбце **Описание**.

Получение файла с устройства

Вы можете получать файлы с устройств пользователей с помощью задачи *Получение файла с устройства*.

Например, вы можете получить файл журнала событий, который создало стороннее приложение.

Вы можете создавать и запускать задачу *Получение файла с устройства*, а также изменять ее параметры в Web Console.

Вы не можете создавать, запускать или настраивать задачу *Получение файла с устройства* с помощью командной строки. Просмотр задачи *Получение файла с устройства*, созданной из Web Console, недоступен по команде `kesl-control --get-task-list` в командной строке.

Таблица **Получение файла** на закладке **Параметры приложения** содержит следующие столбцы:

- **Путь к директории**.

  Путь к директории файла, находящегося на устройстве.

- **Тип проверки контрольной суммы**.

  Тип проверки контрольной суммы файла, находящегося на устройстве.

С помощью кнопок над таблицей вы можете добавлять, изменять или удалять данные файлов, находящихся на устройстве. Задача *Получение файла с устройства* выполняется для файлов, указанных в таблице **Получение файла**.

При нажатии на кнопку **Добавить** открывается окно **Получение файла**, в котором вы можете настроить параметры задачи *Получение файла с устройства*.

Параметр	Описание
Укажите файл, который требуется получить	В раскрывающемся списке вы можете выбрать способ указания пути к файлу: • **По пути к директории и контрольной сумме**. • **По полному пути**.
Полный путь к файлу	Поле ввода полного пути к файлу. Это поле отображается, если в раскрывающемся списке **Укажите файл, который требуется получить** вы выбрали значение **По полному пути**.
Тип контрольной суммы	В раскрывающемся списке вы можете выбрать тип контрольной суммы файла: • **MD5**. • **SHA256**. Этот раскрывающийся список отображается, если в раскрывающемся списке **Укажите файл, который требуется получить** вы выбрали значение **По пути к директории и контрольной сумме**.
Контрольная сумма файла	Поле ввода контрольной суммы файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, который требуется получить** вы выбрали значение **По пути к директории и контрольной сумме**.
Путь к директории с файлом	Поле ввода пути к директории файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, который требуется получить** вы выбрали значение **По пути к директории и контрольной сумме**.

В результате выполнения задачи *Получение файла с устройства* копия файла сохраняется в резервном хранилище устройства. Вы можете загрузить эту копию из резервного хранилища через Web Console на то устройство, с которого вы инициировали загрузку.

Размер файла не должен превышать 100 МБ.

Оригинал файла на устройстве пользователя остается в исходной директории.

Все файлы, полученные через задачу *Получение файла с устройства*, будут иметь статус *Заражен* в резервном хранилище Kaspersky Security Center независимо от результатов проверки файла.

Результат выполнения задачи можно посмотреть в разделе **Активы (Устройства)** → **Задачи** → <название задачи> на закладке **Результаты** в столбце **Описание**.

Удаление файла с устройства

Вы можете удалять файлы с устройства с помощью задачи *Удаление файла с устройства*. Это может быть необходимо, например, при реагировании на угрозы.

Критически важные системные объекты (англ. System Critical Object, SCO) удалить невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Endpoint Security.

Вы можете создавать и запускать задачу *Удаление файла с устройства*, а также изменять ее параметры в Web Console.

Вы не можете создавать, запускать или настраивать задачу *Удаление файла с устройства* с помощью командной строки. Просмотр задачи *Удаление файла с устройства*, созданной из Web Console, недоступен по команде `kesl-control --get-task-list` в командной строке.

Параметры задачи Удаление файла с устройства

Параметр	Описание
Укажите файл, который нужно удалить	В раскрывающемся списке вы можете выбрать способ указания пути к удаляемому файлу: • **По пути и контрольной сумме**. • **По полному пути**.
Полный путь к файлу	Поле ввода полного пути к удаляемому файлу. Это поле отображается, если в раскрывающемся списке **Укажите файл, который нужно удалить** вы выбрали значение **По полному пути**.
Тип контрольной суммы	В раскрывающемся списке вы можете выбрать тип контрольной суммы удаляемого файла: • **MD5**. • **SHA256**. Этот раскрывающийся список отображается, если в раскрывающемся списке **Укажите файл, который нужно удалить** вы выбрали значение **По пути и контрольной сумме**.
Контрольная сумма файла	Поле ввода контрольной суммы удаляемого файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, который нужно удалить** вы выбрали значение **По пути и контрольной сумме**.
Путь к директории	Поле ввода пути к директории удаляемого файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, который нужно удалить** вы выбрали значение **По пути и контрольной сумме**.
Включать вложенные директории	Флажок включает или выключает вложенные директории.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки устройства. После перезагрузки устройства убедитесь, что файл удален.

Задача *Удаление файла с устройства* может быть завершена с ошибкой *Доступ запрещен*, если вы пытаетесь удалить запущенный исполняемый файл. Создайте и выполните задачу *Завершение процесса* для этого файла, а затем повторите попытку.

Результат выполнения задачи можно посмотреть в разделе **Активы (Устройства)** → **Задачи** → <название задачи> на закладке **Результаты** в столбце **Описание**.

Интеграция с Kaspersky Managed Detection and Response

Решение Kaspersky Managed Detection and Response обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию. Интеграцию с решением Kaspersky Managed Detection and Response обеспечивает компонент приложения Kaspersky Endpoint Security – Managed Detection and Response (далее также MDR).

При взаимодействии с Kaspersky Managed Detection and Response приложение Kaspersky Endpoint Security может выполнять следующие функции:

- Отправка данных телеметрии в Kaspersky Managed Detection and Response для обнаружения угроз.
- Выполнение команд от Kaspersky Managed Detection and Response, направленных на обеспечение функций безопасности.

Для настройки интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response требуется выполнить следующие действия:

- Убедиться, что включены компоненты Защита от файловых угроз и Анализ поведения. Если эти компоненты выключены, устройство в Kaspersky Managed Detection and Response будет иметь красный статус.

  Рекомендуется также включить компоненты Защита от веб-угроз и Защита от сетевых угроз. Если эти компоненты выключены, устройство в Kaspersky Managed Detection and Response будет иметь желтый статус.

  Подробнее о статусах устройств см. в справке решения Kaspersky Managed Detection and Response.

- Включить использование Kaspersky Security Network в расширенном режиме.

  Вы можете включить использование Kaspersky Security Network в командной строке, в Web Console или в Консоли администрирования.

- Настроить Kaspersky Private Security Network. Использование KPSN требуется для отправки телеметрии.

  Вы можете настроить Kaspersky Private Security Network только в Web Console или в Консоли администрирования.

  > Настройка KPSN с помощью команд приложения Kaspersky Endpoint Security недоступна.

- Включить компонент Managed Detection and Response и загрузить конфигурационный файл BLOB, который находится в ZIP-архиве конфигурационного файла MDR.

  Вы можете включить компонент Managed Detection and Response и загрузить конфигурационный файл BLOB в командной строке, в Web Console или в Консоли администрирования.

Настройка KPSN для интеграции с Kaspersky Managed Detection and Response

Вы можете настроить использование Kaspersky Private Security Network для интеграции с Kaspersky Managed Detection and Response только в Web Console или в Консоли администрирования.

Для настройки KPSN требуется загрузить на Сервер администрирования Kaspersky Security Center конфигурационный файл Kaspersky Security Network (файл с расширением pkcs7), который находится в ZIP-архиве конфигурационного файла MDR.

Загружая конфигурационный файл Kaspersky Security Network, вы соглашаетесь автоматически передавать данные с устройства с установленным приложением Kaspersky Endpoint Security в "Лабораторию Касперского" для обработки. Не загружайте конфигурационный файл, если вы не согласны на обработку передаваемых данных. Подробное описание передаваемых данных см. в документации Kaspersky Managed Detection and Response.

Чтобы настроить KPSN для интеграции с Kaspersky Managed Detection and Response в Web Console:

1. В главном окне Web Console откройте окно свойств Сервера администрирования.
2. В списке слева выберите раздел **Параметры прокси-сервера KSN**.
3. Включите переключатель **Включить прокси-сервер KSN на Сервере администрирования**, чтобы включить службу прокси-сервера KSN.
4. Включите переключатель **Использовать Kaspersky Private Security Network**.
5. В открывшемся окне с предупреждением об особенностях использования прокси-сервера KSN на точках распространения с установленной старой версией Агента администрирования нажмите на кнопку **OK**.
6. Нажмите на кнопку **Файл с параметрами прокси-сервера KSN**.
7. Выберите конфигурационный файл Kaspersky Security Network (файл с расширением pkcs7) и нажмите на кнопку **Открыть**.
8. Нажмите на кнопку **Сохранить**.

Чтобы настроить KPSN для интеграции с Kaspersky Managed Detection and Response в Консоли администрирования:

1. В дереве Консоли администрирования откройте окно свойств Сервера администрирования.
2. Выберите раздел **Прокси-сервер KSN → Параметры прокси-сервера KSN**.
3. Установите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы включить службу прокси-сервера KSN.
4. Установите флажок **Настроить Локальный KSN**.
5. В открывшемся окне с предупреждением об особенностях использования прокси-сервера KSN на точках распространения с установленной старой версией Агента администрирования нажмите на кнопку **OK**.
6. Нажмите на кнопку **Файл с параметрами прокси-сервера KSN**.
7. Выберите конфигурационный файл Kaspersky Security Network (файл с расширением pkcs7) и нажмите на кнопку **Открыть**.
8. Нажмите на кнопку **Применить**.

Настройка интеграции с Kaspersky Managed Detection and Response в Web Console

В Web Console вы можете включать и выключать интеграцию приложения Kaspersky Endpoint Security с Kaspersky Managed Detection and Response и загружать конфигурационный файл BLOB в свойствах политики (**Параметры приложения** → **Detection and Response** → **Managed Detection and Response**).

Параметры интеграции с MDR

Параметр	Описание
Managed Detection and Response включен / выключен	Переключатель включает или выключает компонент Managed Detection and Response, необходимый для интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response. По умолчанию переключатель выключен.
Загрузить	По нажатию на кнопку открывается стандартное окно, в котором вы можете выбрать конфигурационный файл BLOB.

Конфигурационный файл BLOB находится в ZIP-архиве, который входит в поставку решения Kaspersky Managed Detection and Response.

Загружая конфигурационный файл BLOB, вы соглашаетесь автоматически передавать данные с устройства с установленным приложением Kaspersky Endpoint Security в "Лабораторию Касперского" для обработки. Не загружайте конфигурационный файл, если вы не согласны на обработку передаваемых данных. Подробное описание передаваемых данных см. в справке Kaspersky Managed Detection and Response.

Настройка интеграции с Kaspersky Managed Detection and Response в Консоли администрирования

В Консоли администрирования вы можете включать и выключать интеграцию приложения Kaspersky Endpoint Security с Kaspersky Managed Detection and Response и загружать конфигурационный файл BLOB в свойствах политики (**Detection and Response** → **Managed Detection and Response**).

Параметры интеграции с MDR

Параметр	Описание
Включить Managed Detection and Response	Флажок включает компонент Managed Detection and Response, необходимый для интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response. По умолчанию флажок снят.
Загрузить	По нажатию на кнопку открывается стандартное окно Microsoft Windows, в котором вы можете выбрать конфигурационный файл BLOB.

Конфигурационный файл BLOB находится в ZIP-архиве, который входит в поставку решения Kaspersky Managed Detection and Response.

Загружая конфигурационный файл BLOB, вы соглашаетесь автоматически передавать данные с устройства с установленным приложением Kaspersky Endpoint Security в "Лабораторию Касперского" для обработки. Не загружайте конфигурационный файл, если вы не согласны на обработку передаваемых данных. Подробное описание передаваемых данных см. в справке Kaspersky Managed Detection and Response.

Настройка интеграции с Kaspersky Managed Detection and Response в командной строке

В командной строке вы можете:

- включать и выключать компонент Managed Detection and Response;
- загружать и удалять конфигурационный файл BLOB, необходимый для интеграции;
- изменять время запуска служебной задачи *Mdr_Autostart_Scan*, которая создается автоматически после интеграции Kaspersky Endpoint Security с Managed Detection and Response.

Настройку интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response рекомендуется выполнять в Консоли администрирования или в Web Console.

Вы можете включать и выключать компонент Managed Detection and Response с помощью параметра `UseMDR` из общих параметров приложения. Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `UseMDR` может принимать следующие значения:

- `Yes` – включить компонент Managed Detection and Response.
- `No` – выключить компонент Managed Detection and Response.

Вы можете загружать и удалять конфигурационный файл BLOB с помощью команд управления лицензионными ключами.

Чтобы загрузить конфигурационный файл BLOB, выполните следующую команду:

```
kesl-control --load-mdr-blob <путь к конфигурационному файлу MDR BLOB>
```

Чтобы удалить конфигурационный файл BLOB, выполните следующую команду:

```
kesl-control --remove-mdr-blob
```

После включения интеграции в приложении создается служебная задача *Mdr_Autostart_Scan* с режимом запуска один раз в сутки. Если требуется, вы можете настроить время запуска этой задачи. Другие параметры задачи и другие параметры ее расписания недоступны для изменения.

Настройка параметров использования приложения в режиме Легкого агента

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Для работы приложения Kaspersky Endpoint Security в режиме Легкого агента требуется постоянное взаимодействие между Легким агентом и Сервером защиты, установленным на SVM. Если соединение с Сервером защиты отсутствует, Легкий агент не может передавать фрагменты файлов на проверку Серверу защиты, проверка не выполняется.

Для взаимодействия с Сервером защиты Легкий агент устанавливает и поддерживает подключение к SVM, на которой установлен этот Сервер защиты.

Вы можете настраивать параметры подключения Легкого агента к SVM в Web Console или в Консоли администрирования. В командной строке настройка параметров недоступна, вы можете только просматривать информацию об использовании приложения в режиме Легкого агента.

Вы можете настраивать следующие параметры подключения Легкого агента к SVM:

- Способ обнаружения SVM. Вы можете выбрать способ, который будут использовать Легкие агенты для обнаружения доступных для подключения SVM. Легкий агент может обнаруживать SVM, работающие в сети, одним из следующих способов:
  - С помощью Сервера интеграции. SVM передают информацию о себе на Сервер интеграции. Сервер интеграции формирует список доступных для подключения SVM и предоставляет его Легким агентам.

    Для использования этого способа обнаружения SVM требуется подключение SVM и Легких агентов к Серверу интеграции.
  - С использованием списка адресов SVM. Вы можете задать список адресов SVM, к которым могут подключаться Легкие агенты.
- Алгоритм выбора SVM для подключения. После получения информации о доступных SVM Легкий агент выбирает оптимальную для подключения SVM в соответствии с алгоритмом выбора SVM. Вы можете указать, какой алгоритм должны использовать Легкие агенты при выборе SVM для подключения.
- Теги для подключения. Вы можете регулировать подключение Легких агентов к SVM с помощью тегов для подключения. Если вы используете теги для подключения, Легкий агент может подключаться только к тем SVM, на которых настроено использование этого тега для подключения.
- Защита соединения между Легким агентом и Сервером защиты. Вы можете защищать соединение между Легкими агентами и Серверами защиты с помощью шифрования.

Подробнее о параметрах подключения Легкого агента к SVM см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Настройка параметров Легкого агента в Web Console

В Web Console вы можете настраивать параметры подключения Легкого агента к SVM в свойствах политики (**Параметры приложения** → **Режим Легкого агента**).

Параметры обнаружения SVM

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

В этом окне вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM.

Параметры обнаружения SVM

Параметр	Описание
Использовать Сервер интеграции	Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них. Если вы хотите использовать Сервер интеграции, вам нужно настроить параметры подключения Легких агентов к Серверу интеграции.
Использовать список адресов SVM, заданный вручную	Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.
Список адресов SVM	Список IP-адресов в формате IPv4 или полных доменных имен (FQDN) SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением политики. По нажатию на кнопку **Добавить** открывается окно, в котором вы можете указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки. Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения. Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**. Список адресов SVM отображается, если выбран вариант **Использовать список адресов SVM, заданный вручную**.

Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

Параметры подключения к Серверу интеграции

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Подключение к Серверу интеграции требуется, если вы хотите, чтобы Легкие агенты получали информацию об SVM через Сервер интеграции, или если вы хотите защищать соединение между Сервером защиты и Легким агентом.

В этом окне отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. По нажатию на кнопку **Изменить** открывается окно **Подключение к Серверу интеграции**, в котором вы можете настроить подключение к Серверу интеграции.

Окно Подключение к Серверу интеграции

В этом окне вы можете указать или изменить параметры подключения Легких агентов к Серверу интеграции.

Параметры подключения к Серверу интеграции

Параметр	Описание
Адрес	IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции. Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.
Порт	Порт для подключения к Серверу интеграции. По умолчанию указан порт 7271.
Проверить	По нажатию на кнопку веб-плагин проверяет SSL-сертификат, полученный от Сервера интеграции. Кнопка доступна после ввода адреса и порта для подключения к Серверу интеграции. Если сертификат содержит ошибку или не является доверенным, в окне **Подключение к Серверу интеграции** отображается сообщение об этом.
Посмотреть полученный сертификат	По нажатию на строку вы можете посмотреть информацию о сертификате, полученном от Сервера интеграции.
Игнорировать	Выберите этот вариант, чтобы сохранить полученный сертификат и продолжить подключение к Серверу интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.
Отменить	Выберите этот вариант, чтобы прервать подключение к Серверу интеграции.
Пароль	Пароль учетной записи администратора Сервера интеграции (пароль учетной записи

	admin). Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев.
Проверить	По нажатию на кнопку веб-плагин выполняет подключение к Серверу интеграции. После подключения к Серверу интеграции с правами администратора в политику автоматически передается пароль учетной записи agent, которая используется для подключения Легких агентов к Серверу интеграции. Пароль хранится в зашифрованном виде.

Тег для подключения к SVM

В этом окне вы можете включить использование тегов Легким агентом и назначить тег, который Легкий агент будет использовать для подключения.

Убедитесь, что использование тегов для подключения также настроено в параметрах Сервера защиты: См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент. Легкие агенты, которым назначен тег, могут подключаться только к SVM, для которых разрешено подключение Легких агентов с этим тегом.

Параметры использования тегов для подключения

Параметр	Описание
Использовать теги для подключения Легких агентов	Флажок включает или выключает использование Легким агентом тегов для подключения к SVM.
Тег	Тег, который назначается Легким агентам. В качестве тега вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа `;`. Поле доступно, если установлен флажок **Использовать теги для подключения Легких агентов**.

Алгоритм выбора SVM

В этом окне вы можете указать, какой алгоритм выбора SVM должны использовать Легкие агенты для Linux, и настроить параметры применения расширенного алгоритма выбора SVM.

Алгоритм выбора SVM

Параметр	Описание
Использовать стандартный алгоритм выбора SVM	Если выбран этот вариант, после установки и запуска на виртуальной машине Легкий агент выбирает для подключения SVM, которая является локальной для Легкого агента. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент.

	Если нет доступных для подключения локальных SVM, Легкий агент выбирает SVM, к которой подключено наименьшее количество Легких агентов, независимо от расположения SVM в виртуальной инфраструктуре. Этот вариант выбран по умолчанию.
Использовать расширенный алгоритм выбора SVM	Если выбран этот вариант, вы можете указать с помощью ползунка **Расположение SVM**, как расположение SVM в виртуальной инфраструктуре будет учитываться при определении локальности SVM относительно Легкого агента. Легкий агент сможет подключаться только к тем SVM, которые являются локальными. Также вы можете указать, что расположение SVM в виртуальной инфраструктуре не должно учитываться при выборе SVM для подключения. При выборе SVM Легкие агенты учитывают количество Легких агентов, подключенных к этой SVM, чтобы обеспечить равномерное распределение Легких агентов между доступными для подключения SVM.
Расположение SVM	Позволяет указать тип расположения SVM в виртуальной инфраструктуре, который учитывается при выборе SVM для подключения: • **Гипервизор**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры): ◦ SVM развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис (Скала-Р), HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer). ◦ SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС). Если на том же гипервизоре или в той же Группе серверов, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM. • **Кластер**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры): ◦ SVM развернута в том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис (Скала-Р), HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer). ◦ SVM развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС). Если в том же кластере гипервизоров или в рамках того же проекта OpenStack, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM. • **Дата-центр**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры): ◦ SVM развернута в том же дата-центре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на

	платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис (Скала-Р), HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer). ○ SVM расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС). Если в том же дата-центре или в той же Зоне доступности, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM. • **Не учитывать расположение SVM**. Легкий агент не учитывает при выборе SVM ее расположение. По умолчанию выбрано значение **Гипервизор**. Параметр доступен, если выбран вариант **Использовать расширенный алгоритм выбора SVM**.

Если для Легкого агента применяется расширенный алгоритм выбора SVM и в качестве способа обнаружения SVM выбран список адресов SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. Требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

Защита соединения

В этом окне вы можете включить шифрование канала передачи данных между Легким агентом и Сервером защиты.

Убедитесь что шифрование канала передачи данных между Легким агентом и Сервером защиты включено в параметрах Сервера защиты на SVM. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Параметры защиты соединения

Параметр	Описание
Шифровать канал передачи данных между Легким агентом и Сервером защиты	Защитить соединение между Легкими агентами и Сервером защиты с помощью шифрования. Если флажок установлен, между Легким агентом, находящимся под управлением политики, и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается защищенное соединение. Легкий агент, для которого включена защита соединения, может подключиться только к SVM, на которой также включена защита соединения или разрешено незащищенное соединение с Сервером защиты. Если флажок снят, между Легким агентом и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается незащищенное соединение. По умолчанию флажок снят.

Настройка параметров Легкого агента в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры подключения Легкого агента к SVM в свойствах политики (**Режим Легкого агента**).

Подключение к Серверу интеграции

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Подключение к Серверу интеграции требуется, если вы хотите, чтобы Легкие агенты получали информацию об SVM через Сервер интеграции, или если вы хотите защищать соединение между Сервером защиты и Легким агентом.

В этом окне отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. По нажатию на кнопку **Изменить** открывается окно **Подключение к Серверу интеграции**, в котором вы можете настроить подключение к Серверу интеграции.

Окно Подключение к Серверу интеграции

В этом окне вы можете указать или изменить параметры подключения Легких агентов к Серверу интеграции.

Параметры подключения к Серверу интеграции

Параметр	Описание
Адрес	IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции. Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен, в поле по умолчанию указано доменное имя этого устройства. Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или Сервер интеграции установлен на другом устройстве, поле требуется заполнить вручную. Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.
Порт	Порт для подключения к Серверу интеграции. По умолчанию указан порт 7271.

Окно Проверка сертификата Сервера интеграции

Это окно отображается, если SSL-сертификат, полученный от Сервера интеграции, содержит ошибку или не является доверенным.

С помощью ссылки в окне вы можете посмотреть информацию о полученном сертификате.

При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

Окно Аутентификация на Сервере интеграции

Это окно отображается, если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов.

Укажите пароль администратора Сервера интеграции (пароль учетной записи `admin`) и нажмите на кнопку **ОК**.

Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев.

После подключения к Серверу интеграции с правами администратора в политику автоматически передается пароль учетной записи `agent`, которая используется для подключения Легких агентов к Серверу интеграции.

Параметры обнаружения SVM

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

В этом окне вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM.

Параметры обнаружения SVM

Параметр	Описание
Использовать Сервер интеграции	Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них. Если вы хотите использовать Сервер интеграции, вам нужно настроить параметры подключения Легких агентов к Серверу интеграции.
Использовать список адресов SVM, заданный вручную	Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.
Список SVM	Список IP-адресов в формате IPv4 или полных доменных имен (FQDN) SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением

политики.

По нажатию на кнопку **Добавить** открывается окно, в котором вы можете указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки.

Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения.

Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**.

Список адресов SVM отображается, если выбран вариант **Использовать список адресов SVM, заданный вручную**.

Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

Тег для подключения к SVM

В этом окне вы можете включить использование тегов Легким агентом и назначить тег, который Легкий агент будет использовать для подключения.

Убедитесь, что использование тегов для подключения также настроено в параметрах Сервера защиты: см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент. Легкие агенты, которым назначен тег, могут подключаться только к SVM, для которых разрешено подключение Легких агентов с этим тегом.

Параметры использования тегов для подключения

Параметр	Описание
Использовать теги для подключения Легких агентов	Флажок включает или выключает использование Легким агентом тегов для подключения к SVM.
Тег	Тег, который назначается Легким агентам. В качестве тега вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа **;**. Поле доступно, если установлен флажок **Использовать теги для подключения Легких агентов**.

Алгоритм выбора SVM

В этом окне вы можете указать, какой алгоритм выбора SVM должны использовать Легкие агенты для Linux, и настроить параметры применения расширенного алгоритма выбора SVM.

Алгоритм выбора SVM

Параметр	Описание
Использовать стандартный алгоритм выбора SVM	Если выбран этот вариант, после установки и запуска на виртуальной машине Легкий агент выбирает для подключения SVM, которая является локальной для Легкого агента. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент. Если нет доступных для подключения локальных SVM, Легкий агент выбирает SVM, к которой подключено наименьшее количество Легких агентов, независимо от расположения SVM в виртуальной инфраструктуре. Этот вариант выбран по умолчанию.
Использовать расширенный алгоритм выбора SVM	Если выбран этот вариант, вы можете указать с помощью ползунка **Расположение SVM**, как расположение SVM в виртуальной инфраструктуре будет учитываться при определении локальности SVM относительно Легкого агента. Легкий агент сможет подключаться только к тем SVM, которые являются локальными. Также вы можете указать, что расположение SVM в виртуальной инфраструктуре не должно учитываться при выборе SVM для подключения. При выборе SVM Легкие агенты учитывают количество Легких агентов, подключенных к этой SVM, чтобы обеспечить равномерное распределение Легких агентов между доступными для подключения SVM.
Расположение SVM	Позволяет указать тип расположения SVM в виртуальной инфраструктуре, который учитывается при выборе SVM для подключения: • **Гипервизор**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры): ◦ SVM развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис (Скала-Р), HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer). ◦ SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС). Если на том же гипервизоре или в той же Группе серверов, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM. • **Кластер**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры): ◦ SVM развернута в том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис (Скала-Р), HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer). ◦ SVM развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС).

	Если в том же кластере гипервизоров или в рамках того же проекта OpenStack, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM. • **Дата-центр**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры): ◦ SVM развернута в том же дата-центре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис (Скала-Р), HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer). ◦ SVM расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС). Если в том же дата-центре или в той же Зоне доступности, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM. • **Не учитывать расположение SVM**. Легкий агент не учитывает при выборе SVM ее расположение. По умолчанию выбрано значение **Гипервизор**. Параметр доступен, если выбран вариант **Использовать расширенный алгоритм выбора SVM**.

Если для Легкого агента применяется расширенный алгоритм выбора SVM и в качестве способа обнаружения SVM выбран список адресов SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. Требуется установить для параметра **Расположение SVM** значение **Не учитывать расположение SVM**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

Защита соединения

В этом окне вы можете включить шифрование канала передачи данных между Легким агентом и Сервером защиты.

Убедитесь, что шифрование канала передачи данных между Легким агентом и Сервером защиты включено в параметрах Сервера защиты на SVM. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Параметры защиты соединения

Параметр	Описание
Шифровать канал передачи данных	Защитить соединение между Легкими агентами и Сервером защиты с помощью шифрования.

между Легким агентом и Сервером защиты	Если флажок установлен, между Легким агентом, находящимся под управлением политики, и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается защищенное соединение. Легкий агент, для которого включена защита соединения, может подключиться только к SVM, на которой также включена защита соединения или разрешено незащищенное соединение с Сервером защиты. Если флажок снят, между Легким агентом и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается незащищенное соединение. По умолчанию флажок снят.

Просмотр в командной строке информации об использовании приложения в режиме Легкого агента

В командной строке вы можете посмотреть следующую информацию об использовании приложения в режиме Легкого агента для защиты виртуальных сред:

- о параметрах использования приложения в режиме Легкого агента;
- о подключении Легкого агента к Серверу интеграции;
- о подключении Легкого агента к SVM.

Чтобы посмотреть информацию о параметрах использования приложения в режиме Легкого агента, выполните следующую команду:

```
kesl-control [-V] --ksvla-info
```

В результате выполнения команды в консоль выводится следующая информация:

- Режим Легкого агента для защиты виртуальных сред: включен/выключен.

  Если режим Легкого агента включен, приложение используется в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент. Если режим Легкого агента выключен, приложение используется в стандартном режиме.

- Режим защиты инфраструктуры VDI: включен/выключен.

  Режим защиты инфраструктуры VDI позволяет оптимизировать работу приложения Kaspersky Endpoint Security на временных виртуальных машинах. Если режим защиты инфраструктуры VDI включен, то обновления, требующие перезагрузки защищенной виртуальной машины, не устанавливаются на временных виртуальных машинах. При получении обновлений, требующих перезагрузки, Легкий агент, установленный на временной виртуальной машине, отправляет в Kaspersky Security Center сообщение о необходимости обновления шаблона защищенных виртуальных машин.

- Тип защищенной виртуальной машины: временная или постоянная.
- Роль защищенной виртуальной машины в виртуальной инфраструктуре: сервер или рабочая станция.
- Идентификатор (UUID) защищенной виртуальной машины.

Чтобы посмотреть информацию о подключении Легкого агента к Серверу интеграции, выполните следующую команду:

```
kesl-control [-V] --viis-info
```

В результате выполнения команды в консоль выводится следующая информация:

- Адрес и порт Сервера интеграции, к которому подключается Легкий агент.
- Статус подключения к Серверу интеграции.
- Дата и время последнего соединения Легкого агента с Сервером интеграции.

Чтобы посмотреть информацию о подключении Легкого агента к SVM, выполните следующую команду:

```
kesl-control [-V] --svm-info
```

В результате выполнения команды в консоль выводится следующая информация:

- Адрес SVM, к которой подключен Легкий агент, и расположение SVM в виртуальной инфраструктуре относительно Легкого агента: локальная или не локальная.
- Способ обнаружения SVM Легким агентом: с помощью Сервера интеграции или с использованием списка адресов SVM, заданных вручную.
- Список адресов SVM, если в качестве способа обнаружения SVM выбрано использование списка адресов SVM.
- Тег для подключения Легкого агента к SVM.
- Алгоритм выбора SVM: стандартный или расширенный. Если применяется расширенный алгоритм выбора SVM, также выводится тип расположения SVM в виртуальной инфраструктуре.
- Наличие защиты соединения между Легким агентом и Сервером защиты.

Информацию о параметрах подключения Легких агентов к Серверу интеграции и SVM см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Просмотр событий и отчетов

В процессе работы приложения возникают различного рода *события*. Они могут иметь информационный характер или нести важную информацию. Например, с помощью события приложение может уведомлять об успешно выполненном обновлении баз приложения или может фиксировать ошибку в работе компонента, которую требуется устранить.

Kaspersky Endpoint Security позволяет вносить информацию о событиях, возникающих в работе приложения, в следующие журналы:

- Журнал событий приложения. По умолчанию приложение сохраняет информацию о событиях в базе данных /var/opt/kaspersky/kesl/private/storage/events.db. Вы можете настраивать параметры журнала событий приложения в командной строке.

- Журнал операционной системы (syslog). По умолчанию журнал операционной системы не используется. Вы можете включить запись событий в этот журнал.

Для доступа к журналу событий приложения и к журналу операционной системы требуются root-права.

Если управление приложением Kaspersky Endpoint Security осуществляется с помощью Kaspersky Security Center, данные о событиях могут передаваться на Сервер администрирования Kaspersky Security Center. Для некоторых событий действуют правила агрегирования. В случае, если за короткий промежуток времени в процессе работы приложения создается много событий одного типа, приложение переключается в режим агрегирования событий и отправляет в Kaspersky Security Center одно агрегированное событие с описанием параметров этих событий. Для разных событий могут использоваться разные правила агрегирования. Подробнее о событиях см. в справке Kaspersky Security Center.

Вы можете получать информацию о событиях приложения следующими способами:

- В Консоли администрирования и в Web Console.

- В командной строке.

- Если вы используете графический пользовательский интерфейс Kaspersky Endpoint Security – во всплывающих окнах приложения.

Некоторые события могут содержать пути к файлам. При выводе путь к файлу рассматривается как строка в кодировке UTF-8. В случае если какой-то из байт в пути не соответствует правилам кодирования UTF-8, то он заменяется на символ `?`. Также на символ `?` заменяется последовательность из четырех байт, кодирующая код символов, выходящих за пределы диапазона Unicode (больше 0x10FFFF). Специальные символы экранируются (заменяются) определенным образом.

Правила экранирования символов в путях к файлам в событиях при выводе по команде `kesl-control -E --query`:

- символы '\a', '\b', '\t', '\n', '\v', '\f', '\r' заменяются двумя символами следующим образом:

  '\a' -> "\\a"

  '\b' -> "\\b"

  '\t' -> "\\t"

  '\n' -> "\\n"

  '\v' -> "\\v"

  '\f' -> "\\f"

  '\r' -> "\\r"

- все прочие специальные символы выводятся без изменений.

Правила экранирования символов в путях к файлам в событиях при выводе по команде `kesl-control -E --query --json`:

- символы '\b', '\f', '\n', '\r', '\t', '"', '\\' экранируются, в соответствии с форматом JSON, следующим образом:

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\""

  '\\' -> "\\\\"

- все прочие специальные символы экранируются в соответствии с общими правилами экранирования специальных символов для формата JSON ('\a' -> '\u0007').

Правила экранирования символов в путях к файлам в событиях при передаче в syslog:

- символы '\b', '\f', '\n', '\r', '\t', '"', '\\' экранируются, в соответствии с форматом JSON, следующим образом:

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\""

  '\\' -> "\\\\"

- все прочие специальные символы экранируются в соответствии с общими правилами экранирования специальных символов для формата JSON ('\a' -> '\u0007').

Первый обратный слеш в последовательности при описании правил – это символ экранирования.

Примеры:
`'\a'` – это один символ (управляющий);

`'\\a'` – это два символа (обратный слеш + символ `a`);

`'\\'` – это один символ (обратный слеш), `'\\\\'` – это два символа (обратный слеш + обратный слеш).

На основе событий, происходящих во время работы приложения, можно формировать различные *отчеты*. В отчеты записываются информация о работе каждого компонента приложения Kaspersky Endpoint Security и результаты выполнения каждой задачи и работы всего приложения в целом.

Вы можете просматривать отчеты следующими способами:

- В Консоли администрирования и в Web Console доступны отчеты Kaspersky Security Center. С их помощью вы можете, например, получить сведения о зараженных файлах, использовании ключей и баз приложения. Подробную информацию о работе с отчетами Kaspersky Security Center см. в справке Kaspersky Security Center.

- В графическом пользовательском интерфейсе Kaspersky Endpoint Security доступны отчеты приложения.

В событиях и отчетах могут содержаться следующие персональные данные:

- имена и идентификаторы пользователей в операционной системе;
- пути к файлам пользователя;
- IP-адреса удаленных устройств, проверяемых компонентом Защита от шифрования;
- IP-адреса отправителей и получателей сетевых пакетов, проверяемых компонентом Управление сетевым экраном;
- веб-адреса источников обновлений;
- значения общих параметров приложения;
- имена и параметры задач командной строки;
- обнаруженные вредоносные, фишинговые, рекламные веб-адреса и веб-адреса, содержащие легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным;
- названия контейнеров и образов;
- пути к контейнерам и образам;
- названия и идентификаторы устройств;
- веб-адреса репозиториев;
- имена файлов, пути к файлам и хеш-суммы исполняемых файлов приложений;
- названия категорий приложений.

Настройка записи событий в журнал операционной системы

По умолчанию события, возникающие в работе приложения Kaspersky Endpoint Security, не записываются в журнал операционной системы. Вы можете включить запись событий в этот журнал с помощью Web Console, Консоли администрирования или командной строки.

В Kaspersky Security Center вы также можете выбрать события, которые будут записываться в журнал операционной системы.

Настройка в Web Console

В Web Console вы можете настраивать запись событий в журнал операционной системы в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры приложения**).

По ссылке **Настроить уведомления** в блоке **Уведомления** открывается окно **Уведомления**. В этом окне вы можете с помощью флажков выбрать события, которые приложение будет записывать в журнал операционной системы.

Вы можете выбирать отдельные типы событий или все типы событий определенного уровня важности.

По умолчанию все флажки сняты.

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать запись событий в журнал операционной системы в свойствах политики (**Общие параметры** → **Параметры приложения**).

По ссылке **Настроить** в блоке **Уведомления** открывается окно **Параметры уведомлений**. В этом окне вы можете с помощью флажков выбрать события, которые приложение будет записывать в журнал операционной системы.

Вы можете выбирать отдельные типы событий или все типы событий определенного уровня важности.

По умолчанию все флажки сняты.

Настройка в командной строке

В командной строке вы можете включать и выключать запись событий в журнал операционной системы с помощью параметра `UseSyslog` из общих параметров приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `UseSyslog` может принимать следующие значения:

- `Yes` – включить запись событий в syslog.
- `No` (значение по умолчанию) – выключить запись событий в syslog.

Настройка параметров журнала событий приложения

По умолчанию информация о событиях сохраняется в журнале событий приложения, расположенном на устройстве. В командной строке вы можете настраивать следующие параметры журнала событий приложения с помощью общих параметров приложения:

- Изменять путь к базе данных журнала событий приложения с помощью параметра `EventsStoragePath`. Значение по умолчанию: /var/opt/kaspersky/kesl/private/storage/events.db.
- Задавать максимальное количество событий, которые будет хранить приложение с помощью параметра `MaxEventsNumber`. Значение по умолчанию: 500000. При превышении заданного количества событий приложение удаляет наиболее давние события.

Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Просмотр событий в Kaspersky Security Center

Список всех событий в работе приложения Kaspersky Endpoint Security отображается в Web Console и в Консоли администрирования.

Вы можете настроить уведомления о событиях. *Уведомление* – это сообщение с информацией о событии, которое произошло защищенном устройстве. С помощью уведомлений вы можете своевременно получать информацию о событиях в работе приложения. Вы можете настроить выполнение скрипта при получении события из приложения или получение уведомлений о событиях по электронной почте.

Подробнее о работе с событиями в Kaspersky Security Center см. в справке Kaspersky Security Center.

Просмотр событий в командной строке

С помощью командной строки вы можете просматривать:

- текущие события приложения;
- события из журнала событий приложения.

Вывод текущих событий

Вы можете выводить в консоль информацию обо всех текущих событиях приложения или о текущих событиях, связанных с запуском или остановкой указанной задачи. С помощью фильтра вы так же можете выводить определенные текущие события, например, события указанного типа.

Чтобы вывести в консоль информацию обо всех текущих событиях приложения, выполните следующую команду:

```
kesl-control -W
```

Команда возвращает название события и дополнительную информацию о событии.

Чтобы вывести в консоль информацию только о текущих событиях, связанных с запущенной задачей, выполните следующую команду:

```
kesl-control --start-task <идентификатор/имя задачи> -W
```

Пример:
Включить вывод текущих событий запущенной задачи с ID=1:

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

Чтобы вывести в консоль информацию о текущих событиях, соответствующих условиям фильтра, выполните следующую команду:

```
kesl-control -W --query "<условия фильтра>"
```

Условия фильтра задаются с помощью одного или нескольких логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`.

Пример:
Вывести события TaskStateChanged:

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

Вывести события TaskSettingsChanged, инициированных пользователем User:

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

Вывод событий из журнала событий

Вы можете выводить в консоль или в файл информацию о событиях из журнала событий приложения. Вы можете использовать фильтр для вывода определенных событий.

Чтобы вывести в консоль информацию обо всех событиях в журнале событий приложения, выполните следующую команду:

```
kesl-control -E --query [--db <файл базы данных>]
```

где:

- `<файл базы данных>` – полный путь к файлу базы данных журнала событий, из которого вы хотите вывести события. По умолчанию приложение сохраняет информацию о событиях в базе данных /var/opt/kaspersky/kesl/private/storage/events.db. Расположение базы данных определяется общим параметром приложения `EventsStoragePath`.

Вы можете использовать утилиту `less`, чтобы перемещаться по списку отображаемых событий. По умолчанию в приложении хранится до 500 000 событий. Максимальное количество событий, которые хранит приложение, определяется общим параметром приложения `MaxEventsNumber`.

Если журнал событий расположен в базе данных по умолчанию, вы можете выводить в консоль информацию обо всех событиях с помощью команды:

```
kesl-control -E
```

Чтобы вывести в консоль информацию о событиях в журнале событий приложения, соответствующих определенным условиям, выполните следующую команду:

```
kesl-control -E --query "<условия фильтра>" [--db <файл базы данных>] [-n
<количество>] [--json] [--reverse]
```

где:

- `<условия фильтра>` – одно или несколько логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.
- `<количество>` – количество последних событий из выборки (то есть количество записей от конца выборки), которые нужно вывести.
- `--json` – выводить события в формате JSON.
- `--reverse` – выводить события в обратном порядке (от самого нового события наверху к более старым внизу).

Чтобы вывести в файл информацию о событиях в журнале событий приложения, соответствующих определенным условиям, выполните следующую команду:

```
kesl-control -E --query "<условия фильтра>" [--db <файл базы данных>] [-n
<количество>] --file <путь к файлу> [--json]
```

где `--file <путь к файлу>` – полный путь к файлу, в который вы хотите вывести события.

Проверка целостности компонентов приложения

Приложение Kaspersky Endpoint Security содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленники могут заменить один или несколько исполняемых модулей или файлов приложения другими файлами, содержащими вредоносный код. Чтобы предотвратить такую замену модулей и файлов, в приложении Kaspersky Endpoint Security предусмотрена проверка целостности компонентов приложения. Приложение проверяет модули и файлы на наличие неавторизованных изменений и повреждений. Если модуль или файл приложения имеет некорректную контрольную сумму, то он считается поврежденным.

Проверка целостности выполняется для следующих компонентов приложения, если они установлены на устройстве:

- пакет приложения;
- пакет графического пользовательского интерфейса;
- пакет Агента администрирования Kaspersky Security Center;
- плагин управления приложением Kaspersky Endpoint Security.

Приложение проверяет целостность файлов, перечисленных в специальных списках, которые называются *файлы манифеста*. Для каждого компонента приложения существует свой файл манифеста, содержащий список файлов приложения, целостность которых важна для корректной работы этого компонента приложения. Имя файла манифеста для каждого компонента одно и тоже, но содержимое файлов манифестов различается. Файлы манифеста подписаны цифровой подписью, их целостность также проверяется.

Проверка целостности компонентов приложения выполняется с помощью утилиты проверки целостности.

Утилиту проверки целостности требуется запускать под учетной записью с root-правами.

Для проверки целостности вы можете использовать как утилиту, устанавливаемую вместе с приложением, так и утилиту, поставляемую на сертифицированном CD-диске.

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

Утилита проверки целостности, устанавливаемая вместе с приложением, расположена по следующим путям:

- для проверки пакета приложения, пакета графического пользовательского интерфейса и Агента администрирования: /opt/kaspersky/kesl/bin/integrity_checker;
- для проверки плагина управления Kaspersky Endpoint Security – в директории, где расположены исполняемые модули (DLL) плагина управления:
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<версия плагина>.plg\integrity_checker.exe – для 32-битных операционных систем;
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<версия плагина>.plg\integrity_checker.exe – для 64-битных операционных систем.

Файлы манифеста расположены по следующим путям:

- /opt/kaspersky/kesl/bin/integrity_check.xml – для проверки целостности пакета приложения;
- /opt/kaspersky/kesl/bin/gui_integrity_check.xml – для проверки целостности пакета графического пользовательского интерфейса;
- /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – для проверки Агента администрирования для 32-битных операционных систем;
- /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml – для проверки Агента администрирования для 64-битных операционных систем.

Чтобы проверить целостность компонентов приложения, выполните следующую команду:

- для проверки пакета приложения и пакета графического пользовательского интерфейса:

  `integrity_checker [<путь к файлу манифеста>] --signature-type kds-with-filename`

- для проверки плагина управления Kaspersky Endpoint Security и Агента администрирования:

  `integrity_checker [<путь к файлу манифеста>]`

  По умолчанию используется путь к файлу манифеста, расположенному в той же директории, в которой расположена утилита проверки целостности.

Вы можете запустить утилиту со следующими необязательными параметрами:

- `--crl <директория>` – путь к директории, содержащей список отозванных сертификатов (Certificate Revocation List).
- `--version` – отобразить версию утилиты.
- `--verbose` – детализировать вывод информации о выполненных действиях и результатах. Если вы не укажете этот параметр, будут отображаться только ошибки, объекты, не прошедшие проверку, и общая статистика проверки.
- `--trace <имя файла>`, где `<имя файла>` – имя файла, в который будут записываться события с уровнем детализации DEBUG, произошедшие во время проверки.
- `--signature-type kds-with-filename` – тип проверяемой сигнатуры (этот параметр является обязательным для проверки пакета приложения, пакета графического пользовательского интерфейса и Агента администрирования).
- `--single-file <файл>` – проверить только один файл, входящий в состав манифеста, остальные объекты манифеста игнорировать.

Вы можете просмотреть описание всех доступных параметров утилиты проверки целостности в справке параметров утилиты, выполнив команду `integrity_checker --help`.

Результат проверки файла манифеста отображается в следующем виде:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата 0).
- `FAILED` – целостность файлов не подтверждена (код возврата отличен от 0).

Если при запуске приложения обнаружено нарушение целостности приложения или Агента администрирования, приложение Kaspersky Endpoint Security формирует событие *IntegrityCheckFailed* в журнале событий и в Kaspersky Security Center.

Управление приложением через графический пользовательский интерфейс

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, графический пользовательский интерфейс не поддерживается.

С помощью графического пользовательского интерфейса приложения Kaspersky Endpoint Security вы можете:

- Просматривать информацию о состоянии защиты устройства.
- Включать и выключать компоненты приложения:
  - Защита от файловых угроз.
  - Проверка съемных дисков.
  - Защита от веб-угроз.
  - Защита от сетевых угроз.
  - Защита от шифрования.
  - Управление сетевым экраном.
  - Контроль приложений.
  - Контроль устройств.
  - Анализ поведения.
  - Контроль целостности системы.
- Запускать и останавливать задачи проверки:
  - Поиск вредоносного ПО.
  - Проверка важных областей.
  - Проверка контейнеров.
- Запускать и останавливать задачи обновления и отката обновления баз.
- Запускать выборочную проверку файлов и директорий (запускается при нажатии кнопкой мыши на файле или директории, которые вы хотите проверить).
- Включать и выключать использование Kaspersky Security Network.
- Просматривать статистику работы и отчеты приложения.
- Управлять лицензионными ключами приложения и просматривать информацию о лицензии, по которой используется приложение, и о связанном с лицензией ключе.
- Просматривать информацию об объектах, помещенных в резервное хранилище.

- Создавать файлы трассировки приложения.

Если компонент и задача приложения работает в информирующем режиме, в графическом пользовательском интерфейсе приложения для компонента и задачи отображается предупреждение *Выбран информирующий режим работы*.

Графический пользовательский интерфейс

Значок приложения в области уведомлений

После установки пакета графического пользовательского интерфейса приложения Kaspersky Endpoint Security на устройстве в области уведомлений панели задач справа появляется значок приложения.

Значок приложения обеспечивает доступ к контекстному меню и главному окну приложения.

Контекстное меню значка приложения содержит следующие пункты:

- **Kaspersky Endpoint Security 12.1 для Linux**. Открывает главное окно приложения, в котором отображается состояние защиты устройства и находятся элементы интерфейса, предоставляющие доступ к функциям приложения.
- **Выход**. Выполняет выход из графического пользовательского интерфейса приложения.

Главное окно приложения

Вы можете открыть главное окно приложения одним из следующих способов:

- С помощью правой кнопки мыши или двойным щелчком мыши по значку приложения в области уведомлений панели задач.
- Выбрав название приложения в меню приложений оконного менеджера операционной системы.

Главное окно приложения разделено на несколько частей:

- В центральной части главного окна приложения отображается статус защиты устройства. При нажатии кнопкой мыши на этой области окна открывается окно **Центр защиты**. В этом окне отображается информация о состоянии защиты устройства и рекомендации о действиях, которые вам нужно выполнить для устранения проблем в защите (при их наличии).
- На кнопке **Проверка** отображается состояние задачи поиска вредоносного ПО и количество обнаруженных угроз. При нажатии на эту кнопку открывается окно **Проверка**. В этом окне вы можете запустить и остановить задачи *Поиск вредоносного ПО*, *Проверка важных областей* и *Проверка контейнеров*. Вы также можете просмотреть отчеты для этих задач.
- На кнопке **Обновление** отображается состояние задачи *Обновление*. При нажатии на эту кнопку открывается окно **Обновление**. В этом окне вы можете запустить задачи *Обновление* и *Откат обновления баз*. Вы также можете просмотреть отчеты для этих задач.
- В нижней части главного окна приложения находятся следующие элементы:
  - Кнопка **Отчеты**. При нажатии на эту кнопку открывается окно **Отчеты**, в котором вы можете просмотреть статистику работы компонентов и задач и различные отчеты.

- Кнопка **Резервное хранилище**. При нажатии на эту кнопку открывается окно **Резервное хранилище**, в котором содержится информация об объектах в резервном хранилище.

- Кнопка **Настройка**. При нажатии на эту кнопку открывается окно **Настройка**, в котором вы можете включить или выключить компоненты приложения, а также настроить использование Kaspersky Security Network.

- Кнопка **Поддержка**. При нажатии на эту кнопку открывается окно **Поддержка**, в котором отображается текущая версия приложения и следующая информация:

  - **Ключ** – активный лицензионный ключ, добавленный в приложение, или информация об отсутствии ключа. По ссылке в этом поле вы можете открыть окно **Лицензия**, в котором отображается подробная информация о лицензии.

  - **Статус ключа** – информация о статусе активного лицензионного ключа или информация об отсутствии ключа.

  - **Дата выпуска баз** – состояние и дата выпуска баз приложения.

  - **Операционная система** – сведения об операционной системе устройства.

  В нижней части окна **Поддержка** отображаются ссылки на информационные ресурсы "Лаборатории Касперского" и ссылка, по которой открывается окно **Трассировка**. В этом окне вы можете создавать файлы трассировки приложения и настраивать уровень детализации файлов трассировки.

- В нижней части главного окна приложения отображается информация о лицензии и о ключе, а также о проблемах лицензирования (при их наличии). При нажатии кнопкой мыши на этой области окна открывается окно **Лицензия**, в котором отображается подробная информация о лицензии.

  По кнопке **Приобрести лицензию** в этом окне вы можете открыть веб-сайт интернет-магазина "Лаборатории Касперского", где вы можете приобрести лицензию. После приобретения лицензии вы получите код активации или файл ключа, с помощью которых нужно активировать приложение.

Включение и выключение компонентов приложения

С помощью графического пользовательского интерфейса вы можете включать и выключать компоненты приложения. Если компонент включен, доступна кнопка **Выключить**. По умолчанию включены компоненты Защита от файловых угроз, Контроль устройств и Анализ поведения. Компонент Защита от веб-угроз может включаться автоматически, если на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен) и в системе обнаружен один из поддерживаемых браузеров.

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

Чтобы включить или выключить компонент приложения:

1. Откройте главное окно приложения.

2. В нижней части главного окна приложения нажмите на кнопку **Настройка**.

   Откроется окно **Настройка**.

3. Нажмите на кнопку **Включить** или **Выключить** для нужного компонента.

Запуск и остановка задач проверки

Чтобы запустить или остановить задачу проверки:

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
3. Выполните одно из следующих действий:

   - Если вы хотите запустить задачу проверки, нажмите на кнопку **Запустить**, расположенную под той задачей проверки, которую вы хотите запустить.

     Отобразится ход выполнения задачи проверки.

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

     Задача проверки остановится, отобразится информация о проверенных объектах и обнаруженных угрозах.
4. Если вы хотите просмотреть отчет по задаче проверки, нажмите на кнопку **Показать отчет**.

При обнаружении зараженного объекта или при завершении задачи проверки отображается всплывающее окно в области уведомлений рядом со значком приложения в правой части панели задач.

Также в окне **Проверка** отображается ход и результат выполнения временных задач проверки загрузочных секторов (*Scan_Boot_Sectors_{идентификатор}*) и временных задач выборочной проверки файлов (*Scan_File_{идентификатор}*). Вы можете скрыть информацию о выполненных временных задачах, нажав на крестик или закрыв окно **Проверка** (при переходе в главное окно или при выходе из приложения).

Запуск и остановка задачи обновления

Чтобы запустить или остановить задачу обновления:

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на кнопку **Обновление**.

   Откроется окно **Обновление**.
3. Выполните одно из следующих действий:

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

     Отобразится ход выполнения задачи обновления.

     При успешном завершении задачи обновления становится доступна ссылка **Откатить обновление**, с помощью которой вы можете откатить последнее успешное обновление баз.

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

     Задача обновления остановится.

4. Если вы хотите просмотреть отчет по задаче, нажмите на кнопку **Показать отчет**.

Чтобы запустить задачу отката обновления:

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на раздел **Обновление**.

   Откроется окно **Обновление**.
3. Запустите задачу отката обновления баз по ссылке **Откатить обновление**.

Настройка использования Kaspersky Security Network

С помощью графического пользовательского интерфейса вы можете включать или выключать использование Kaspersky Security Network.

Чтобы включить использование Kaspersky Security Network:

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Настройка**.

   Откроется окно **Настройка**.
3. В окне **Настройка** выберите один из следующих вариантов:

   - **Расширенный режим KSN**, если вы хотите использовать Kaspersky Security Network, получать информацию из базы знаний и отправлять анонимную статистику и данные о типах и источниках угроз.
   - **Стандартный режим KSN**, если вы хотите использовать Kaspersky Security Network, получать информацию из базы знаний, но не отправлять анонимную статистику и данные о типах и источниках угроз.
4. Нажмите на кнопку **Включить**.

   Откроется окно **Использование Kaspersky Security Network**.
5. В окне **Использование Kaspersky Security Network** внимательно прочитайте Положение о Kaspersky Security Network и выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.
6. Нажмите **OK**.

   Кнопка **OK** недоступна, если в окне **Использование Kaspersky Security Network** не выбран ни один из вариантов.

Чтобы выключить использование Kaspersky Security Network:

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Настройка**.

   Откроется окно **Настройка**.
3. Нажмите на кнопку **Выключить**.

4. В открывшемся окне нажмите на кнопку **Да**, чтобы отказаться от использования Kaspersky Security Network.

Просмотр отчетов

С помощью графического пользовательского интерфейса вы можете просматривать отчеты приложения. В отчеты записывается информация о работе компонентов и задач приложения.

Данные в отчетах представлены в виде таблицы, которая содержит список событий. Каждая строка в таблице содержит информацию об отдельном событии. Атрибуты события отображаются в столбцах таблицы. События, зарегистрированные в работе разных компонентов и задач, имеют разный набор атрибутов.

В отчетах предусмотрены следующие уровни важности событий:

- *Критический* – события критической важности, на которые нужно обратить внимание, поскольку они указывают на проблемы в работе приложения или на уязвимости в защите устройства.
- *Высокий.*
- *Средний.*
- *Низкий.*
- *Информационный.*
- *Ошибка.*

Отчеты отображаются в окне, которое открывается по кнопке **Отчеты**, расположенной в нижней части главного окна приложения.

В приложении доступны следующие отчеты:

- **Статистика**. Этот отчет содержит статистические данные о работе компонента Защита от файловых угроз и о задачах проверки. Вы можете обновить отображаемый отчет, нажав на кнопку **Обновить**.
- **Системный аудит**. Этот отчет содержит информацию о событиях, которые произошли во время работы приложения и во время взаимодействия пользователя с приложением.
- **Защита от угроз**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы следующих компонентов приложения:
  - Защита от файловых угроз.
  - Проверка съемных дисков.
  - Защита от шифрования.
  - Защита от веб-угроз.
  - Защита от сетевых угроз.
  - Управление сетевым экраном.
  - Контроль приложений.

- Контроль устройств.
- Анализ поведения.
- Контроль целостности системы.

- **Задачи по требованию**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время выполнения задач проверки, задач обновления и проверки целостности системы.

Чтобы просмотреть отчет:

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Отчеты**.

   Откроется окно **Отчеты**.
3. В левой части окна **Отчеты** выберите нужный тип отчета.

   В правой части окна отобразится отчет, содержащий список событий.

   По умолчанию события в отчете отсортированы по возрастанию значений столбца **Дата**.
4. Если вы хотите посмотреть подробную информацию о событии, выберите это событие в отчете.

   В нижней части окна отобразится блок, который содержит атрибуты этого события.

Для удобства работы с отчетами вы можете изменять представление данных на экране следующими способами:

- фильтровать список событий по времени возникновения;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке.

Просмотр объектов резервного хранилища

С помощью графического пользовательского интерфейса вы можете выполнять следующие действия с объектами резервного хранилища:

- Просматривать информацию об объектах, помещенных в резервное хранилище на устройстве.
- Восстанавливать объекты из резервного хранилища в их исходные директории.
- Удалять объекты из резервного хранилища. Удаленные объекты восстановить невозможно.

Информация о восстановлении и удалении объектов записывается в журнал событий.

Чтобы просмотреть объекты в резервном хранилище:

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Резервное хранилище**.

   Откроется окно **Резервное хранилище**.

В окне отображается следующая информация об объектах резервного хранилища:

- название объекта;
- полный путь к объекту;
- дата добавления объекта в резервное хранилище;
- дата удаления объекта из резервного хранилища (это поле отображается, если задано ограничение на время хранения объектов в резервном хранилище);
- размер объекта.

Управление лицензионными ключами

С помощью графического пользовательского интерфейса вы можете добавлять и удалять лицензионные ключи приложения, а также просматривать информацию о лицензии, по которой используется приложение, и о связанном с лицензией ключе.

Вы можете активировать приложение, добавив активный лицензионный ключ.

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии приложения в течение срока действия лицензии.

Если вы используете приложение по лицензии, которая не включает функциональность Kaspersky Endpoint Detection and Response Optimum, для активации этой функциональности вам нужно добавить дополнительный лицензионный ключ Kaspersky Endpoint Detection and Response Optimum Add-on (далее также "ключ EDR Optimum").

Вы также можете добавить в приложение резервный ключ. Резервный ключ становится активным либо по истечении срока действия лицензии, связанной с активным ключом, либо при удалении активного ключа. Наличие резервного ключа позволяет избежать ограничения функциональности приложения в момент окончания срока действия лицензии.

Резервный ключ может быть добавлен только после добавления активного лицензионного ключа.

Добавление лицензионного ключа

Чтобы добавить активный лицензионный ключ в приложение:

1. Откройте главное окно приложения.
2. Выполните одно из следующих действия:
   - В нижней части главного окна приложения нажмите на область окна, в которой отображается информация о лицензии и о ключе.

- В нижней части главного окна приложения нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** откройте окно **Лицензия** по ссылке в поле **Ключ**.

Откроется окно **Лицензия**. По кнопке **Приобрести лицензию** в этом окне вы можете открыть веб-сайт интернет-магазина "Лаборатории Касперского", где вы можете приобрести лицензию.

3. Вы можете активировать приложение по коммерческой лицензии или по пробной лицензии.

   Чтобы активировать приложение по коммерческой лицензии:

   a. Нажмите на кнопку **Добавить** в блоке **Коммерческий ключ** и выполните следующие действия в зависимости от способа добавления ключа:

      - Если вы хотите добавить ключ с помощью кода активации, введите код активации и нажмите на кнопку **Далее**.

      - Если вы хотите добавить ключ с помощью файла ключа, нажмите на кнопку **Добавить ключ** и в открывшемся окне выберите файл с расширением key.

      В окне отобразится информация о ключе и связанной с ним лицензии.

   b. Нажмите на кнопку **Активировать**.

   Чтобы активировать приложение по пробной лицензии, нажмите на кнопку **Активировать** в блоке **Пробный ключ**. В окне отобразится информация о пробной лицензии и связанном с ней ключе.

   > Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

После добавления активного ключа приложения вы можете добавить резервный ключ и, если требуется, дополнительный ключ EDR Optimum. Для запуска процедуры добавления резервного или дополнительного ключа используйте кнопку **Добавить** в верхней части окна **Лицензия**.

Удаление лицензионного ключа

Чтобы удалить лицензионный ключ, добавленный в приложение:

1. Откройте главное окно приложения.

2. Выполните одно из следующих действий:

   - В нижней части главного окна приложения нажмите на область окна, в которой отображается информация о лицензии и о ключе.

   - В нижней части главного окна приложения нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** откройте окно **Лицензия** по ссылке в поле **Ключ**.

   Откроется окно **Лицензия**.

3. Нажмите на кнопку **Удалить**, расположенную справа от информации о ключе, который вы хотите удалить.

4. Подтвердите удаление в открывшемся окне.

Просмотр информации о лицензии

Чтобы просмотреть информацию о лицензии:

1. Откройте главное окно приложения.

2. Выполните одно из следующих действия:

   - В нижней части главного окна приложения нажмите на область окна, в которой отображается информация о лицензии и о ключе.

   - В нижней части главного окна приложения нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** откройте окно **Лицензия** по ссылке в поле **Ключ**.

   Откроется окно **Лицензия**.

В окне отображается информация о лицензии, по которой используется приложение, и о лицензии, связанной с резервным ключом, если резервный ключ добавлен в приложение. По ссылке **Подробнее** вы можете просматривать полную информацию о лицензиях и ключах.

В блоке **Действующие лицензии** отображается информация об активных ключах и связанных с ними лицензиях:

- Тип активной лицензии приложения, лицензионное ограничение и срок действия лицензии.
- **Ключ** – уникальная буквенно-цифровая последовательность.
- **Статус ключа** – статус ключа или сообщение о каких-либо проблемах, связанных с ключом (при их наличии).
- **Действует с** – дата активации приложения путем добавления этого ключа.
- **Истекает** – количество дней до истечения срока действия лицензии и дата окончания срока действия лицензии в формате UTC.
- **Название приложения** – название приложения, для активации которого предназначен ключ.
- **Защита** – информация об ограничении функций защиты и функции обновления баз приложения.

Если вы добавили в приложение активный ключ EDR Optimum, информация об этом ключе и связанной с ним лицензии также отображается в блоке **Действующие лицензии**.

В блоке **Резервные ключи** отображается информация о резервных ключах и связанных с ними лицензиях:

- Тип резервного ключа, лицензионное ограничение и срок действия лицензии, связанной с ключом.
- **Ключ** – уникальная буквенно-цифровая последовательность.
- **Тип лицензии** – тип лицензии, связанной с резервным ключом.
- **Название приложения** – название приложения, для активации которого предназначен ключ.
- **Защита** – информация об ограничении функций защиты и функции обновления баз приложения.

Если вы добавили в приложение резервный ключ EDR Optimum, информация об этом ключе и связанной с ним лицензии также отображается в блоке **Резервные ключи**.

Создание файла трассировки

С помощью графического пользовательского интерфейса вы можете создавать файлы трассировки приложения и настраивать уровень детализации файлов трассировки.

Чтобы создать файл трассировки:

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Поддержка**.

   Откроется окно **Поддержка**.
3. По ссылке **Трассировка** откройте окно **Трассировка**.
4. В раскрывающемся списке **Уровень** выберите уровень детализации файла трассировки.

   Рекомендуется уточнить требуемый уровень детализации у специалистов Службы технической поддержки "Лаборатории Касперского". По умолчанию установлено значение **Диагностический (300)**.
5. Нажмите на кнопку **Включить**, чтобы запустить процесс трассировки.
6. Воспроизведите ситуацию, при которой у вас возникает проблема.
7. Нажмите на кнопку **Выключить**, чтобы остановить процесс трассировки.

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

Контейнерное приложение Kaspersky Endpoint Security (KESL-контейнер)

В комплект поставки приложения Kaspersky Endpoint Security включены файлы для сборки контейнерного приложения (далее KESL-контейнер) для встраивания во внешние системы с целью проверки образов контейнеров из репозиториев с образами.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, функциональность KESL-контейнера не поддерживается.

KESL-контейнер позволяет:

- Проверять образы контейнеров, размещенных в репозиториях.
- Переносить проверенные образы, не содержащие зараженные объекты, в доверенный репозиторий.

После развертывания, активации и настройки KESL-контейнера в нем доступны следующие функциональные компоненты и задачи приложения Kaspersky Endpoint Security:

- Компонент Защита от файловых угроз.
- Задачи проверки:
  - Поиск вредоносного ПО;
  - Проверка важных областей;
  - Проверка контейнеров.
- Компонент Мониторинг контейнеров.

В KESL-контейнере доступны следующие дополнительные функции приложения Kaspersky Endpoint Security:

- Активация приложения с помощью файла ключа или кода активации.
- Обновление баз приложения и откат обновления баз.
- Сохранение резервных копий файлов в резервном хранилище, расположенном на устройстве.

Взаимодействие с KESL-контейнером осуществляется через REST API, также вы можете настраивать параметры KESL-контейнера в Kaspersky Security Center с помощью политик.

Для корректной работы KESL-контейнеров в Kaspersky Security Center рекомендуется помещать устройства, которые соответствуют KESL-контейнерам, в отдельную группу администрирования со своей политикой. В свойствах политики доступны для редактирования все функции и параметры приложения Kaspersky Endpoint Security, но настройка параметров, не поддерживаемых в KESL-контейнере, не влияет на работу KESL-контейнера.

Управление KESL-контейнером через командную строку не поддерживается.

Если KESL-контейнер был активирован при развертывании и подключен к Kaspersky Security Center, в котором настроено автоматическое распространение лицензионного ключа на управляемые устройства, то на устройства, соответствующие KESL-контейнерам, этот ключ не распространяется.

Развертывание и активация KESL-контейнера

Описание пакета распространения

Пакет распространения содержит следующие файлы:

- docker-service-<версия>.tgz – архив с файлами, необходимыми для создания образа;
- kesl-<версия>.rpm – инсталляционный пакет приложения Kaspersky Endpoint Security;
- klnagent.rpm – инсталляционный пакет Агента администрирования Kaspersky Security Center.

Архив docker-service-<версия>.tgz содержит следующие файлы:

- kesl-service – директория файлов контейнерного приложения;
- Dockerfile – файл для сборки образа docker с версией ниже 18.06;
- Dockerfile.1809 – файл для сборки образа docker с версией выше 18.05;
- build.sh.example – пример скрипта для сборки образа;
- run.sh.example – пример скрипта для запуска KESL-контейнера;
- kesl-service.config.example – пример конфигурационного файла контейнерного приложения;
- klnagent.conf.example – пример конфигурационного файла для подключения к Kaspersky Security Center;
- readme.md – краткая справка.

Развертывание и активация KESL-контейнера

Чтобы подготовить KESL-контейнер к использованию:

1. Распакуйте архив tar -xvf docker-service-<версия>.tgz.
2. Если вы хотите настраивать параметры KESL-контейнера через Kaspersky Security Center, выполните следующие действия:
   a. В файле klnagent.conf.example укажите значения переменных Агента администрирования. Дополнительная информация приведена в справке Kaspersky Security Center (раздел "*Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)*").
   b. Скопируйте klnagent.conf.example в kesl-service/klnagent.conf.
3. Соберите Docker-образ KESL-контейнера с помощью скрипта установки build.sh.example:

a. Если используется прокси-сервер, укажите нужные значения для переменной COMMON_AGRS.

b. Если требуется, измените имя целевого образа kesl-service на нужное.

c. Скопируйте build.sh.example в build.sh и поставьте ему атрибут исполняемого файла.

d. Запустите build.sh.

4. Проверьте, что сборка завершилась успешно, выполнив команду `docker images -a`.

   Отобразится следующий результат выполнения команды:

   ```
   REPOSITORY TAG IMAGE ID CREATED SIZE
   kesl-service latest <hex> < время создания > < размер >
   ```

5. Активируйте KESL-контейнер одним из следующих способов:

   - Через Kaspersky Security Center. Чтобы активировать KESL-контейнер, вам нужно добавить ключ на устройства, которые соответствуют KESL-контейнерам, в Web Console или в Консоли администрирования.

     > Для корректной работы KESL-контейнеров в Kaspersky Security Center рекомендуется помещать устройства, которые соответствуют KESL-контейнерам, в отдельную группу администрирования со своей политикой. При остановке KESL-контейнера эти устройства автоматически удаляются из группы администрирования, при этом освобождается ключ, который использовался на этих устройствах.

   - Через конфигурационный файл.

   - Через переменную окружения (см. шаг 7).

6. Настройте KESL-контейнер (Настройка KESL-контейнера, Параметры KESL-контейнера).

7. Запустите KESL-контейнер, используя команду `docker run --privileged --init -p < порт_KESL-контейнера >:< порт_устройства > \`

   ```
   -e < переменная _1> -e < переменная _2> ... -e < переменная _n> \
   -v < точка_монтирования _1> -v < точка_монтирования _2> ... -v < точка_монтирования _n> \
   < имя_образа >
   ```

   где:

   - `< порт_KESL-контейнера >` – порт KESL-контейнера, который должен быть доступным для сети вне KESL-контейнера;

   - `< порт_устройства >` – порт устройства, на котором установлен KESL-контейнер.

   При запуске KESL-контейнера вы можете активировать KESL-контейнер через переменную окружения:

   - Если вы используете код активации, добавьте параметр `KRAS4D_ACTIVATION='< код активации >'`:

     ```
     docker run ... -e KRAS4D_ACTIVATION='< код активации >'
     ```

   - Если вы используете файл ключа, добавьте параметры `KRAS4D_ACTIVATION='< файл ключа >'` и `KRAS4D_KEYPATH=/root/kesl-service/keys`:

     ```
     docker run ... -e KRAS4D_ACTIVATION='< файл ключа >' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v < путь к директории ключей >:/root/kesl-service/keys
     ```

Вы можете посмотреть пример команды запуска в файле run.sh.example.

Настройка KESL-контейнера

Параметры KESL-контейнера инициализируются несколькими способами:

- По умолчанию (если не указан другой способ).
- Из конфигурационного файла. В этом случае значения из конфигурационного файла имеют приоритет над значениями по умолчанию.
- Передачей значений в KESL-контейнер при его запуске в виде переменных окружения. Переменные окружения имеют приоритет над параметрами конфигурационного файла.
- В теле запроса на проверку. Параметры в теле запроса имеют максимальный приоритет, но действуют только в рамках одного запроса.

Параметры KESL-контейнера

Параметры KESL-контейнера и их значения по умолчанию приведенные в таблице ниже.

Параметры KESL-контейнера

Описание параметра	Возможные значения	Значение по умолчанию
Порт для прослушивания REST API		8085
Уровень важности событий	`debug` – отладочный `info` – информационный `warning` – предупреждение `error` – ошибка `critical` – критический `noset` – не указан	noset
Ключ авторизации	Если задан параметр `KRAS4D_XAPIKEY`, то каждый запрос проверяется на наличие заголовка x-api-key и соответствие его содержимого значению параметра `KRAS4D_XAPIKEY`. При невыполнении этих условий запрос будет отклонен. При отсутствии этого параметра проверка не выполняется.	
Код активации или файл ключа	Чтобы активировать KESL-контейнер с помощью кода активации, при запуске KESL-контейнера требуется указать код активации в конфигурационном файле или передать код активации через переменную окружения: `docker run ... -e KRAS4D_ACTIVATION='<код активации>'`	

	Чтобы активировать KESL-контейнер с помощью файла ключа, при запуске KESL-контейнера требуется указать файл ключа в конфигурационном файле или передать файл ключа через переменную окружения: `docker run ... -e KRAS4D_ACTIVATION='<файл ключа>' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v <путь к директории ключей>:/root/kesl-service/keys` Для активации KESL-контейнера с помощью файла ключа требуется наличие точки монтирования /root/kesl-service/keys.	
Дополнительные параметры проверки	Необязательный параметр `KRAS4D_SCANOPTIONS` позволяет настраивать параметры задачи Проверка контейнеров: `docker run ... -e KRAS4D_SCANOPTIONS='<параметры>'` где `<параметры>` – параметры задачи Проверка контейнеров.	
Дополнительные параметры обновления	Необязательный параметр `KRAS4D_UPDATEOPTIONS` позволяет настраивать параметры задачи Обновление. `docker run ... -e KRAS4D_UPDATEOPTIONS='<параметры>'` где `<параметры>` – параметры задачи Обновление `SourceType`, `ApplicationUpdateMode` и параметры секции `CustomSources.item_#`.	
Обновлять базы приложения при запуске KESL-контейнера	По умолчанию базы приложения при запуске KESL-контейнера скачиваются в директорию /var/opt/kaspersky/kesl/private/updates. Для реализации совместной работы нескольких KESL-контейнеров с одним экземпляром баз приложения и/или ускорения запуска KESL-контейнера рекомендуется вынести эту директорию на устройство, где установлен KESL-контейнер, путем монтирования: `docker run ... -v <путь к директории баз>:/var/opt/kaspersky/kesl/private/updates`	True
Не обрабатывать образ, если он уже имеется в целевом репозитории		False
Максимальное время ожидания выполнения команд приложения в секундах		600
Максимальное время ожидания выполнения задачи обновления баз приложения в секундах		600

Название конфигурационного файла KESL-контейнера		kesl-service.config

Переменные окружения

Для настройки KESL-контейнера предусмотрены следующие переменные окружения:

- KRAS4D_PORT – порт для прослушивания REST API.
- KRAS4D_LOGLEVEL – уровень важности событий.
- KRAS4D_XAPIKEY – ключ авторизации запроса.
- KRAS4D_ACTIVATION – код активации или имя файла ключа.
- KRAS4D_SCANOPTIONS – дополнительные параметры проверки.
- KRAS4D_UPDATEOPTIONS – дополнительные параметры обновления.
- KRAS4D_FORCEUPDATE – обновлять базы приложения при запуске KESL-контейнера.
- KRAS4D_SKIPIMAGEIFEXISTS – не обрабатывать образ, если он уже имеется в целевом репозитории.
- KRAS4D_GENERALTIMEOUT – максимальное время ожидания выполнения команд приложения.
- KRAS4D_UPDTASKTIMEOUT – максимальное время ожидания выполнения задачи обновления баз приложения.
- KRAS4D_CFGNAME – название конфигурационного файла KESL-контейнера.

Конфигурационный файл

Конфигурационный файл KESL-контейнера имеет формат yaml. Для обеспечения возможности чтения параметров из файла требуется смонтировать путь /root/kesl-service/config/ на устройство, где установлен KESL-контейнер, и указать название конфигурационного файла, если оно отличается от названия по умолчанию. Таким образом, для каждого набора KESL-контейнеров можно указать свой конфигурационный файл.

Пример запуска KESL-контейнера:

```
docker run ... \
-e KRAS4D_CFGNAME='unique_file_name' \
-v <HOST_PATH>:/root/kesl-service/config \
kesl-service
```

В таблице ниже приведены параметры конфигурационного файла и соответствующие им переменные окружения.

Соответствие параметров переменным окружения

Параметр конфигурационного файла	Переменная окружения
Секция common	
port: <порт для прослушивания>	# KRAS4D_PORT=8085
sqlpath: <полный путь к файлу базы данных результатов проверок>	# KRAS4D_SQLPATH
certdir: <путь к директории с сертификатами реестров>	# KRAS4D_CERTDIR
keypath: <путь к директории с лицензионными ключами>	# KRAS4D_KEYPATH
tmppath: <полный путь ко временной директории>	# KRAS4D_TMPPATH
logpath: <полный путь к журналу событий>	# KRAS4D_LOGPATH
loglevel: [noset|debug|info|warning|error|critical]	# KRAS4D_LOGLEVEL
Секция control	
xapikey: <ключ авторизации запроса>	# KRAS4D_XAPIKEY=None
forceupdate: <принудительное обновление баз при старте контейнера [True|False]>	# KRAS4D_FORCEUPDATE
activation: <код активации или имя файла ключа из /root/kesl-service/config/>	# KRAS4D_ACTIVATION
detectaction: [delete|skip]	# KRAS4D_DETECTACTION
scanoptions: <параметры проверки [ScanArchived=yes ScanSfxArchived=yes ...]>	# KRAS4D_SCANOPTIONS
skipimageifexist: <не проверять образ, если он уже есть на сервере, на который нужно скопировать проверенный образ>	# KRAS4D_SKIPIMAGEIFEXIST
generaltimeout: <максимальное время ожидания выполнения команд приложения>	# KRAS4D_GENERALTIMEOUT
updtasktimeout: <максимальное время ожидания выполнения задачи обновления баз приложения>	# KRAS4D_UPDTASKTIMEOUT
Секция repositories	
<server>:<port>: адрес и порт реестра образов, на котором требуется авторизация при запросе на проверку	
Подсекция credentials	
user: имя пользователя для авторизации в реестре образов	
pass: пароль для авторизации в реестре образов	

Пример конфигурационного файла:

```
common:
    port: 8085
    sqlpath: './data/scans.sqlite'
    tmppath: './tmp/'
    keypath: './keys/'
    certdir: './certificates/'
    logpath: '/var/log/kaspersky/kesl-service/'
    loglevel: 'debug'
control:
    xapikey: 0000
    activation: XXXX-XXXX-XXXX-XXXX or XXXX.key
    scanoptions: 'ScanArchives=yes'
    updateoptions: ''
    forceupdate: True
    skipimageifexists: False
    generaltimeout: 600
    updtasktimeout: 1000
repositories:
    repository.any.com:
        certificate: repository_any_comcert.pem
        credentials:
            user: user
            pass: password
```

Доступные точки монтирования

Для работы с KESL-контейнером доступны следующие точки монтирования:

- /root/kesl-service/data/scans.sqlite – путь к файлу базы данных результатов проверок;
- /var/opt/kaspersky/kesl/private/updates – путь к базам приложения;
- /root/kesl-service/certificates – путь к директории с сертификатами репозиториев;
- /root/kesl-service/keys – путь к директории с лицензионными ключами;
- /var/log/kaspersky/ – путь к директории журналов событий;
- /root/kesl-service/config/ – путь к конфигурационным файлам;
- /var/lib/containers/vfs-storage – обязательная точка монтирования для корректной работы утилиты Podman.

Управление KESL-контейнером через REST API

Взаимодействие с KESL-контейнером реализовано через REST API. Средствами REST API вы можете:

- Выполнить проверку файла или нескольких файлов. Для этого отправьте запрос на проверку (POST).

  Пример:
  POST http://<server>:<port>/scans

  Файл или несколько файлов.

- Выполнить проверку Docker-образа или нескольких Docker-образов. Для этого отправьте запрос на проверку (POST).

  Пример:
  POST http://<server>:<port>/scans

  Ссылка на Docker-образ или Docker-образы для проверки.

- Выполнить проверку Docker-образа или нескольких Docker-образов с дополнительными параметрами. Для этого отправьте запрос на проверку (POST).

  Пример:
  POST http://<server>:<port>/scans

  JSON определенного вида.

- Получить список сессий проверки. Для этого отправьте запрос на получение информации по сессиям проверки (GET).

  Пример:
  GET http://<server>:<port>/scans

- Получить информацию по сессии проверки. Для этого отправьте запрос на получение информации по сессиям проверки (GET).

  Пример:
  GET http://<server>:<port>/scans/<уникальный идентификатор сессии проверки>

- Добавить сертификат реестра без перезагрузки KESL-контейнера. Для этого отправьте запрос на добавление сертификата реестра (POST).

  Пример:
  POST http://<server>:<port>/addcert

- Получить информацию о состоянии KESL-контейнера. Для этого отправьте запрос на получении информации о состоянии KESL-контейнера (GET).

  Пример:
  GET http://<server>:<port>/status

Запрос на проверку (POST)

Назначение

Проверка объекта, указанного в теле запроса.

Предусмотрена проверка следующих объектов:

- одного файла;
- нескольких файлов;
- Docker-образа или нескольких Docker-образов, расположенных в определенном репозитории;
- Docker-образ или несколько Docker-образов, расположенных в определенном репозитории, с указанием дополнительных параметров.

Путь

http://<server>:<port>/scans[?wait=1]

Параметры

Необязательный параметр `wait` задает тип сессии проверки.

Если параметру присвоено значение `1`, то выполняется синхронная проверка и приложение присылает отчет после окончания проверки.

Если параметру присвоено значение `0`, то выполняется асинхронная проверка, а ответ будет иметь вид:

```
{

  "id"="7d27e9b4-a4d7-469b-bdcf-ebfe953498e4",

  "location"="/scans/7d27e9b4-a4d7-469b-bdcf-ebfe953498e4"

}
```

где:

- id – уникальный идентификатор сессии проверки;
- location – путь для запроса информации по этой секции вида http://<server>:<port>/scans/<location>.

Заголовки запроса

Запрос может содержать следующие заголовки:

- Content-Type

  Определяет тип объекта, который передается на проверку.

  Поддерживаемые значения:

  - application/octet-stream – один файл;
  - multipart/form-data – несколько файлов;
  - text/plain – Docker-образ или несколько Docker-образов, расположенных в определенном репозитории;
  - application/json – Docker-образ или несколько Docker-образов, расположенных в определенном репозитории, с указанием дополнительных параметров.

- x-api-key (необязательный)

  API-ключ, заданный в переменной окружения KRAS4D_XAPIKEY или переменной xapikey конфигурационного файла.

Возможные ошибки

Если в заголовке Content-Type указано неподдерживаемое значение, приложение вернет ошибку следующего вида:

```
{
```

```
  "error"={

"code"="NOT_SUPPORTED_CONTENT_TYPE",
"details"="<content type>",
"message"="Not supported Content-Type"
  },

  "status"="error"

}
```

Запрос на проверку файла

Content-Type

application/octet-stream

Тело запроса

Файл.

Пример ответа:

```
{

  "completed": "Mon, 01 Mar 2021 06:54:39 GMT",

  "created": "Mon, 01 Mar 2021 06:54:38 GMT",

  "progress": 100,

  "scan_result": {

"noname": {
"started": "2021-03-01 06:54:39",
"stopped": "2021-03-01 06:54:39",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/b8eb4128-8cb4-4964-87cf-b9853e6544ec"
}
],
"verdict": "infected"
```

```
}
  },
  "status": "completed",
  "verdicts": [
"infected"
  ]
}
```

Запрос на проверку нескольких файлов

Content-Type

multipart/form-data

Тело запроса

Несколько файлов.

Пример ответа:

```
{
  "completed": "Mon, 01 Mar 2021 06:55:44 GMT",
  "created": "Mon, 01 Mar 2021 06:55:43 GMT",
  "progress": 100,
  "scan_result": {
"clean": {
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "clean"
},
"corrupted.com": {
"errors": [
{
"error": "Corrupted object",
```

```
"object": "/root/kesl-service/tmp/75d28fe6-8154-4361-9382-90a76861518a"
}
],
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "non scanned"
},
"error.com": {
"errors": [
{
"error": "read error",
"object": "/root/kesl-service/tmp/37f6e0dd-13f9-4d11-899c-5fe0f23e407d"
}
],
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"verdict": "non scanned"
},
"infected.com": {
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/7d664646-bf56-4060-b958-5ce9e746c929"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"clean",
"non scanned",
"infected"
  ]

}
```

Запрос на проверку Docker-образов

Content-Type

text/plain

Тело запроса

Ссылка на Docker-образ или Docker-образы для проверки.

Возможны следующие значения:

- Путь в репозитории к одному образу (например, https://index.docker.io/jerbi/eicar:latest).
- Маска пути, соответствующая несколькими образам (например, https://index.docker.io/<name mask>:<tag mask>). Для указания маски можно использовать символы ? и *.

Пример ответа:

```
{

  "completed": "Sun, 31 Jan 2021 10:29:26 GMT",

  "created": "Sun, 31 Jan 2021 10:29:20 GMT",

  "progress": 100,

  "scan_result": {

"jerbi/eicar:latest": {
"started": "2021-01-31 10:29:25",
"stopped": "2021-01-31 10:29:26",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}

  },

  "status": "completed",
```

```
  "verdicts": [

"infected"

  ]

}
```

Возможные ошибки

Для получения списка образов по маске используется запрос с использованием Docker REST API.

Однако на многих публичных серверах эта возможность запрещена по причинам безопасности. Попытка проверки образов по маске на таких серверах приводит к ошибке.

Пример ошибки:

```
{

  "completed": "Mon, 01 Mar 2021 07:02:24 GMT",

  "created": "Mon, 01 Mar 2021 07:02:22 GMT",

  "scan_errors": [

{
"code": 401,
"details": {
"context": {
"image_mask": "/jerbi/eic*:latest",
"repository": "index.docker.io",
"repository_base": "index.docker.io"
},
"errors": [
"Unauthorized"
]
},
"message": "Invalid source"
},
[
"Unauthorized"
]
  ],

  "status": "completed"
```

```
  }
```

Запрос на проверку Docker-образов с дополнительными параметрами

Content-Type

application/json

Тело запроса

JSON следующего вида:

```
{
  "source": "https://index.docker.io/jerbi/eicar:latest",
  "params": {
"destination": "https://fake",
"skipimageifexists": true,
"custom_callbacks": {
"on_detect": {
"uri": "http://10.16.42.75:5050",
"content-type": "application/json",
"body": {
"session_id": "100",
"session_init": "20201105T072403+0300",
"infected_items": "$infected"
}
},
"on_complete": {
"body": {
"session_id": "100",
},
"uri": "http://10.16.42.75:5050/on_complete",
}
}
  }
}
```

Дополнительные параметры запроса

Секция `params` может содержать следующие параметры:

- `destination` (необязательный параметр) – сервер, на который нужно скопировать проверенный образ.
- `skipimageifexists` (необязательный параметр) – не проверять и не копировать образ, если на сервере-приемнике уже есть образ с тем же именем и хеш-суммой SHA256. Этот параметр можно указать только при наличии параметра `destination`.
- `custom_callbacks` (необязательный параметр) – описываются запросы, которые должны быть отправлены после окончания проверки:
  - on_detect – запрос отправляется в случае нахождения угрозы.
  - on_complete – запрос отправляется всегда по окончании проверки.

В описании тела запроса можно указать переменную подстановки `$infected`, вместо которой подставляется список зараженный объектов.

Пример ответа:


```
{
  "completed": "Mon, 01 Mar 2021 07:13:49 GMT",
  "created": "Mon, 01 Mar 2021 07:13:42 GMT",
  "progress": 100,
  "scan_errors": [
{
"code": 500,
"message": "Unable to get images hash from destination registry"
}
  ],
  "scan_params": {
"destination": "https://fake",
"skipimageifexists": true
  },
  "scan_result": {
"jerbi/eicar:latest": {
"started": "2021-03-01 07:13:48",
"stopped": "2021-03-01 07:13:49",
```

```
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"infected"
  ]

}
```

Запрос на получение информации по сессиям проверки (GET)

Назначение

Получение информации о сессиях проверки.

Путь

http://<server>:<port>/scans[?force] – запрос на получение списка сессий

http://<server>:<port>/scans/<уникальный идентификатор сессии проверки>[?force] – запрос на получение информации по конкретной сессии

Параметры

KESL-контейнер хранит данные о сессиях проверки в памяти, записывая их в базу данных результатов проверок.

Необязательный параметр `?force` инициирует чтение информации из базы данных в случае, если несколько экземпляров KESL-контейнера работают с одной и той же базой данных. В случае отсутствия параметра будет выводиться информация только о тех сессиях, которые были инициированы конкретным экземпляром KESL-контейнера.

Запрос на получение списка сессий проверки

Путь

http://<server>:<port>/scans[?force]

Пример ответа:


```
{
  "629ae0a9-28de-4e2f-b130-67e87ba4d61d": {
"progress": 100,
"status": "completed"
  },
  "655b96fc-34ca-4915-9c41-d52724a277de": {
"progress": 100,
"status": "completed"
  },
  "7d27e9b4-a4d7-469b-bdcf-ebfe953498e4": {
"progress": 100,
"status": "completed"
  },
  "c32ca88f-2d24-47ec-b040-0540366bea4b": {
"progress": 100,
"status": "completed"
  },
  "df11ad81-26aa-42f9-94bb-39dee4304807": {
"progress": 0,
"status": "completed"
  },
  "fa25340f-4898-497f-ab59-8df494f4ea47": {
```

```
"progress": 100,
"status": "completed"
  }

}
```

Запрос на получение информации по конкретной сессии

Путь

http://<server>:<port>/scans/<уникальный идентификатор сессии проверки>[?force]

Пример ответа:

```
{
  "completed": "Mon, 01 Mar 2021 06:45:19 GMT",

  "created": "Mon, 01 Mar 2021 06:45:19 GMT",

  "progress": 100,

  "scan_result": {

"noname": {
"started": "2021-03-01 06:45:19",
"stopped": "2021-03-01 06:45:19",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/65b55d89-b758-4609-a2f3-f63ef839815d"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"infected"
  ]
```

```
}
```

Запрос на добавление сертификата реестра (POST)

Назначение

Добавление сертификата реестра без перезагрузки KESL-контейнера.

Путь

http://<server>:<port>/addcert

Заголовки запроса

Запрос содержит заголовок Content-Type.

Поддерживаемые значения:

- application/octet-stream – один файл сертификата;
- multipart/form-data – несколько файлов сертификатов.

Запрос на получение информации о состоянии KESL-контейнера (GET)

Назначение

Получение информации о текущем состоянии KESL-контейнера и тех параметров состояния приложения, от которых зависит состояние KESL-контейнера (состояние приложения, лицензии и баз данных).

Путь

http://<server>:<port>/status

Пример ответа:

```
{'product info': {'databases_date': '<дата выпуска баз>', 'databases_loaded': True,
'license_expiration': '<дата окончания срока действия лицензии>', 'license_info':
'The key is valid', 'policy': 'Not applied', 'version': '<версия приложения>'},
'status': 'service available'}
```

Возможные ошибки

Пример ошибки (приложение не запущено в KESL-контейнере):

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
```

Пример ошибки (не скачались базы приложения):

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': '<дата окончания срока действия лицензии>', 'license_info':
'Inconsistent update', 'policy': 'Not applied', 'version': '<версия приложения>'},
'status': 'service not available', 'status_reason': ['Databases not loaded', 'License
error: Inconsistent update']}
```

Пример ошибки (истекла дата окончания срока действия лицензии):

```
{'product info': {'databases_date': '<дата выпуска баз>', 'databases_loaded': True,
'license_expiration': '<дата окончания срока действия лицензии>', 'license_info':
'Expired', 'policy': 'Not applied', 'version': '<версия кесл>'}, 'status': 'service
not available', 'status_reason': ['License error: Expired']}
```

Обращение в Службу технической поддержки

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

Kaspersky предоставляет поддержку Kaspersky Endpoint Security в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

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

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

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

Портал Kaspersky CompanyAccount доступен на следующих языках:

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

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Получение информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас прислать *файл трассировки* или *файл дампа*.

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на устройстве, подробные отчеты работы компонентов приложения.

Во время работ по диагностике специалисты Службы технической поддержки могут попросить вас изменить параметры приложения:

- активировать функциональность получения расширенной диагностической информации;
- выполнить более тонкую настройку работы отдельных компонентов приложения, недоступную через стандартные средства пользовательского интерфейса;
- изменить параметры хранения полученной диагностической информации;
- настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав полученных в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Полученная расширенная диагностическая информация сохраняется на устройстве пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия требуется выполнять только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы приложения способами, не описанными в документации к приложению или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе приложения и операционной системы, снижению уровня защиты вашего устройства, а также к нарушению доступности и целостности обрабатываемой информации.

О файлах трассировки приложения

Файл трассировки приложения Kaspersky Endpoint Security позволяет отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка.

По умолчанию файлы трассировки приложения не создаются. Вы можете включать и выключать создание файлов трассировки приложения и настраивать уровень детализации файлов трассировки в командной строке с помощью общих параметров приложения, а также с помощью графического пользовательского интерфейса.

Если вы включили создание файлов трассировки приложения, по умолчанию файлы трассировки хранятся в директории /var/log/kaspersky/kesl/. Для доступа к этой директории требуются root-права.

Файлы трассировки хранятся на устройстве в течение всего времени использования приложения и удаляются без возможности восстановления при удалении приложения. Автоматическая отправка файлов трассировки в "Лабораторию Касперского" не выполняется.

Файлы трассировки хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Содержимое файлов трассировки приложения

В файлах трассировки содержатся следующие общие данные:

- время возникновения события;
- номер потока исполнения;
- компонент приложения, инициировавший событие;
- уровень важности события (информационное событие, предупреждение, критическое событие, ошибка);
- описание события, связанного с выполнением команды компонентом приложения, и результат выполнения этой команды.

В файлах трассировки могут храниться следующие данные в дополнение к общим данным:

- статусы компонентов приложения и их рабочие данные;
- данные о действиях пользователей в приложении;
- данные об оборудовании, установленном на устройстве;
- данные обо всех объектах и событиях операционной системы, а также данные о действиях пользователей;
- данные, содержащиеся в объектах операционной системы (например, содержимое файлов, в которых могут находиться персональные данные пользователей);
- данные о сетевом трафике (например, содержимое полей ввода на веб-сайте, которые могут включать данные банковской карты или любые другие конфиденциальные данные);
- данные, полученные с серверов "Лаборатории Касперского" (например, версия баз приложения);
- данные, полученные с серверов KATA.
- данные о потребленных ресурсах центрального процессора;
- данные о потребленных ресурсах оперативной памяти;
- данные об операциях чтения и записи файлов приложениями;
- данные о количестве кешированной информации, необходимой для работы приложения.

Настройка параметров трассировки приложения

Если вы управляете приложением Kaspersky Endpoint Security через Kaspersky Security Center, вы можете настраивать параметры трассировки приложения в параметрах политики Kaspersky Endpoint Security с помощью Web Console или Консоли администрирования.

Если вы управляете приложением через командную строку, вы можете настраивать параметры трассировки приложения в общих параметрах приложения.

Настройка параметров трассировки в Web Console

В Web Console вы можете настраивать параметры трассировки приложения в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Параметры трассировки и записи дампов**) (см. таблицу ниже).

Параметры трассировки приложения

Параметр	Описание
Путь к директории с файлами трассировки	Поле ввода пути к директории, в которой хранятся файлы трассировки. Значение по умолчанию: /var/log/kaspersky/kesl. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, под которой работает Kaspersky Endpoint Security. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права.
Максимальное количество файлов трассировки	Поле ввода максимального количества файлов трассировки приложения. Значение по умолчанию: 10.
Максимальный размер файла трассировки (МБ)	Поле ввода максимального размера файла трассировки приложения (в мегабайтах). Значение по умолчанию: 500.

Для применения параметров трассировки требуется перезапустить приложение.

Настройка параметров трассировки в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры трассировки приложения в свойствах политики (**Общие параметры** → **Параметры приложения**).

В блоке **Параметры трассировки и записи дампов** по ссылке **Настроить** открывается окно, в котором вы можете настроить параметры трассировки (см. таблицу ниже).

Параметры трассировки приложения

Параметр	Описание
Путь к директории с файлами трассировки	Поле ввода пути к директории, в которой хранятся файлы трассировки. Значение по умолчанию: /var/log/kaspersky/kesl. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, под которой работает Kaspersky Endpoint Security. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права.
Максимальный	Поле ввода максимального размера файла трассировки приложения (в мегабайтах).

размер файла трассировки (МБ)	Значение по умолчанию: 500.
Максимальное количество файлов трассировки	Поле ввода максимального количества файлов трассировки приложения. Значение по умолчанию: 10.

Для применения параметров трассировки требуется перезапустить приложение.

Настройка параметров трассировки в командной строке

В командной строке вы можете настраивать параметры трассировки приложения с помощью параметров `TraceLevel`, `TraceFolder`, `TraceMaxFileCount` и `TraceMaxFileSize` в общих параметрах приложения.

Параметр `TraceLevel` позволяет включить или выключить создание трассировки приложения и указать уровень детализации файлов трассировки. Параметр может принимать следующие значения:

- `Detailed` – создавать детализированный файл трассировки.
- `MediumDetailed` – создавать файл трассировки, содержащий информационные сообщения и сообщения об ошибках.
- `NotDetailed` – создавать файл трассировки, содержащий сообщения об ошибках.
- `None` (значение по умолчанию) – не создавать файл трассировки.

Параметр `TraceFolder` позволяет указать директорию, в которой хранятся файлы трассировки приложения. Значение по умолчанию: /var/log/kaspersky/kesl. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, под которой работает Kaspersky Endpoint Security. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права.

`TraceMaxFileCount` позволяет указать максимальное количество файлов трассировки приложения. Параметр может принимать значения от 1 до 10000. Значение по умолчанию: 10.

`TraceMaxFileSize` позволяет указать максимальный размер файла трассировки приложения (в мегабайтах). Параметр может принимать значения от 1 до 1000. Значение по умолчанию: 500.

Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

После изменения значений параметров `TraceFolder`, `TraceMaxFileCount`, `TraceMaxFileSize` требуется перезапустить приложение.

О файлах трассировки плагинов управления приложением

Автоматическая отправка файлов трассировки плагинов управления в "Лабораторию Касперского" не выполняется.

Файлы трассировки хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Файлы трассировки mmc-плагина управления

Если для управления приложением Kaspersky Endpoint Security вы используете Консоль администрирования, информация о событиях, возникающих во время работы mmc-плагина управления, может записываться в файл трассировки mmc-плагина Kaspersky Endpoint Security на устройстве, где установлен Сервер администрирования. Имя файла содержит номер версии приложения, дату и время создания файла и идентификатор процесса (PID). В этот файл записывается информация о событиях, возникающих во время работы mmc-плагина, в частности, о работе политик и задач.

По умолчанию файлы трассировки mmc-плагина не создаются. Вы можете создать файл трассировки mmc-плагина с помощью ключей реестра. За подробной информацией о том, как создать файлы трассировки, вы можете обратиться к специалистам Службы технической поддержки.

Все созданные файлы трассировки mmc-плагина расположены в папке, указанной пользователем во время настройки ключей реестра.

Файлы трассировки веб-плагина управления

Если для управления приложением Kaspersky Endpoint Security вы используете Web Console, информация о событиях, возникающих во время работы веб-плагина управления, может записываться в файлы трассировки веб-плагина.

Файлы трассировки веб-плагина создаются автоматически, если в мастере установки Web Console включена запись в журнал активности Web Console (см. подробнее в справке Kaspersky Security Center).

Файлы трассировки веб-плагина сохраняются в папке установки Web Console во вложенной папке logs.

Содержимое файлов трассировки плагинов управления

В файлах трассировки содержатся следующие общие данные:

- время возникновения события;
- номер потока исполнения;
- компонент приложения, инициировавший событие;
- уровень важности события (информационное событие, предупреждение, критическое событие, ошибка);
- описание события, связанного с выполнением команды компонентом приложения, и результат выполнения этой команды.

Помимо общих данных файлы трассировки могут содержать следующую информацию:

- персональные данные, в том числе фамилию, имя и отчество, если эти данные являются частью пути к файлам;
- имя учетной записи для входа в операционную систему, если имя учетной записи является частью имени файла.

О файлах дампа

Файл дампа содержит всю информацию о рабочей памяти процессов приложения Kaspersky Endpoint Security на момент создания файла дампа. По умолчанию файлы дампа не создаются. Вы можете включать и выключать запись дампов при сбое в работе приложения.

Если вы включили запись дампов, по умолчанию файлы дампа хранятся в директориях /var/opt/kaspersky/kesl/common/dumps и /var/opt/kaspersky/kesl/common/dumps-user.

Для доступа к файлам дампа требуются root-права.

Файлы дампа хранятся на устройстве в течение всего времени использования приложения и удаляются без возможности восстановления при удалении приложения. Автоматическая отправка файлов дампа в "Лабораторию Касперского" не выполняется.

Файлы дампа могут содержать персональные данные. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Включение и выключение записи дампов

Если вы управляете приложением Kaspersky Endpoint Security через Kaspersky Security Center, вы можете включать и выключать запись дампов в параметрах политики Kaspersky Endpoint Security с помощью Web Console или Консоли администрирования.

Если вы управляете приложением через командную строку, вы можете включать и выключать запись дампов с помощью конфигурационного файла kesl.ini.

Максимальное количество файлов дампов ограничено.

При некоторых параметрах операционной системы пользовательские файлы дампа могут не создаваться. Убедитесь, что значение параметра `sysctl kernel.yama.ptrace_scope=0`.

Включение и выключение записи дампов в Web Console

В Web Console вы можете включать и выключать запись дампов в свойствах политики (**Параметры приложения** → **Общие параметры** → **Параметры приложения**, блок **Параметры трассировки и записи дампов**) (см. таблицу ниже).

Параметры записи дампов

Параметр	Описание
Создавать файл дампа при сбое в работе приложения	Флажок включает или выключает создание файла дампа при сбое в работе приложения. По умолчанию флажок снят.
Путь к директории с файлами дампа	Поле ввода пути к директории, в которой хранятся файлы дампа. Размер поля ввода ограничен 128 символами.

	Значение по умолчанию: /var/opt/kaspersky/kesl/common/dumps.

Для применения параметров записи дампов требуется перезапустить приложение.

Включение и выключение записи дампов в Консоли администрирования

В Консоли администрирования вы можете включать и выключать запись дампов в свойствах политики (**Общие параметры → Параметры приложения**).

В блоке **Параметры трассировки и записи дампов** по ссылке **Настроить** открывается окно, в котором вы можете настроить параметры записи дампов (см. таблицу ниже).

Параметры записи дампов

Параметр	Описание
Создавать файл дампа при сбое в работе приложения	Флажок включает или выключает создание файла дампа при сбое в работе приложения. По умолчанию флажок снят.
Путь к директории с файлами дампа	Поле ввода пути к директории, в которой хранятся файлы дампа. Размер поля ввода ограничен 128 символами. Значение по умолчанию: /var/opt/kaspersky/kesl/common/dumps.

Для применения параметров записи дампов требуется перезапустить приложение.

Включение и выключение записи дампов в командной строке

Чтобы включить или выключить запись дампов с помощью конфигурационного файла kesl.ini:

1. Остановите Kaspersky Endpoint Security.
2. Откройте файл /var/opt/kaspersky/kesl/common/kesl.ini на редактирование.
3. В секции **[General]** установите значение параметра:
   - `CoreDumps=yes` – включить запись дампов при сбое в работе приложения.
   - `CoreDumps=no` – выключить запись дампов.
4. Если вы хотите изменить директорию, в которой сохраняются файлы дампа по умолчанию, укажите путь к директории в параметре `CoreDumpsPath`.
5. Запустите Kaspersky Endpoint Security.

Об удаленной диагностике устройства с помощью Kaspersky Security Center

В Kaspersky Security Center вы можете выполнять удаленную диагностику клиентских устройств. Процедура удаленной диагностики позволяет удаленно выполнять следующие операции:

- включать и выключать трассировку;
- изменять уровень трассировки;
- загружать файлы трассировки;
- загружать журнал удаленной установки приложения;
- загружать системные журналы событий (syslog);
- запускать, останавливать и перезапускать приложения.

Удаленная диагностика с помощью Web Console

Если вы управляете приложением Kaspersky Endpoint Security через Web Console, удаленная диагностика клиентского устройства выполняется в окне удаленной диагностики.

Чтобы открыть окно удаленной диагностики устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите устройство, для которого вы хотите выполнить удаленную диагностику, и нажмите на название устройства.

   Откроется окно свойств устройства.

3. На закладке **Дополнительно** выберите раздел **Удаленная диагностика**.

В окне удаленной диагностики устройства вы можете посмотреть журнал удаленной установки приложения.

Чтобы просмотреть журнал удаленной установки приложения на устройстве:

1. Откройте окно удаленной диагностики устройства.
2. На закладке **Журналы событий** в блоке **Файлы трассировки** нажмите на ссылку **Журналы удаленной установки**.

   Откроется окно **Журналы событий трассировки устройства**.

Подробнее об удаленной диагностике см. в справке Kaspersky Security Center.

Удаленная диагностика с помощью Консоли администрирования

Если вы управляете приложением Kaspersky Endpoint Security через Консоль администрирования, удаленная диагностика выполняется с помощью специальной утилиты удаленной диагностики Kaspersky Security Center, которая автоматически устанавливается на устройство совместно с Консолью администрирования.

Чтобы открыть главное окно утилиты удаленной диагностики устройства:

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.

2. В рабочей области выберите закладку **Устройства**.

3. В списке управляемых устройств выберите устройство, к которому вы хотите подключить утилиту удаленной диагностики, и в контекстном меню устройства выберите пункт **Внешние инструменты** → **Удаленная диагностика**.

   Откроется главное окно утилиты удаленной диагностики **Утилита удаленной диагностики Kaspersky Security Center**.

С помощью утилиты удаленной диагностики устройства вы можете посмотреть журнал удаленной установки приложения.

Чтобы просмотреть журнал удаленной установки приложения на устройстве:

1. Откройте главное окно утилиты удаленной диагностики устройства.

2. Если требуется, настройте параметры подключения утилиты к устройству. В главном окне утилиты удаленной диагностики нажмите на кнопку **Войти**.

3. В открывшемся окне в дереве объектов выберите папку **Журналы удаленной установки**.

Подробнее об утилите удаленной диагностики см. в справке 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 расположена в директории /opt/kaspersky/klnagent/bin в 32-битной операционной системе и в директории /opt/kaspersky/klnagent64/bin в 64-битной операционной системе. В зависимости от используемых ключей Агент администрирования выполняет следующие действия при запуске:

- записывает в файл журнала событий или выводит на экран значения параметров подключения Агента администрирования, установленного на клиентском устройстве, к Серверу администрирования;
- записывает в файл журнала событий или выводит на экран статистику Агента администрирования (с момента его последнего запуска) и результаты выполнения утилиты;
- предпринимает попытку установить соединение Агента администрирования с Сервером администрирования;
- если соединение установить не удалось, посылает ICMP-пакет для проверки статуса устройства, 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 событий. 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 расположена в директории /opt/kaspersky/klnagent/bin в 32-битной операционной системе и в директории /opt/kaspersky/klnagent64/bin в 64-битной операционной системе. В зависимости от используемых ключей Агент администрирования выполняет следующие действия при запуске:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;

- записывает в файл журнала событий или выводит на экран результаты выполнения операции.

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 выводятся в stdout.

- `-address <адрес сервера>` – адрес Сервера администрирования, используемого для подключения. Это может быть IP-адрес, NetBIOS или DNS-имя устройства.

- `-pn <номер порта>` – номер порта, по которому устанавливается незашифрованное соединение с Сервером администрирования. По умолчанию используется порт 14000.

- `-ps <номер SSL-порта>` – номер SSL-порта, по которому устанавливается зашифрованное соединение с Сервером администрирования по протоколу SSL. По умолчанию используется порт 13000.

- `-nossl` – использовать незашифрованное соединение с Сервером администрирования. Если этот ключ не указан, Агент соединяется с Сервером администрирования через зашифрованный протокол SSL.

- `-cert <путь к файлу сертификата>` – использовать указанный файл сертификата для аутентификации доступа к новому Серверу администрирования. Если ключ не используется, Агент администрирования получит сертификат при первом подключении к Серверу администрирования.

- `-silent` – запустить утилиту в неинтерактивном режиме. Использование ключа может быть полезно, например, при запуске утилиты из сценария запуска при регистрации пользователя.

- `-dupfix` – этот файл ключа используется, если способ установки Агента администрирования отличается от способа установки в составе комплекте поставки, например, восстановление с диска.

- `-cloningmode 1` – перейти в режим клонирования.

- `-cloningmode 0` – выйти из режима клонирования.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст справки.

Приложение 1. Оптимизация потребления ресурсов

При проверке объектов Kaspersky Endpoint Security использует ресурсы процессора, ввод-вывод дисковой подсистемы и оперативную память.

Чтобы посмотреть потребление ресурсов приложением, выполните следующую команду:

```
top -bn1|grep kesl
```

Выполнять команду требуется в момент нагрузки на систему.

Вывод команды показывает количество потребляемой памяти и занимаемого процессорного времени:

```
651 root 20 0 3014172 2.302g 154360 S 120.0 30.0 0:32.80 kesl
```

В столбце 6 отображается количество резидентной памяти – `2.302g`.

В столбце 9 отображается процент использования ядер процессора – 120.0, где каждое ядро принимается за 100 процентов. Таким образом, 120% означает, что одно ядро занято полностью, а второе – на 20%.

Если работа Kaspersky Endpoint Security при проверке объектов критически замедляет работу системы, требуется провести настройку приложения для оптимизации потребления ресурсов системы.

Определение задачи, которая занимает ресурсы

Для того чтобы определить, какая задача или задачи приложения занимают ресурсы системы, требуется разделить потребление ресурсов задачей Защита от файловых угроз (тип OAS) и задачами проверки по требованию (типы ODS и ContainerScan).

Если приложение находится под управлением политики Kaspersky Security Center, требуется на время проведения исследования разрешить управление локальными задачами.

Анализ работы задачи Защита от файловых угроз

Чтобы проанализировать работу задачи Защита от файловых угроз:

1. Остановите все задачи проверки и мониторинга.
2. Убедитесь, что задачи проверки по требованию не будут запущены во время проверки или не имеют расписания. Вы можете сделать это через Kaspersky Security Center или локально, выполнив следующие действия:

a. Получите список всех задач приложения, выполнив следующую команду:

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

b. Получите параметры расписания задачи поиска вредоносного ПО, выполнив следующую команду:

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

Если команда выводит `RuleType=Manual`, то задача запускается только вручную.

c. Получите параметры расписания всех ваших задач поиска вредоносного ПО и выборочной проверки, если такие были созданы, и укажите им запуск вручную, выполнив следующую команду:

```
kesl-control --set-schedule <ID задачи> RuleType=Manual
```

3. Включите создание файлов трассировки приложения с высоким уровнем детализации, выполнив следующую команду:

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

4. Запустите задачу Защита от файловых угроз, если она не была запущена, выполнив следующую команду:

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

5. Создайте нагрузку на систему в том же режиме, который вызвал проблемы с производительностью, достаточно нескольких часов.

Под нагрузкой приложение записывает много информации в файлы трассировки, при этом по умолчанию хранится 5 файлов по 500 МБ, поэтому старая информация будет перезаписываться. Если проблемы с производительностью и потреблением ресурсов перестали проявляться, значит, скорее всего, проблемы вызывают задачи проверки по требованию и можно перейти к анализу работы задач проверки с типами ContainerScan и ODS.

6. Выключите создание файлов трассировки приложения, выполнив следующую команду:

```
kesl-control --set-app-settings TraceLevel=None
```

7. Определите список объектов, которые были проверены наибольшее количество раз, выполнив следующую команду:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -r|less
```

Результат загружается в приложение просмотра текста less, где в самом начале отображаются те объекты, которые были проверены наибольшее количество раз.

8. Определите, являются ли опасными объекты, которые были проверены наибольшее количество раз. В случае затруднения обратитесь в Службу технической поддержки.

Например, неопасными можно признать директории и файлы журналов, если запись в них ведет доверенный процесс, файлы баз данных.

9. Запишите пути к неопасным, по вашему мнению, объектам, они потребуются в дальнейшем для настройки исключений из проверки.

10. Если в системе осуществляется частая запись файлов различными сервисами, такие файлы будут повторно проверяться в отложенной очереди. Определите список путей, которые были проверены в отложенной очереди наибольшее количество раз, выполнив следующую команду:

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $9}' | sort | uniq -c | sort -k1 -n -r
```

Файлы, проверенные наибольшее количество раз, будут отображаться в начале списка.

11. Если счетчик по одному файлу превышает несколько тысяч за несколько часов, определите, можно ли доверять этому файлу, чтобы исключить его из проверки.

Логика определения такая же, как и для предыдущего исследования (см. п. 8): файлы журналов можно признать неопасными, так как они не могут быть запущены.

12. Даже если некоторые файлы исключены из проверки постоянной защитой, они все равно могут перехватываться приложением. Если исключение определенных файлов из постоянной защиты не приносит существенного прироста производительности, вы можете полностью исключить из перехвата приложением точку монтирования, где расположены эти файлы. Для этого выполните следующие действия:

    a. Получите список файлов, перехваченных приложением, выполнив следующую команду:

    ```
    grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | sort | uniq -c | sort -k1 -n -r
    ```

    b. С помощью полученного списка определите пути, по которым происходит большое количество перехватов файловых операций, и настройте исключения из перехвата.

Анализ работы задач проверки по требованию

Также большое потребление ресурсов может быть вызвано использованием задач с типами ODS и ContainerScan. Следуйте следующим рекомендациям по использованию задач с типом ODS:

- Убедитесь, что не выполняется запуск нескольких задач проверки по требованию одновременно. Приложение позволяет работать в таком режиме, но потребление ресурсов может сильно увеличиться. Проверьте расписание всех задач с типами ODS и ContainerScan локально (как описано для задачи Защита от файловых угроз) или через Kaspersky Security Center.
- Запускайте проверку во время наименьшей нагрузки на сервер.
- Убедитесь, что по указанному пути проверки нет примонтированных удаленных ресурсов (SMB / NFS). Если задача состоит в проверке удаленного ресурса и нет возможности выполнять ее непосредственно на сервере, предоставляющем ресурс, не выполняйте проверку на серверах с критическими сервисами, так как такая задача может выполняться достаточно долго (в зависимости от скорости соединения и количества файлов).
- Выполните оптимизацию параметров задачи проверки по требованию перед запуском.

Настройка задачи Защита от файловых угроз

Если после выполнения анализа работы задачи Защита от файловых угроз вы сформировали список директорий и файлов, которые можно исключить из проверки задачи, вам нужно добавить их в исключения.

Исключения из проверки

Чтобы исключить директорию /tmp/logs и все поддиректории и файлы рекурсивно, выполните следующую команду:

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

Чтобы исключить конкретный файл или файлы по маске в директории /tmp/logs, выполните следующую команду:

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

Чтобы исключить по рекурсивной маске все файлы с расширением .log в директории /tmp/ и поддиректориях, выполните следующую команду:

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Исключения из перехвата

Если вы хотите исключить файлы определенной директории не только из проверки, но и из перехвата, вы можете исключить точку монтирования целиком.

Чтобы исключить точку монтирования целиком:

1. Если директория не является точкой монтирования, нужно создать из нее точку монтирования. Например, чтобы создать точку монтирования из директории /tmp, выполнив следующую команду:

   ```
   mount --bind /tmp/ /tmp
   ```

2. Чтобы точка монтирования сохранилась после перезагрузки сервера, добавьте в файл /etc/fstab следующую строку:

   ```
   /tmp /tmp none defaults,bind 0 0
   ```

3. Добавьте директорию /tmp в глобальные исключения, выполнив следующую команду:

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

4. Если требуется добавить несколько директорий, увеличивайте счетчик item_0000 на единицу (item_0001, item_0002 и так далее).

Исключать точки монтирования также рекомендуется, если это примонтированный удаленный ресурс с нестабильным или медленным соединением.

Изменение типа проверки

По умолчанию задача Защита от файловых угроз может проверять файлы при открытии и закрытии. Если в ходе анализа работы задачи Защита от файловых угроз было выявлено слишком много записываемых файлов, вы можете перевести задачу в режим работы только при открытии файлов, выполнив следующую команду:

```
kesl-control --set-set 1 ScanByAccessType=Open
```

При таком режиме работы изменения, внесенные в файл после открытия, не будут проверяться до следующего обращения к файлу.

Настройка задачи проверки по требованию

Исключения из проверки

Для задач проверки по требованию с типами ODS и ContainerScan вы можете настроить исключения из проверки. Настройка выполняется аналогично настройке исключений из проверки для задачи Защита от файловых угроз.

Параметры исключений из проверки для одной задачи проверки не действуют на другие задачи проверки. Для каждой задачи проверки требуется настроить свои исключения.

Ограничение использования памяти для распаковки архивов

Задача проверки по требованию при рекурсивной проверке во время проверки архивов будет распаковывать их, используя оперативную память. В приложении предусмотрена возможность регулировать размер оперативной памяти, используемой приложением при проверке файлов, с помощью параметра `ScanMemoryLimit` в конфигурационном файле kesl.ini. Значение параметра по умолчанию равно 8192 МБ. Минимальное значение параметра: 2 МБ. Если указанное значение параметра меньше 2 МБ, приложение будет использовать минимальное значение (2 МБ). Если указанное значение параметра превышает размер оперативной памяти системы, приложение будет использовать до 25% оперативной памяти. Это значение изменить невозможно.

Установка ограничения на использование памяти приложением

Вы можете ограничивать количество оперативной памяти, которое приложение Kaspersky Endpoint Security использует во время выполнения задач проверки с типами OAS, ODS и ContainerScan.

О граничение на использование памяти может быть полезным для систем с большим объемом оперативной памяти (более 5 ГБ).

Вы можете регулировать размер оперативной памяти, используемой приложением при проверке файлов, с помощью параметра `ScanMemoryLimit` в конфигурационном файле kesl.ini. Значение параметра по умолчанию: 8192 МБ. Минимальное значение параметра: 2 МБ. Если указанное значение параметра меньше 2 МБ, приложение будет использовать минимальное значение (2 МБ). Если указанное значение параметра превышает размер оперативной памяти устройства, приложение будет использовать до 25% оперативной памяти. Это значение изменить невозможно.

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

Чтобы указать ограничение на использование памяти при проверке файлов:

1. Остановите Kaspersky Endpoint Security.
2. Откройте файл /var/opt/kaspersky/kesl/common/kesl.ini на редактирование.
3. В секции **[General]**: укажите нужное количество оперативной памяти в значении параметра `ScanMemoryLimit`:

   `ScanMemoryLimit=< количество памяти в мегабайтах >`
4. Запустите Kaspersky Endpoint Security.

Ограничение на использование памяти при проверке файлов изменится при перезапуске приложения.

Приложение 2. Команды управления Kaspersky Endpoint Security

Управление приложением Kaspersky Endpoint Security в командной строке выполняется с помощью команд управления Kaspersky Endpoint Security.

Вы можете посмотреть справку по командам управления с помощью команды:

```
kesl-control --help <префикс группы команд>
```

где <префикс группы команд> может принимать следующие значения:

- -A – команды управления контролем приложений.
- -B – команды управления резервным хранилищем.
- -C – команды управления общими параметрами проверки контейнеров.
- -D – команды управления контролем устройств.
- -E – команды управления событиями приложения.
- -F – команды управления сетевым экраном.
- -H – команды управления заблокированными устройствами.
- -L – команды управления лицензионными ключами.
- -N – команды управления параметрами проверки защищенных соединений.
- -R – команды управления параметрами интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA) и с Kaspersky Endpoint Detection and Response Optimum.
- -S – команды статистики.
- -T – команды управления задачами и параметрами приложения.
- -U – команды управления пользователями и ролями пользователей.
- -V – команды приложения в режиме Легкого агента для защиты виртуальных сред.
- -W – команды вывода событий.

Команды управления параметрами и задачами приложения

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

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

-N – префикс, указывающий, что команда принадлежит к группе команд управления параметрами проверки защищенных соединений.

Команда kesl-control --export-settings

Команда позволяет вывести в консоль или экспортировать в конфигурационный файл все параметры приложения (включая общие параметры проверки контейнеров, параметры проверки защищенных соединений, общие параметры приложения и параметры задач).

Синтаксис команды

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

Аргументы и ключи

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

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kesl-control --import-settings

Команда позволяет импортировать из конфигурационного файла все параметры приложения (включая общие параметры проверки контейнеров, параметры проверки защищенных соединений, общие параметры приложения и параметры задач).

Синтаксис команды

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

Аргументы и ключи

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

`--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команда kesl-control --update-application

Команда позволяет установить загруженное обновление модулей приложения.

> Команда может быть выполнена, только если приложение используется в стандартном режиме.

Синтаксис команды

```
kesl-control [-T] --update-application
```

Команды управления общими параметрами приложения

Команда kesl-control --get-app-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения общих параметров приложения.

Синтаксис команды

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

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены общие параметры приложения. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kesl-control --set-app-settings

Команда позволяет устанавливать значения общих параметров приложения с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

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

Задать параметры с помощью конфигурационного файла:

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

Аргументы и ключи

`<имя параметра>=<значение параметра>` – имя и значение одного из общих параметров приложения.

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

`--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команды управления параметрами задач

Команда kesl-control --get-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения параметров указанной задачи.

Синтаксис команды

```
kesl-control [-T] --get-settings <идентификатор/имя задачи> [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены параметры задачи. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kesl-control --set-settings

Команда позволяет устанавливать значения параметров указанной задачи с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kesl-control [-T] --set-settings <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>] [--add-path <путь>] [--del-path <путь>] [--add-exclusion <путь>] [--del-exclusion <путь>]
```

Задать параметры с помощью конфигурационного файла:

```
kesl-control [-T] --set-settings <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`<имя параметра>=<значение параметра>` – имя и значение одного из параметров задачи.

`--add-path <путь>` – добавить путь к директории с проверяемыми объектами.

`--del-path <путь>` – удалить путь к директории с проверяемыми объектами.

`--add-exclusion <путь>` – добавить путь к директории с объектами, которые нужно исключить из проверки.

`--del-exclusion <путь>` – удалить путь к директории с исключаемыми объектами.

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

`--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команда kesl-control --set-to-default

Команда позволяет восстановить значения по умолчанию для параметров указанной задачи.

Синтаксис команды

```
kesl-control [-T] --set-settings <идентификатор/имя задачи> --set-to-default
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда kesl-control --get-schedule

Команда позволяет вывести в консоль или в конфигурационный файл текущее расписание запуска указанной задачи.

Синтаксис команды

```
kesl-control [-T] --get-schedule <идентификатор/имя задачи> [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены параметры расписания задачи. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kesl-control --set-schedule

Команда позволяет устанавливать расписание указанной задачи с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kesl-control [-T] --set-schedule <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kesl-control [-T] --set-schedule <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`<имя параметра>=<значение параметра>` – имя и значение одного из параметров расписания задач.

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

`--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команды управления задачами

Команда kesl-control --get-task-list

Команда позволяет вывести список существующих задач приложения.

Синтаксис команды

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

Аргументы и ключи

`--json` – выводить параметры в формате JSON.

Команда kesl-control --get-task-state

Команда позволяет вывести состояние указанной задачи.

Синтаксис команды

```
kesl-control [-T] --get-task-state <идентификатор/имя задачи> [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`--json` – выводить параметры в формате JSON.

Команда kesl-control --create-task

Команда позволяет создать задачу указанного типа с параметрами по умолчанию или с параметрами, указанными в конфигурационном файле.

Синтаксис команды

Создать задачу с параметрами по умолчанию:

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

Создать задачу с параметрами из конфигурационного файла:

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

Аргументы и ключи

`<имя задачи>` – имя, которое вы задаете для новой задачи.

`<тип задачи>` – обозначение типа создаваемой задачи.

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, параметры из которого будут использоваться при создании задачи.

`--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команда kesl-control --delete-task

Команда позволяет удалить задачу.

Синтаксис команды

```
kesl-control [-T] --delete-task <идентификатор/имя задачи>
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда kesl-control --start-task

Команда позволяет запустить задачу.

Синтаксис команды

```
kesl-control [-T] --start-task <идентификатор/имя задачи> [-W] [--progress]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`[-W]` – включить вывод текущих событий.

`[--progress]` – отображать ход выполнения задачи.

Команда kesl-control --stop-task

Команда позволяет остановить задачу.

Синтаксис команды

```
kesl-control [-T] --stop-task <идентификатор/имя задачи> [-W]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`[-W]` – включить вывод текущих событий.

Команда kesl-control --suspend-task

Команда позволяет приостановить задачу.

Синтаксис команды

```
kesl-control [-T] --suspend-task <идентификатор/имя задачи>
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда kesl-control --resume-task

Команда позволяет возобновить выполнение задачи.

Синтаксис команды

```
kesl-control [-T] --resume-task <идентификатор/имя задачи>
```

Аргументы и ключи

< идентификатор/имя задачи > – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда kesl-control --scan-file

Команда позволяет создать и запустить задачу выборочной проверки.

Синтаксис команды

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

Аргументы и ключи

< путь > – путь к файлу или директории, которые нужно проверить. Вы можете указать несколько путей, разделяя их пробелами.

`--action < действие >` – действие, которое приложение будет выполнять над зараженными объектами. Если вы не укажете ключ `--action`, приложение будет выполнять рекомендуемое действие.

Команда kesl-control --scan-container

Команда позволяет создать и запустить задачу выборочной проверки контейнера или образа.

Синтаксис команды

```
kesl-control [-T] --scan-container < контейнер/образ [: тег ]>
```

Аргументы и ключи

< контейнер/образ [: тег]> – имя или идентификатор контейнера или образа. Для проверки нескольких объектов можно использовать маски.

Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ * вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file*/` или `/dir/file**/`.

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

Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

Команды управления общими параметрами проверки контейнеров

Команда kesl-control --get-container-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения общих параметров проверки контейнеров.

Синтаксис команды

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

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены общие параметры проверки контейнеров. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kesl-control --set-container-settings

Команда позволяет устанавливать значения общих параметров проверки контейнеров с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

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

Задать параметры с помощью конфигурационного файла:

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

Аргументы и ключи

`<имя параметра>=<значение параметра>` – имя и значение одного из общих параметров проверки контейнеров.

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого в приложение будут импортированы общие параметры проверки контейнеров.

`--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команды управления параметрами проверки защищенных соединений

-N – префикс, указывающий, что команда принадлежит к группе команд управления параметрами проверки защищенных соединений.

Команда kesl-control -N --query

Команда позволяет выводить списки исключений из проверки защищенных соединений:

- список исключений, добавленных пользователем;
- список исключений, добавленных приложением;
- список исключений, полученных из баз приложения.

Синтаксис команды

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

kesl-control -N --query auto

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

Команда kesl-control --clear-web-auto-excluded

Команда позволяет очистить список доменов, которые приложение автоматически исключило из проверки.

Синтаксис команды

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

Команда kesl-control --get-net-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения параметров проверки защищенных соединений.

Синтаксис команды

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

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу, в который будут выведены параметры проверки защищенных соединений. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kesl-control --set-net-settings

Команда позволяет устанавливать значения параметров проверки защищенных соединений с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kesl-control [-N] --set-net-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

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

Аргументы и ключи

`<имя параметра>=<значение параметра>` – имя и значение одного из параметров проверки защищенных соединений.

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры проверки защищенных соединений.

`--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команда kesl-control --add-certificate

Команда позволяет добавить сертификат в список сертификатов, которые приложение будет считать доверенными.

Синтаксис команды

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

Аргументы и ключи

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

Команда kesl-control --remove-certificate

Команда позволяет удалить сертификат из списка доверенных сертификатов.

Синтаксис команды

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

Команда kesl-control --list-certificates

Команда позволяет вывести список доверенных сертификатов.

Синтаксис команды

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

Команды статистики

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

Команда kesl-control --app-info

Команда позволяет вывести информацию о приложении.

Синтаксис команды

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

Аргументы и ключи

`--json` – выводить параметры в формате JSON.

Команда kesl-control --omsinfo

Команда позволяет создать файл формата JSON для интеграции с Microsoft Operations Management Suite.

Синтаксис команды

```
kesl-control [-S] --omsinfo --file <путь к файлу>
```

Команды вывода событий

Команда kesl-control -W

Команда включает вывод текущих событий приложения. Команда возвращает название события и дополнительную информацию о событии. Вы можете использовать команду для вывода всех текущих событий приложения или только событий, связанных с запущенной задачей.

Синтаксис команды

```
kesl-control -W [--query "<условия фильтра>"]
```

Аргументы и ключи

`<условия фильтра>` – одно или несколько логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`, для вывода определенных текущих событий.

Команды управления событиями приложения

-E – префикс, указывающий, что команда принадлежит к группе команд управления событиями приложения.

Команда kesl-control -E

Команда позволяет вывести информацию обо всех событиях из журнала событий приложения. С помощью утилиты `less` вы можете перемещаться по списку отображаемых событий.

Синтаксис команды

```
kesl-control -E
```

Команда kesl-control -E --query

Команда позволяет вывести информацию о событиях из журнала событий приложения. С помощью утилиты `less` вы можете перемещаться по списку отображаемых событий. Вы можете использовать фильтр для вывода определенных событий, а также выводить список событий в указанный файл.

Синтаксис команды

```
kesl-control -E --query "<условия фильтра>" [--db <файл базы данных>] [-n <количество>]
[--file <путь к файлу>] [--json] [--reverse]
```

Аргументы и ключи

`<файл базы данных>` – полный путь к файлу базы данных журнала событий, из которого вы хотите вывести события. По умолчанию приложение сохраняет информацию о событиях в базе данных /var/opt/kaspersky/kesl/private/storage/events.db. Расположение базы данных определяется общим параметром приложения `EventsStoragePath`.

`<условия фильтра>` – одно или несколько логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.

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

`--file <путь к файлу>` – полный путь к файлу, в который вы хотите вывести события. Если вы укажете имя файла, не указав путь 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, файл не будет создан.

Если вы не укажете ключ `--file`, список событий будет выведен в консоль.

`--json` – выводить события в формате JSON.

`--reverse` – выводить события в обратном порядке (от самого нового события наверху к более старым внизу).

Команды управления лицензионными ключами

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

Команды добавления и удаления лицензионных ключей могут быть выполнены, только если приложение используется в стандартном режиме. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, команды управления лицензионными ключами завершаются с ошибкой. Вы активируете приложение в составе решения Kaspersky Security для виртуальных сред Легкий агент, отдельно активировать приложение не требуется.

Команда kesl-control --add-active-key

Команда позволяет добавить в приложение активный лицензионный ключ с помощью файла ключа или кода активации.

С помощью этой команды вы можете добавить как активный лицензионный ключ приложения, так и активный лицензионный ключ EDR Optimum. Указывать тип ключа в команде не требуется.

Синтаксис команды

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

kesl-control [-L] --add-active-key <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.

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

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

Команда kesl-control --add-reserve-key

Команда позволяет добавить в приложение резервный лицензионный ключ с помощью файла ключа или кода активации.

С помощью этой команды вы можете добавить как резервный лицензионный ключ приложения, так и резервный лицензионный ключ EDR Optimum. Указывать тип ключа в команде не требуется.

Если активный ключ еще не добавлен в приложение на устройстве, команда завершается с ошибкой.

Синтаксис команды

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

kesl-control [-L] --add-reserve-key <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.

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

```
kesl-control --add-reserve-key /home/test/00000002.key
```

Команда kesl-control --remove-active-key

Команда позволяет удалить активный лицензионный ключ.

Синтаксис команды

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

Аргументы и ключи

`--edr-optimum` – удалить активный лицензионный ключ EDR Optimum. Если вы не укажете ключ `--edr-optimum`, будет удален активный лицензионный ключ приложения Kaspersky Endpoint Security.

Команда kesl-control --remove-reserve-key

Команда позволяет удалить резервный лицензионный ключ.

Синтаксис команды

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

Аргументы и ключи

`--edr-optimum` – удалить резервный лицензионный ключ EDR Optimum. Если вы не укажете ключ `--edr-optimum`, будет удален резервный лицензионный ключ приложения Kaspersky Endpoint Security.

Команда kesl-control -L --query

Команда `-L --query` позволяет вывести информацию о лицензии, по которой активировано приложение, и об используемых лицензионных ключах.

Синтаксис команды

```
kesl-control -L --query [--json]
```

Аргументы и ключи

`--json` – выводить данные в формате JSON.

Команда kesl-control --load-mdr-blob

Команда `--load-mdr-blob` позволяет загрузить конфигурационный файл BLOB, необходимый для интеграции с Kaspersky Managed Detection and Response.

Синтаксис команды

```
kesl-control [-L] --load-mdr-blob <путь к конфигурационному файлу MDR BLOB>
```

Команда kesl-control --remove-mdr-blob

Команда `--remove-mdr-blob` позволяет удалить конфигурационный файл BLOB, необходимый для интеграции с Kaspersky Managed Detection and Response.

Синтаксис команды

```
kesl-control [-L] --remove-mdr-blob
```

Команды управления сетевым экраном

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

Команда kesl-control --add-rule

Команда позволяет добавить новое сетевое пакетное правило.

Синтаксис команды

```
kesl-control [-F] --add-rule [--name <название правила>] [--action <действие>] [--protocol <протокол>] [--direction <направление>] [--remote <удаленный адрес>[:<диапазон портов>]] [--local <локальный адрес>[:<диапазон портов>]] [--at <индекс>]
```

Аргументы и ключи

`--name <название правила>` – название сетевого пакетного правила.

`--action <действие>` – действие, применяемое к соединениям, указанным в сетевом пакетном правиле.

`--protocol <протокол>` – тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность.

`--direction <направление>` – направление отслеживаемой сетевой активности.

`--remote <удаленный адрес>[:<диапазон портов>]` – сетевой адрес удаленного устройства.

`--local <локальный адрес>[:<диапазон портов>]` – сетевой адрес устройства с установленным приложением Kaspersky Endpoint Security.

`--at <индекс>` – порядковый номер правила в списке сетевых пакетных правил. Если ключ `--at` не указан или его значение больше количества правил в списке, новое правило добавляется в конец списка.

Для параметров, значения которых вы не указали в команде, устанавливаются значения по умолчанию.

Команда kesl-control --del-rule

Команда позволяет удалить сетевое пакетное правило с указанным названием или с указанным индексом в списке правил.

Синтаксис команды

```
kesl-control [-F] --del-rule --name <название правила>

kesl-control [-F] --del-rule --index <индекс>
```

Аргументы и ключи

`--name <название правила>` – название сетевого пакетного правила.

`--index <индекс>` – порядковый номер правила в списке сетевых пакетных правил.

Команда kesl-control --move-rule

Команда позволяет изменить приоритет выполнения сетевого пакетного правила.

Синтаксис команды

```
kesl-control [-F] --move-rule --name <название правила> --at <индекс>

kesl-control [-F] --move-rule --index <индекс> --at <индекс>
```

Аргументы и ключи

`--name <название правила>` – название сетевого пакетного правила.

`--index <индекс>` – текущий порядковый номер правила в списке сетевых пакетных правил.

`--at <индекс>` – новый порядковый номер правила в списке сетевых пакетных правил.

Команда kesl-control --add-zone

Команда позволяет добавить адрес в сетевую зону.

Синтаксис команды

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

Аргументы и ключи

`--zone <зона>` – предустановленное имя сетевой зоны.

`--address <адрес>` – сетевой адрес или подсеть.

Команда kesl-control --del-zone

Команда позволяет удалить адрес из сетевой зоны.

Синтаксис команды

```
kesl-control [-F] --del-zone --zone <зона> --address <адрес>

kesl-control [-F] --del-zone --zone <зона> --index <индекс адреса>
```

Аргументы и ключи

`--zone <зона>` – предустановленное имя сетевой зоны.

`--address <адрес>` – сетевой адрес или подсеть.

`--index <индекс адреса>` – порядковый номер адреса в сетевой зоне.

Команда kesl-control -F --query

Команда позволяет посмотреть правила сетевого экрана, созданные с помощью приложения Kaspersky Endpoint Security.

Синтаксис команды

```
kesl-control -F --query
```

Команды управления заблокированными устройствами

-H –префикс, указывающий, что команда принадлежит к группе команд управления устройствами, заблокированными Защитой от шифрования и Защитой от сетевых угроз.

Команда kesl-control --get-blocked-hosts

Команда позволяет вывести в консоль список заблокированных устройств.

Синтаксис команды

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

Команда kesl-control --allow-hosts

Команда позволяет разблокировать заблокированные устройства.

Синтаксис команды

```
kesl-control [-H] --allow-hosts <адрес>
```

Аргументы и ключи

< адрес > – IP-адрес устройства или подсети (IPv4/IPv6, включая адреса в короткой форме). Вы можете указать несколько IP-адресов устройств или подсетей, разделяя их пробелами.

Команды управления Контролем устройств

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

Команда kesl-control --get-device-list

Команда позволяет вывести в консоль список устройств, которые установлены на клиентском устройстве или подключены к нему.

Синтаксис команды

```
kesl-control [-D] --get-device-list [--json]
```

Аргументы и ключи

`--json` – выводить данные в формате JSON.

Команды управления Контролем приложений

-A – префикс, указывающий, что команда принадлежит к группе команд управления контролем приложений.

Команда kesl-control --get-app-list

Команда позволяет вывести список приложений, обнаруженных на клиентском устройстве во время выполнения задачи Инвентаризация.

Синтаксис команды

```
kesl-control [-A] --get-app-list [--json]
```

Аргументы и ключи

`--json` – выводить данные в формате JSON.

Команда kesl-control --get-categories

Команда позволяет вывести список созданных категорий контроля приложений.

Синтаксис команды

```
kesl-control [-A] --get-categories [--names < название категории 1 > < название категории 2 > ... < название категории N >] [--file < путь к конфигурационному файлу >] [--json]
```

Аргументы и ключи

<название категории 1> <название категории 2> ... <название категории N> – названия категорий, информацию о которых вы хотите просмотреть. Если вы хотите просмотреть информацию о нескольких категориях, укажите названия категорий через пробел.

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу формата JSON, в который будут выведены параметры.

--json – выводить данные в формате JSON.

Команда kesl-control --set-categories

Команда позволяет создать или изменить список созданных категорий контроля приложений.

Синтаксис команды

```
kesl-control [-A] --set-categories [--names <название категории 1> <название категории 2> ... <название категории N>] --file <путь к конфигурационному файлу>
```

Аргументы и ключи

<название категории 1> <название категории 2> ... <название категории N> – названия категорий, информацию о которых вы хотите изменить. Если вы хотите изменить информацию о нескольких категориях, укажите названия категорий через пробел. Если вы не укажите название категории, она будет удалена из списка.

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу с параметрами категорий.

Команда kesl-control --get-settings 21

Команда позволяет вывести список созданных правил контроля приложений.

Синтаксис команды

```
kesl-control --get-settings 21 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

--file <путь к конфигурационному файлу> – полный путь к конфигурационному файлу, в который будут выведены параметры.

--json – выводить данные в формате JSON.

Команда kesl-control --set-settings 21

Команда позволяет изменить список созданных категорий приложений и правил контроля приложений.

Синтаксис команды

```
kesl-control --set-settings 21 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

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

`--json` – импорт данных из файла в формате JSON.

Команда kesl-control --set-to-default 21

Команда позволяет удалить список категорий приложений и правил контроля приложений.

Синтаксис команды

```
kesl-control --set-settings 21 --set-to-default
```

Команды управления Веб-Контролем

Команда kesl-control --get-settings 26

Команда позволяет вывести список настроенных параметров Веб-Контроля.

Синтаксис команды

```
kesl-control --get-settings 26 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут выведены параметры.

`--json` – выводить данные в формате JSON.

Команда kesl-control --set-settings 26

Команда позволяет изменить список настроенных параметров Веб-Контроля.

Синтаксис команды

```
kesl-control --set-settings 26 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

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

`--json` – импорт данных из файла в формате JSON.

Команда kesl-control --set-to-default 26

Команда позволяет удалить настроенные параметры и восстановить значения параметров Веб-Контроля до правила по умолчанию.

Синтаксис команды

```
kesl-control --set-settings 26 --set-to-default
```

Команды управления резервным хранилищем

-B – префикс, указывающий, что команда принадлежит к группе команд управления резервным хранилищем.

Команда kesl-control --mass-remove

Команда позволяет удалить из резервного хранилища все или только указанные объекты.

Синтаксис команды

Удалить все объекты:

```
kesl-control [-B] --mass-remove
```

Удалить объекты, соответствующие условиям фильтра:

```
kesl-control [-B] --mass-remove --query "< условия фильтра >"
```

Аргументы и ключи

`< условия фильтра >` – одно или несколько логических выражений в формате `< поле > < операция сравнения > '< значение >'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.

Команда kesl-control -B --query

Команда позволяет вывести информацию об объектах резервного хранилища.

Синтаксис команды

Вывести информацию обо всех объектах резервного хранилища:

```
kesl-control -B --query [-n < количество >] [--json] [--reverse]
```

Вывести информацию об объектах резервного хранилища, соответствующих условиям фильтра:

```
kesl-control -B --query ["< условия фильтра >"] [-n < количество >] [--json] [--reverse]
```

Аргументы и ключи

`< условия фильтра >` – одно или несколько логических выражений в формате `< поле > < операция сравнения > '< значение >'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса. Если вы не укажете условия фильтра, приложение выведет информацию обо всех объектах резервного хранилища.

`< количество >` – количество последних объектов из хранилища, которые нужно вывести. Если вы не укажете ключ `-n`, будут выведены последние 30 объектов. Чтобы показать все объекты, укажите значение 0.

`--json` – выводить данные в формате JSON.

Команда kesl-control --restore

Команда позволяет восстановить объект из резервного хранилища.

Синтаксис команды

```
kesl-control [-B] --restore <идентификатор объекта> [--file <путь к файлу>]
```

Аргументы и ключи

`<идентификатор объекта>` – идентификатор объекта в резервном хранилище.

`--file <путь к файлу>` – новое имя файла и путь к директории, в которой его требуется сохранить. Если вы не укажете ключ `--file`, объект будет восстановлен с исходным именем в исходное местоположение.

Команды управления пользователями и ролями

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

Команда kesl-control --get-user-list

Команда позволяет вывести список пользователей и ролей.

Синтаксис команды

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

Команда kesl-control --grant-role

Команда позволяет присвоить роль определенному пользователю.

Синтаксис команды

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

Команда kesl-control --revoke-role

Команда позволяет отозвать роль у определенного пользователя.

Синтаксис команды

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

Команды управления параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA)

-R – префикс, указывающий, что команда принадлежит к группе команд управления параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA) и с Kaspersky Endpoint Detection and Response Optimum.

Команда kesl-control --add-kataedr-server-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат сервера KATA.

Синтаксис команды

```
kesl-control [-R] --add-kataedr-server-certificate <путь к файлу>
```

Аргументы и ключи

<путь к файлу> – путь к файлу, содержащему сертификат сервера.

Команда kesl-control --remove-kataedr-server-certificate

Команда позволяет удалить сертификат сервера KATA.

Синтаксис команды

```
kesl-control [-R] --remove-kataedr-server-certificate
```

Команда kesl-control --query-kataedr-server-certificate

Команда позволяет вывести информацию о сертификате сервера KATA.

Синтаксис команды

```
kesl-control [-R] --query-kataedr-server-certificate
```

Команда kesl-control --add-kataedr-client-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат клиента, используемый для защиты подключения к серверу KATA.

Синтаксис команды

```
kesl-control [-R] --add-kataedr-client-certificate <путь к файлу>
```

Аргументы и ключи

<путь к файлу> – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

Команда kesl-control --remove-kataedr-client-certificate

Команда позволяет удалить сертификат клиента, используемый для защиты подключения к серверу KATA.

Синтаксис команды

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Команда kesl-control --query-kataedr-client-certificate

Команда позволяет вывести информацию о сертификате клиента.

Синтаксис команды

```
kesl-control [-R] --query-kataedr-client-certificate
```

Команда kesl-control --isolation-stat

Команда позволяет вывести в консоль текущее состояние сетевой изоляции: включена или выключена.

Синтаксис команды

```
kesl-control [-R] --isolation-stat
```

Команда kesl-control --isolation-off

Команда позволяет временно выключить сетевую изоляцию устройства.

Синтаксис команды

```
kesl-control [-R] --isolation-off
```

Команды управления параметрами интеграции с Kaspersky Endpoint Detection and Response Optimum

-R – префикс, указывающий, что команда принадлежит к группе команд управления параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA) и с Kaspersky Endpoint Detection and Response Optimum.

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum выполняется с помощью параметра `UseEdrOptimum` в общих параметрах приложения.

Команда kesl-control --isolation-stat

Команда позволяет вывести в консоль текущее состояние сетевой изоляции: включена или выключена.

Синтаксис команды

```
kesl-control [-R] --isolation-stat
```

Команда kesl-control --isolation-off

Команда позволяет временно выключить сетевую изоляцию устройства.

Синтаксис команды

```
kesl-control [-R] --isolation-off
```

Команды приложения в режиме Легкого агента для защиты виртуальных сред

-V – префикс, указывающий, что команда принадлежит к группе команд приложения Kaspersky Endpoint Security, используемого в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент).

> Команды могут быть выполнены, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Команда kesl-control --ksvla-info

Команда позволяет вывести информацию об использовании приложения в режиме Легкого агента для защиты виртуальных сред.

Синтаксис команды

```
kesl-control --ksvla-info
```

Команда kesl-control --viis-info

Команда позволяет вывести информацию о подключении Легкого агента (приложения Kaspersky Endpoint Security, используемого в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент), к Серверу интеграции.

Синтаксис команды

```
kesl-control --viis-info
```

Команда kesl-control --svm-info

Команда позволяет вывести информацию о подключении Легкого агента (приложения Kaspersky Endpoint Security, используемого в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент), к SVM.

Синтаксис команды

```
kesl-control --svm-info
```

Приложение 3. Конфигурационные файлы и параметры приложения по умолчанию

Для управления работой приложения Kaspersky Endpoint Security используются следующие конфигурационные файлы:

- Конфигурационные файлы, которые содержат параметры первоначальной настройки приложения:
  - конфигурационный файл autoinstall.ini, который используется при установке приложения с помощью Kaspersky Security Center;
  - конфигурационный файл, который используется при установке приложения с помощью командной строки.
- Предустановленные конфигурационные файлы, которые создаются автоматически во время первоначальной настройки приложения и содержат значения параметров, заданные при первоначальной настройке. Эти параметры применяются во время работы приложения.
- Конфигурационные файлы, которые вы можете создавать с помощью команд управления Kaspersky Endpoint Security. Эти конфигурационные файлы могут содержать параметры задач и другие параметры приложения. Вы можете изменять эти файлы и импортировать их в приложение, чтобы изменять соответствующие параметры.

Правила редактирования конфигурационных файлов задач приложения

При редактировании конфигурационного файла соблюдайте следующие правила:

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

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

  Символы "пробел" и "табуляция" игнорируются перед первой кавычкой и после последней кавычки строкового значения, а также в начале и в конце строкового значения, не заключенного в кавычки.
- Если вам нужно указать несколько значений параметра, повторите параметр столько раз, сколько значений вы хотите указать.

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

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

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

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

  Пример:
  ```
  AreaDesc="Проверка почтовых баз"
  ```

  Одиночная кавычка в начале или в конце строки считается ошибкой.

Предустановленные конфигурационные файлы

После первоначальной настройки в приложении создаются следующие конфигурационные файлы:

- /var/opt/kaspersky/kesl/common/agreements.ini

  Конфигурационный файл agreements.ini содержит параметры, связанные с Лицензионным соглашением, Политикой конфиденциальности и Положением о Kaspersky Security Network.
- /var/opt/kaspersky/kesl/common/kesl.ini

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

Если требуется, вы можете изменять значения параметров в этих файлах.

Изменять значения по умолчанию в этих файлах рекомендуется под руководством специалистов Службы технической поддержки по полученным от них инструкциям.

Параметры конфигурационного файла kesl.ini

Параметр	Описание	Значени
Секция **[General]** содержит следующие параметры:		
`Locale`	Языковой стандарт, используемый для локализации текстов, передаваемых приложением Kaspersky Endpoint Security в Kaspersky Security Center (события, уведомления, результаты выполнения задач и другие).	Языковой стандарт в форм в RFC 3066.

	Локализация графического интерфейса и командной строки приложения зависит от локализации, указанной в переменной окружения `LANG`. Если в переменной окружения `LANG` указана локализация, которую не поддерживает приложение Kaspersky Endpoint Security, то графический интерфейс и командная строка отображаются в английской локализации.	Если параметр `Locale` не устанавливается язык лок операционной системы. Е удалось определить язык операционной системы ил операционной системы не устанавливается значение `en_US.utf8`.
`PackageType`	Формат установленного пакета приложения. Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения.	`rpm` – установлен пакет ф `deb` – установлен пакет ф
`UseFanotify`	Использование технологии fanotify. Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения.	`true/yes` – операционна поддерживает технологи `false/no` – операционна поддерживает технологи
`KsvlaMode`	Режим использования приложения Kaspersky Endpoint Security. Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения.	`true/yes` – приложение и режиме Легкого агента дл виртуальных сред. `false/no` – приложение и стандартном режиме.
`StartupTraces`	Включение создания файлов трассировки при запуске приложения.	`true/yes` – создавать фа при запуске приложения. `false/no` (значение по у создавать файлы трассир приложения.
`RevealSensitiveInfoInTraces`	Отображение в файлах трассировки информации, которая может содержать персональные данные (например, пароли).	`true/yes` – отображать и которая может содержать данные, в файлах трассир `false/no` (значение по у отображать информацию, содержать персональные трассировки.
`AsyncTraces`	Включение асинхронной трассировки, при которой запись информации в файлы трассировки происходит в асинхронном режиме.	`true/yes` – включить аси трассировку. `false/no` (значение по у включать асинхронную тр
`CoreDumps`	Включение создания файла дампа при сбое в работе приложения.	`true/yes` – создавать фа работе приложения.

		`false/no` (значение по ум создавать файл дампа при приложения.
`CoreDumpsPath`	Путь к директории, в которой хранятся файлы дампа.	Значение по умолчанию: /var/opt/kaspersky/kesl/co Для доступа к директории дампа, заданной по умолч root-права.
`MinFreeDiskSpace`	Минимальное количество памяти на диске, которое останется после записи файла дампа, в мегабайтах.	Значение по умолчанию: 3
`ScanMemoryLimit`	Ограничение на использование памяти приложением в мегабайтах.	Значение по умолчанию: 8
`MachineId`	Уникальный идентификатор устройства пользователя.	Значение параметра запо автоматически во время у приложения.
`SocketPath`	Путь к сокету для удаленного подключения, по которому подключаются, например, графический интерфейс и утилита kesl-control.	Значение по умолчанию: /
`MaxInotifyWatches`	Ограничение количества подписок на изменения в файлах и директориях (user watches), указанное в файле /proc/sys/fs/inotify/max_user_watches.	Значение по умолчанию: 3
`MaxInotifyInstances`	Ограничение количества подписок на изменения в файлах и директориях на одного пользователя.	Значение по умолчанию: 2
`ExecEnvMax`	Количество переменных окружения, которые приложение будет захватывать из вызова команды.	Значение по умолчанию: 5
`ExecArgMax`	Количество аргументов, которые приложение будет захватывать из вызова exec.	Значение по умолчанию: 5
`DisableFileAvActions`	Выключение функций лечения и удаления файлов для компонентов приложения после его установки. Если функции лечения и удаления файлов выключены, в случае обнаружения угрозы приложение не пытается лечить или удалять файлы, в которых обнаружена угроза, а только информирует пользователя об обнаружении угрозы.	`true/yes` – выключить фу удаления файлов при запу после установки. `false/no` (значение по ум выключать функции лечен файлов при запуске прило установки.
`AdditionalDNSLookup`	Использование публичного DNS.	`true/yes` – использовать доступа к серверам "Лабо Касперского". `false/no` (значение по ум использовать публичный D серверам "Лаборатории К

	При сбоях доступа к серверам через системный DNS приложение будет использовать публичный DNS. Это нужно для обновления баз приложения и поддержки уровня безопасности устройства. Приложение будет использовать следующие публичные DNS в порядке их обхода: • Google Public DNS™ (8.8.8.8). • Cloudflare® DNS (1.1.1.1). • Alibaba Cloud® DNS (223.6.6.6). • Quad9® DNS (9.9.9.9). • CleanBrowsing (185.228.168.168).	Запросы приложения м адреса доменов и внеш пользователя, так как пр устанавливает с DNS-се TCP/UDP-соединение. З нужны, например, для пр сертификата веб-ресур обращении по HTTPS. Е использует публичный D правила обработки дан регламентируются Поли конфиденциальности эт требуется запретить пр использовать публичны обратитесь в Службу те поддержки за приватны
Секция **[Network]** содержит следующие параметры:		
`WtpFwMark`	Метка в правилах утилиты iptables для перенаправления трафика в приложение для обработки компонентом Защита от веб-угроз. Вам может потребоваться изменить эту метку, если на одном устройстве с установленным приложением работает другое ПО, которое использует девятый бит маски TCP-пакета, и возникает конфликт.	Значение задается десяте шестнадцатеричным числ Значение по умолчанию: 0
`NtpFwMark`	Метка в правилах утилиты iptables для перенаправления трафика в приложение для обработки компонентом Защита от сетевых угроз. Вам может потребоваться изменить эту метку, если на одном устройстве с установленным приложением работает другое ПО, которое использует девятый бит маски TCP-пакета, и возникает конфликт.	Значение задается десяте шестнадцатеричным числ Значение по умолчанию: 0
`BypassFwMark`	Метка, которой маркируются пакеты, созданные или проверенные приложением, чтобы они снова не попали в приложение на проверку.	Значение задается десяте шестнадцатеричным числ Значение по умолчанию: 0
`BypassNFlogMark`	Метка, которой маркируются пакеты, созданные или проверенные приложением, чтобы исключить запись о них в журнал утилиты iptable.	Значение задается десяте шестнадцатеричным числ Значение по умолчанию: 0
`ProxyRouteTable`	Номер таблицы маршрутизации.	Значение по умолчанию: 1
Секция **[Virtualization]** содержит следующие параметры:		
`ServerMode`	Роль защищенной виртуальной машины, на которой приложение Kaspersky Endpoint Security	`true/yes` – виртуальная м используется как сервер.

	используется в режиме Легкого агента для защиты виртуальных сред: сервер или рабочая станция. Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения.	`false/no` – виртуальная м используется как рабочая
`VdiMode`	Включение режима защиты инфраструктуры VDI в случае использования приложения в режиме Легкого агента для защиты виртуальных сред. Настройка этого параметра не влияет на работу приложения. Значение параметра заполняется автоматически во время первоначальной настройки приложения.	`true/yes` – режим защит VDI включен. `false/no` – режим защит VDI выключен.
Секция **[Watchdog]** содержит следующие параметры:		
`TimeoutAfterHeadshot`	Максимальное время ожидания завершения процесса kesl от момента отправки сигнала HEADSHOT Watchdog-сервером процессу kesl.	Значение по умолчанию: 2
`StartupTimeout`	Максимальное время ожидания запуска приложения (в минутах), после которого процесс kesl будет перезапущен.	Значение по умолчанию: 3
`TimeoutAfterKill`	Максимальное время ожидания завершения управляемого процесса kesl от момента отправки сигнала SIGKILL Watchdog-сервером процессу kesl. Если по истечении этого времени процесс kesl не завершился, выполняется действие, заданное параметром --failed-kill.	Значение по умолчанию: 2
`PingInterval`	Периодичность, с которой приложение пытается отправить серверу сообщение PONG в ответ на принятое сообщение PING.	Значение по умолчанию: 2
`MaxRestartCount`	Максимальное количество неудачных последовательных попыток запуска приложения.	Значение по умолчанию: 5
`ActivityTimeout`	Максимальный интервал времени, в течение которого приложение должно отправить сообщение Watchdog-серверу. Если в течение этого интервала времени от приложения не будет сообщения, Watchdog-сервер начнет процедуру завершения процесса kesl.	Значение по умолчанию: 2

`ConnectTimeout`	Максимальный интервал времени от момента запуска процесса kesl до момента установления приложением соединения с Watchdog-сервером. Если приложение не успевает создать соединение за этот интервал времени, Watchdog-сервер начнет процедуру завершения процесса kesl.	Значение по умолчанию: 3
`RegisterTimeout`	Максимальный интервал времени от момента соединения приложения с Watchdog-сервером до получения сервером сообщения REGISTER.	Значение по умолчанию: 5
`TimeoutAfterShutdown`	Максимальное время ожидания завершения процесса kesl от момента отправки сигнала SHUTDOWN Watchdog-сервером процессу kesl.	Значение по умолчанию: 2
`MaxMemory`	Ограничение на использование резидентной памяти процесса kesl. Если резидентная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения процесса kesl.	`off` – использование рези ограничено. `< значение >%` – значение процентах от объема пам `< значение >MB` – значени `lowest/< значение >%/<` наименьшее значение меж процентах и значением в м `highest/< значение >%/` наибольшее значение меж процентах и значением в м `auto` – до 50% доступной менее 2ГБ и не более 16ГБ Значение по умолчанию: a
`MaxVirtualMemory`	Ограничение на использование виртуальной памяти процесса kesl. Если виртуальная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения процесса kesl.	`off` (значение по умолчан использование виртуальн ограничено. `< значение >MB` – значени
`MaxSwapMemory`	Ограничение на размер swap-файла управляемого процесса kesl. Если swap-файл управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру завершения процесса kesl.	`off` (значение по умолча swap-файла не ограничен `< значение >%` – значение процентах от объема пам `< значение >MB` – значени `lowest/< значение >%/<` наименьшее значение меж процентах и значением в м `highest/< значение >%/` наибольшее значение меж процентах и значением в м
`TrackProductCrashes`	Включение мониторинга стабильности работы приложения.	`true/yes` – включить мон стабильности работы при

	Если мониторинг стабильности работы приложения включен, Watchdog-сервер отслеживает количество нештатных остановок приложения.	`false/no` (значение по ум выключить мониторинг ст приложения.
`ProductHealthLogFile`	Путь к файлу, с помощью которого осуществляется мониторинг стабильности приложения.	Значение по умолчанию: /var/opt/kaspersky/kesl/pr
`WarnThreshold`	Интервал времени (в секундах), за который приложение должно посчитать количество нештатных остановок, прежде чем вывести уведомление о нестабильной работе.	Значение по умолчанию: 3
`WarnAfter_#_crash`	Количество нештатных остановок приложения, необходимых для отображения уведомления о нестабильной работе приложения.	Значение по умолчанию: 1 Если указано значение 0, у нестабильной работе при отображается.
`WarnRemovingThreshold`	Интервал времени (в секундах), по истечении которого статус о нестабильной работе приложения будет снят.	Значение по умолчанию: 8
Секция **[Environment]** по умолчанию отсутствует в конфигурационном файле.		
`ExperimentalContainerdSupport`	Включение поддержки среды containerd при работе компонента Мониторинг контейнеров. Этот параметр по умолчанию отсутствует в конфигурационном файле. Если вы хотите использовать среду containerd при работе компонента Мониторинг контейнеров, вам нужно вручную добавить в конфигурационный файл секцию `[Environment]` и добавить в нее параметр `ExperimentalContainerdSupport`.	`true/yes` – включить под containerd в работе компо контейнеров. `false/no` – не включать г containerd в работе компо контейнеров.

Параметры задач командной строки по умолчанию

Этот раздел содержит параметры по умолчанию всех предустановленных задач, которые предусмотрены для управления приложением Kaspersky Endpoint Security с помощью командной строки.

Задачи *Rollback* и *License* не имеют параметров.

Параметры по умолчанию задачи File_Threat_Protection (ID:1)

```
ScanArchived=No
```

```
ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

SkipPlainTextFiles=No

TimeLimit=60

SizeLimit=0

FirstAction=Recommended

SecondAction=Block

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanByAccessType=SmartCheck

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Параметры по умолчанию задачи Scan_My_Computer (ID:2)

```
ScanFiles=Yes

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes
```

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Параметры по умолчанию задачи Scan_File (ID:3)

```
ScanFiles=Yes

ScanBootSectors=No
```

```
ScanComputerMemory=No

ScanStartupObjects=No

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Параметры по умолчанию задачи Critical_Areas_Scan (ID:4)

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

Параметры по умолчанию задачи Update (ID:6)

```
SourceType=KLServers

UseKLServersWhenUnavailable=Yes

ApplicationUpdateMode=DownloadOnly

ConnectionTimeout=10
```

Параметры по умолчанию задачи Backup (ID:10)

```
DaysToLive=90

BackupSizeLimit=0

BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

Параметры по умолчанию задачи System_Integrity_Monitoring (ID:11)

```
UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=Kaspersky internal objects

UseScanArea=Yes

Path=/opt/kaspersky/kesl/

AreaMask.item_0000=*
```

Параметры по умолчанию задачи Firewall_Management (ID:12)

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

OpenNagentPorts=Yes

[NetworkZonesTrusted]

[NetworkZonesLocal]

[NetworkZonesPublic]
```

Параметры по умолчанию задачи Anti_Cryptor (ID:13)

```
ActionOnDetect=Block

BlockTime=30

UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=All shared directories

UseScanArea=Yes

Path=AllShared

AreaMask.item_0000=*
```

Параметры по умолчанию задачи Web_Threat_Protection (ID:14)

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Параметры по умолчанию задачи Device_Control (ID:15)

```
OperationMode=Block

[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

[Schedules.item_0000]

ScheduleName=Default

DaysHours=All

[HardDrivePrincipals.item_0000]

Principal=\Everyone

[HardDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[RemovableDrivePrincipals.item_0000]

Principal=\Everyone

[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]
```

```
UseRule=Yes

ScheduleName=Default

Access=Allow

[FloppyDrivePrincipals.item_0000]

Principal=\Everyone

[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[OpticalDrivePrincipals.item_0000]

Principal=\Everyone

[OpticalDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow
```

Параметры по умолчанию задачи Removable_Drives_Scan (ID:16)

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Параметры по умолчанию задачи Network_Threat_Protection (ID:17)

```
ActionOnDetect=Block

BlockAttackingHosts=Yes

BlockDurationMinutes=60

UseExcludeIPs=No
```

Параметры по умолчанию задач Container_Scan (ID:18) и Custom_Container_Scan (ID:19)

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanContainers=Yes

ContainerNameMask=*

ScanImages=Yes

ImageNameMask=*

DeepScan=No

ContainerScanAction=StopContainerIfFailed

ImageAction=Skip

UseGlobalExclusions=Yes
```

Вы можете использовать параметры этого конфигурационного файла также для задачи Выборочная проверка контейнеров.

Параметры по умолчанию задачи Behavior_Detection (ID:20)

```
UseTrustedPrograms=No

TaskMode=Block
```

Параметры по умолчанию задачи Application_Control (ID:21)

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Параметры по умолчанию задачи Inventory_Scan (ID:22)

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

CreateGoldenImage=No

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

Параметры по умолчанию задачи KATAEDR (ID:24)

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=
```

```
Port=443

[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Параметры по умолчанию задачи Web_Control (ID:26)

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

Общие параметры приложения

Общие параметры приложения определяют работу приложения в целом и работу отдельных функций.

Общие параметры приложения

Параметр	Описание	Значения
`SambaConfigPath`	Директория, в которой хранится конфигурационный файл Samba. Конфигурационный файл Samba нужен для обеспечения работы значений `AllShared` или `Shared:SMB` для параметра `Path`.	По умолчанию указана станда конфигурационного файла Sa Значение по умолчанию: /etc После изменения значения эт требуется перезапустить при
`NfsExportPath`	Директория, в которой хранится конфигурационный файл NFS. Конфигурационный файл NFS нужен для обеспечения работы значений `AllShared` или `Shared:NFS` для параметра `Path`.	По умолчанию указана станда конфигурационного файла NF Значение по умолчанию: /etc После изменения значения эт требуется перезапустить при
`TraceLevel`	Включение трассировки приложения и уровень детализации файлов трассировки.	`Detailed` – создавать детал трассировки. `MediumDetailed` – создават содержащий информационны сообщения об ошибках. `NotDetailed` – создавать фа содержащий сообщения об с `None` (значение по умолчани файл трассировки.
`TraceFolder`	Директория, в которой хранятся файлы трассировки	Значение по умолчанию: /var

	приложения.	Если вы указываете другую д убедитесь, что она разрешен для учетной записи, под кото Kaspersky Endpoint Security. Д директории хранения файлов заданной по умолчанию, треб После изменения значения э требуется перезапустить при
`TraceMaxFileCount`	Максимальное количество файлов трассировки приложения.	1–10000 Значение по умолчанию: 10. После изменения значения э требуется перезапустить при
`TraceMaxFileSize`	Максимальный размер файла трассировки приложения (в мегабайтах).	1–1000 Значение по умолчанию: 500 После изменения значения э требуется перезапустить при
`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 проверки пропускают такой файл во время проверки. Этот параметр недоступен для операционных систем, в которых используется технология fanotify.	4096–33554432 Значение по умолчанию: 1638 После изменения значения э требуется перезапустить зад файловых угроз.
`DetectOtherObjects`	Включение обнаружения легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.	`Yes` – включить обнаружение приложений, которые злоумы использовать для нанесения или данным. `No` (значение по умолчанию) обнаружение легальных прил злоумышленники могут испол нанесения вреда устройства
`NamespaceMonitoring`	Включение проверки пространств имен и контейнеров. Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен.	`Yes` (значение по умолчанию проверку пространств имен и `No` – выключить проверку про контейнеров.

`FileBlockDuringScan`	Включение режима перехвата файловых операций с блокированием доступа к файлам на время проверки. Режим перехвата файловых операций влияет на работу компонентов Защита от файловых угроз и Контроль устройств.	`Yes` (значение по умолчанию доступ к файлам на время пр `No` – не блокировать доступ проверки. Обращение к любо разрешается, проверка выпо асинхронном режиме. Такой р файловых операций оказывае на производительность систе работы, но есть риск, что угр будет вылечена или удалена, проверки этот файл сможет, свое имя до принятия прилож статусе этого файла.
`UseKSN`	Включение использования Kaspersky Security Network.	`Basic` – включить использов Security Network в стандартн `Extended` – включить исполь Security Network в расширен `No` (значение по умолчанию) использование Kaspersky Sec
`CloudMode`	Включение облачного режима работы приложения. Облачный режим доступен, если включено использование KSN. Если вы планируете использовать облачный режим, убедитесь, что KSN доступен на устройстве. Параметр применяется, только если приложение используется в стандартном режиме.	`Yes` – включить режим работ приложение Kaspersky Endpo использует облегченную вер вредоносного ПО. `No` (значение по умолчанию) полную версию баз вредонос Облачный режим выключае автоматически, если выклю использование KSN.
`UseMDR`	Включение компонента Managed Detection and Response для интеграции с Kaspersky Managed Detection and Response.	`Yes` – включить компонент M and Response. `No` (значение по умолчанию) компонент Managed Detectio
`UseProxy`	Включение использования прокси-сервера компонентами приложения Kaspersky Endpoint Security. Прокси-сервер может использоваться для взаимодействия с Kaspersky Security Network, с Kaspersky Endpoint Detection and Response (KATA), для активации приложения и при обновлении баз и модулей приложения.	`Yes` – включить использован `No` (значение по умолчанию) использование прокси-серве Если выбрано значение `Yes`, Kaspersky Endpoint Detection (KATA) будет выполняться чер

	Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование прокси-сервера для подключения к Kaspersky Security Network, к SVM и к Серверу интеграции.	
`ProxyServer`	Параметры прокси-сервера в формате `[<пользователь>[:<пароль>]@]<адрес прокси-сервера>[:<порт>]`. Для подключения через HTTP прокси рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP прокси использует незащищенное соединение, и учетная запись может быть скомпрометирована.	—
`MaxEventsNumber`	Максимальное количество событий, которые будет хранить приложение. При превышении заданного количества событий приложение удаляет наиболее давние события.	Значение по умолчанию: 500 Если задано значение 0, то со сохраняются.
`LimitNumberOfScanFileTasks`	Максимальное количество задач выборочной проверки, которые непривилегированный пользователь может одновременно запустить на устройстве. Этот параметр не ограничивает количество задач, которые может запустить пользователь с root-правами.	0–4294967295 Значение по умолчанию: 0. Если задано значение 0, непр пользователь не может запус выборочной проверки. Если во время установки при установили пакет графическ параметра `LimitNumberOfSc` умолчанию используется зна
`UseSyslog`	Включение записи информации о событиях в syslog. Для доступа к syslog требуются root-права.	`Yes` – включить запись инфор syslog. `No` (значение по умолчанию) информации о событиях в sys

`EventsStoragePath`	Директория базы данных, в которой приложение сохраняет информацию о событиях. Для доступа к заданной по умолчанию базе данных событий требуются root-права.	Значение по умолчанию: /var/opt/kaspersky/kesl/privat
`ExcludedMountPoint.item_#`	Точка монтирования, которую требуется исключить из области проверки. Исключение применяется в работе компонентов Защита от файловых угроз, Защита от шифрования, Мониторинг контейнеров и задачи Проверка съемных дисков, а также настраивается в работе задач проверки (типов ODS и ContainerScan). Вы можете указать несколько точек монтирования, которые требуется исключить из проверки. Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды `mount`. Параметр `ExcludedMountPoint.item_#` по умолчанию не указан.	`AllRemoteMounted` – исключ файловых операций все удал смонтированные на устройст протоколов SMB и NFS. `Mounted:NFS` – исключать из файловых операций все удал смонтированные на устройст протокола NFS. `Mounted:SMB` – исключать из файловых операций все удал смонтированные на устройст протокола SMB. `Mounted:<тип файловой с` исключать из перехвата файл смонтированные директории файловой системы. `/mnt` – исключать из перехва находящиеся в точке монтир (включая вложенные директо в качестве временной точки м съемных дисков. `<путь, содержащий маску /mnt/**/user_share>` – иск перехвата объекты, находящи монтирования, имена которы указанную маску.

		Вы можете использовать с
		(звездочка) для формирова
		файла или директории.
		
		Вы можете указать один си
		любого набора символов (в
		набор), предшествующего
		имени файла или директор
		`/dir/*/file` или `/dir/*/`
		
		Вы можете указать два пос
		идущих символа `*` вместо
		символов (включая пустой
		файла или директории, вкл
		`/`. Например, `/dir/**/fil`
		`/dir/file**/`.
		
		Маску `**` можно использо
		директории только один ра
		`/dir/**/**/file` – это не
		маска.
		
		Для исключения точки мон
		требуется указывать имен
		звездочек).
		
		Маска `/dir/*` исключает в
		монтирования на уровень н
		не саму точку монтировани
		`/dir/**` исключает все то
		на любом уровне вложенно
		не саму точку монтировани
		
		Вы можете использовать с
		любого одного символа в и
		директории.

`MemScanExcludedProgramPath.item_#`	Исключение памяти процесса из проверки. Приложение не будет проверять память указанного процесса.	`<полный путь к процессу` проверки процесс в указанно директории. Для указания пут использовать маски.

		Вы можете использовать си
		(звездочка) для формирова
		файла или директории.
		
		Вы можете указать один си
		любого набора символов (в
		набор), предшествующего
		имени файла или директор
		`/dir/*/file` или `/dir/*/`
		
		Вы можете указать два пос
		идущих символа `*` вместо
		символов (включая пустой
		файла или директории, вкл
		`/`. Например, `/dir/**/fil`
		`/dir/file**/`.
		
		Маску `**` можно использо
		директории только один ра
		`/dir/**/**/file` – это не
		маска.
		
		Вы можете использовать си
		любого одного символа в и
		директории.

`UseOnDemandCPULimit`	Включение ограничения на использование ресурсов процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan*.	`Yes` – включить ограничение ресурсов процессора для зад *ContainerScan* и *InventorySca* `No` (значение по умолчанию) ограничение потребления ре для задач.
`OnDemandCPULimit`	Максимальное значение нагрузки на все ядра процессора (в процентах) при работе задач типа *ODS*, *ContainerScan* и *InventoryScan*.	10–100 Значение по умолчанию: 100.
`UseEdrOptimum`	Включение компонента EDR Optimum для интеграции с Kaspersky Endpoint Detection and Response Optimum.	`Yes` – включить компонент ED `No` (значение по умолчанию) компонент EDR Optimum.

Общие параметры проверки контейнеров

Общие параметры проверки контейнеров используются при проверке пространств имен и контейнеров в реальном времени.

Общие параметры проверки контейнеров и пространств имен

Параметр	Описание	Значения
`OnAccessContainerScanAction`	Действие над контейнером при обнаружении зараженного объекта.	`StopContainerIfFailed` (значение по умолчанию)

	Этот параметр доступен при использовании приложения по лицензии, которая включает эту функцию. При проверке объектов внутри контейнера используются параметры задачи Защита от файловых угроз. Действие над контейнером при обнаружении зараженного объекта также зависит от заданных параметров задачи Защита от файловых угроз (см. таблицу ниже).	– остановить контейнер, если не удалось вылечить или удалить зараженный объект. `StopContainer` – остановить контейнер при обнаружении зараженного объекта. `Skip` – не выполнять никаких действий над контейнерами при обнаружении зараженного объекта.
`UseDocker`	Использование среды Docker.	`Yes` (значение по умолчанию) – использовать среду Docker. `No` – не использовать среду Docker.
`DockerSocket`	Путь или URI (универсальный идентификатор ресурса) Docker-сокета.	Значение по умолчанию: /var/run/docker.sock.
`UseCrio`	Использование среды CRI-O.	`Yes` (значение по умолчанию) – использовать среду CRI-O. `No` – не использовать среду CRI-O.
`CrioConfigFilePath`	Путь к конфигурационному файлу CRI-O.	Значение по умолчанию: /etc/crio/crio.conf.
`UsePodman`	Использование утилиты Podman.	`Yes` (значение по умолчанию) – использовать утилиту Podman. `No` – не использовать утилиту Podman.
`PodmanBinaryPath`	Путь к исполняемому файлу утилиты Podman.	Значение по умолчанию: /usr/bin/podman.
`PodmanRootFolder`	Путь к корневой директории хранилища контейнеров.	Значение по умолчанию: /var/lib/containers/storage.
`UseRunc`	Использование утилиты runc.	`Yes` (значение по умолчанию) – использовать утилиту runc. `No` – не использовать утилиту runc.
`RuncBinaryPath`	Путь к исполняемому файлу утилиты runc.	Значение по умолчанию: /usr/bin/runc.
`RuncRootFolder`	Путь к корневой директории хранилища состояний контейнеров.	Значение по умолчанию: /run/runc.

Действие над контейнером при обнаружении зараженного объекта может меняться в зависимости от заданных значений параметров `FirstAction` и `SecondAction` задачи Защита от файловых угроз.

Зависимость действия над контейнером от заданного действия при обнаружении угрозы

Значение параметра FirstAction / SecondAction	Действие, выполняемое над контейнером при выбранном действии StopContainerIfFailed
`Disinfect`	Остановить контейнер, если не удалось вылечить зараженный объект.
`Remove`	Остановить контейнер, если не удалось удалить зараженный объект.

Параметры проверки защищенных соединений

Параметры проверки защищенных соединений

Параметр	Описание	Значения
`EncryptedConnectionsScan`	Включает или выключает проверку зашифрованного трафика. Для FTP-протокола проверка защищенных соединений по умолчанию выключена.	`Yes` (значение по умолчанию) – включить проверку защищенных соединений. `No` – выключить проверку защищенных соединений. Приложение не расшифровывает зашифрованный трафик.
`EncryptedConnectionsScanErrorAction`	Действие, выполняемое приложением при возникновении ошибки проверки защищенных соединений на веб-сайте.	`AddToAutoExclusions` (значение по умолчанию) – добавить домен, на котором возникла ошибка, в список доменов с ошибками проверки. Приложение не будет контролировать зашифрованный сетевой трафик при посещении этого домена. `Disconnect` – заблокировать сетевое соединение.
`CertificateVerificationPolicy`	Задает способ проверки сертификатов приложением Kaspersky Endpoint Security. Если сертификат является самоподписанным, приложение не выполняет дополнительную проверку.	`FullCheck` (значение по умолчанию) – приложение использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата. `LocalCheck` – приложение не использует интернет для проверки сертификата.

`UntrustedCertificateAction`	Действие, выполняемое приложением при обнаружении неподтвержденного сертификата.	`Allow` (значение по умолчанию) – разрешить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом. `Block` – запретить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом.
`ManageExclusions`	Использование исключений при проверке зашифрованного трафика.	`Yes` – не проверять веб-сайты, указанные в секции `[Exclusions.item_#]` (см. ниже). `No` (значение по умолчанию) – проверять все веб-сайты.
`MonitorNetworkPorts`	Способ контроля сетевых портов приложением Kaspersky Endpoint Security.	`Selected` (значение по умолчанию) – контролировать только сетевые порты, указанные в секции `[NetworkPorts.item_#]` (см. ниже). `All` – контролировать все сетевые порты. Выбор этого значения может значительно увеличить нагрузку на операционную систему.
Секция **[Exclusions.item_#]** содержит домены, исключенные из проверки. Приложение не проверяет защищенные соединения, установленные при посещении указанных доменов.		
`DomainName`	Имя домена. Для указания домена можно использовать маски.	Значение по умолчанию не задано.
Секция **[NetworkPorts.item_#]** содержит сетевые порты, контролируемые приложением.		
`PortName`	Описание сетевого порта.	Значение по умолчанию не задано.
`Port`	Номера сетевых портов, контролируемые приложением.	`1 – 65535` Значение по умолчанию не задано.

Параметры расписания задач

Параметры расписания запуска задачи

Параметр	Описание	Значения
`RuleType`	Расписание запуска задачи.	`Once` – запускать задачу один раз.

		`Monthly` – запускать задачу каждый месяц в указанный день и в указанное время. `Weekly` – запускать задачу каждую неделю в указанный день и в указанное время. `Daily` – запускать задачу регулярно, с заданным интервалом в днях. `Hourly` – запускать задачу регулярно, с заданным интервалом в часах, начиная с указанных даты и времени. `Minutely` – запускать задачу регулярно, с заданным интервалом в минутах, начиная с указанного времени. `Manual` – запускать задачу вручную. `PS` – запускать задачу после запуска приложения. `BR` – запускать задачу после обновления баз приложения.
`StartTime`	Дата и время запуска задачи. Параметр `StartTime` является обязательным, если параметр `RuleType` принимает одно из следующих значений Once, Monthly, Weekly, Daily, Hourly, Minutely.	`[<год>/<месяц>/<день месяца>] [чч]:[мм]:[сс]; [<день месяца>|<день недели>]; [<периодичность запуска>]`
`RandomInterval`	Интервал времени от 0 до указанного значения (в минутах), который будет добавлен ко времени запуска задачи, чтобы избежать одновременного запуска задач.	
`RunMissedStartRules`	Включение запуска пропущенной задачи после запуска приложения.	`Yes` – включать запуск пропущенной задачи после запуска приложения. `No` – не включать запуск пропущенной задачи после запуска приложения.

Приложение 4. Коды возврата командной строки

В приложении Kaspersky Endpoint Security предусмотрены следующие коды возврата командной строки:

0 – команда / задача выполнена успешно;

1 – общая ошибка в аргументах команды;

2 – ошибка в переданных параметрах приложения;

64 – приложение Kaspersky Endpoint Security не запущено;

66 – базы приложения 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 приложение работает под политикой;

69 – приложение находится в инфраструктуре Amazon Paid Ami;

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

71 – не приняты условия Положения о Kaspersky Security Network;

72 – при выполнении задачи Выборочная проверка или Выборочная проверка контейнеров обнаружены угрозы;

73 – попытка задать параметры задачи Контроль приложений, влияющие на работу приложения, без их подтверждения с помощью флага `--accept`.

74 – требуется перезапуск приложения Kaspersky Endpoint Security после обновления;

75 – требуется перезагрузка устройства;

76 – соединение запрещено, так как только пользователи с правами root должны иметь права на запись по указанному пути;

77 – указанный лицензионный ключ уже используется на устройстве;

128 – неизвестная ошибка;

65 – все остальные ошибки.

Приложение 5. Настройка совместной работы с Антивирусом Касперского для Linux Mail Server

Чтобы настроить совместную работу приложения Kaspersky Endpoint Security с Антивирусом Касперского для Linux Mail Server:

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>
   ```

Источники информации о Kaspersky Endpoint Security

Страница Kaspersky Endpoint Security в Базе знаний

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

На странице Kaspersky Endpoint Security в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

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

Обсуждение приложений "Лаборатории Касперского" на Форуме

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

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

Глоссарий

SIEM-система

SIEM-система (Security Information and Event Management) – решение для управления информацией и событиями в системе безопасности организации.

SVM

Secure virtual machine – специальная виртуальная машина, на которой установлена служба scanserver (Сервер защиты, компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент).

Активация приложения

Перевод приложения в полнофункциональный режим. Активация выполняется пользователем во время или после установки приложения. Для активации приложения пользователю необходим код активации или файл ключа.

Активная политика

Политика, которую приложение использует в данный момент для контроля утечек данных. Приложение может использовать несколько политик одновременно.

Активный ключ

Ключ, используемый в текущий момент для работы приложения.

База вредоносных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как опасное. Список сформирован специалистами "Лаборатории Касперского", регулярно обновляется и входит в поставку приложения "Лаборатории Касперского".

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами "Лаборатории Касперского" как фишинговые. База регулярно обновляется и входит в поставку приложения "Лаборатории Касперского".

Базы приложения

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска баз. Базы приложения формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

Группа администрирования

Набор устройств, объединенных в Kaspersky Security Center в соответствии с выполняемыми функциями и устанавливаемым на них набором приложений "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы администрирования могут входить другие группы. Для каждого из установленных в группе администрирования приложений могут быть созданы групповые политики и сформированы групповые задачи.

Групповая задача

Задача, назначенная для группы администрирования и выполняемая на всех управляемых устройствах, входящих в состав группы.

Групповая политика

см. Политика.

Доверенное устройство

Устройство, полный доступ к которому разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Зараженный объект

Объект, участок кода которого полностью совпадает с участком кода известной программы, представляющей угрозу. Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими объектами.

Исключение

Исключение – объект, исключаемый из проверки приложением "Лаборатории Касперского". Исключать из проверки можно файлы определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по названию согласно классификации Вирусной энциклопедии. Для каждой задачи могут быть заданы свои исключения.

Легкий агент

Компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент. Устанавливается на каждую виртуальную машину, которую требуется защищать.

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

Лицензия

Ограниченное по времени право на использование приложения, предоставляемое вам на основании Лицензионного соглашения.

Ложное срабатывание

Ситуация, когда незараженный объект определяется приложением "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Маска файла

Представление имени файла общими символами. Основными символами, используемыми в масках файлов, являются * и ? (где * – любое число любых символов, а ? – любой один символ).

Объекты автозапуска

Набор приложений, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

Параметры приложения

Параметры работы приложения, общие для всех типов его задач и отвечающие за работу приложения в целом, например: параметры производительности приложения, параметры ведения отчетов, параметры резервного хранилища.

Подписка

Использование приложения с выбранными настройками (дата окончания, количество устройств). Вы можете приостанавливать или возобновлять подписку, продлевать ее в автоматическом режиме, а также отказываться от нее.

Политика

Политика определяет параметры работы приложения и доступ к настройке приложения, установленного на устройствах группы администрирования. Для каждого приложения требуется создать свою политику. Вы можете создать неограниченное количество различных политик для приложений, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждому приложению.

Прокси-сервер

Служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо 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 клиента или ответ сервера может быть изменен прокси-сервером в определенных целях.

Резервный ключ

Ключ, подтверждающий право на использование приложения, но не используемый в текущий момент.

Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

Сервер интеграции

Компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент. Осуществляет взаимодействие между компонентами Kaspersky Endpoint Security и виртуальной инфраструктурой.

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы и FTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Amazon является товарным знаком Amazon.com, Inc. или аффилированных лиц компании.

FireWire – товарный знак Apple Inc.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Ubuntu и LTS являются зарегистрированными товарными знаками Canonical Ltd.

Citrix, XenServer являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Chrome, Google Public DNS – товарные знаки Google LLC.

HUAWEI, EulerOS, FusionSphere являются товарными знаками Huawei Technologies Co., Ltd.

Intel, Core – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

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

Microsoft, Active Directory, Hyper-V, Outlook, Visual C++ и Windows являются товарными знаками группы компаний Microsoft.

OpenStack – зарегистрированный товарный знак OpenStack Foundation в США и других странах.

Oracle, JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Red Hat, Red Hat Enterprise Linux, CentOS – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

VMware, VMware NSX, VMware NSX Manager, VMware Tools, VMware vCenter, VMware vSphere – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.